EPSON
EXCEED YOUR VISION

# Guia do Administrador

NPD5668-00 PT

# Índice de Conteúdo

**Índice de Conteúdo**



## *Apêndice*



## *Configurações de segurança avançada para empresas*

# Copyright

# Marcas registadas

- ❏ EPSON® é uma marca comercial registada e EPSON EXCEED YOUR VISION ou EXCEED YOUR VISION é uma marca comercial da Seiko Epson Corporation.
- ❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- ❏ Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- ❏ Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ❏ Aviso Geral: outros nomes de produtos aqui utilizados servem apenas propósitos de identificação e podem ser marcas comerciais dos respectivos proprietários. A Epson declina todos e quaisquer direitos sobre essas marcas.

# Informações sobre este manual

## Marcas e símbolos

> ⚠ ***Aviso:***
> *Instruções que têm de ser seguidas com cuidado para evitar ferimentos corporais.*

> ***Importante:***
> *Instruções que têm de ser respeitadas para evitar danos no equipamento.*

***Nota:***
*Instruções que contêm sugestões úteis e restrições relativas ao funcionamento do scanner.*

**Informações relacionadas**

➡ Clicar neste ícone dá-lhe acesso a informações relacionadas.

## Descrições utilizadas neste manual

❏ As capturas dos ecrãs do controlador do scanner e do Epson Scan 2 (controlador do digitalizador) são do Windows 10 ou do OS X El Capitan. O conteúdo apresentado nos ecrãs varia consoante o modelo e a situação.

❏ As ilustrações incluídas neste manual servem apenas como exemplo. Apesar de poderem existir ligeiras diferenças consoante o modelo, o método de funcionamento é idêntico.

❏ Alguns dos itens de menu no ecrã LCD podem variar consoante o modelo e as definições.

## Referências do sistema operativo

**Windows**

Neste manual, termos tais como "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Vista", "Windows XP", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012", "Windows Server 2008 R2", "Windows Server 2008", "Windows Server 2003 R2", e "Windows Server 2003" referem-se aos seguintes sistemas operativos. Adicionalmente, "Windows" é utilizado para se referir a todas as versões.

❏ Sistema operativo Microsoft® Windows® 10

❏ Sistema operativo Microsoft® Windows® 8.1

❏ Sistema operativo Microsoft® Windows® 8

❏ Sistema operativo Microsoft® Windows® 7

❏ Sistema operativo Microsoft® Windows Vista®

❏ Sistema operativo Microsoft® Windows® XP

❏ Sistema operativo Microsoft® Windows® XP Professional x64 Edition

- ❏ Sistema operativo Microsoft® Windows Server® 2016
- ❏ Sistema operativo Microsoft® Windows Server® 2012 R2
- ❏ Sistema operativo Microsoft® Windows Server® 2012
- ❏ Sistema operativo Microsoft® Windows Server® 2008 R2
- ❏ Sistema operativo Microsoft® Windows Server® 2008
- ❏ Sistema operativo Microsoft® Windows Server® 2003 R2
- ❏ Sistema operativo Microsoft® Windows Server® 2003

### Mac OS

Neste manual, "Mac OS" é usado para referir macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x, e Mac OS X v10.6.8.

# Introdução

## Componente de manual

Este manual destina-se ao administrador do dispositivo, o responsável pela ligação do scanner ou impressora à rede, e contém informações sobre como fazer as configurações para usar as funções.

Consulte o *Guia do Utilizador* para mais informações sobre a utilização de funções.

**Preparação**

Explica as tarefas do administrador, como configurar os dispositivos e o software de gestão.

**Ligação**

Explica como ligar um dispositivo à linha de rede ou telefone. Explica também o ambiente de rede, como a utilização de uma porta para o dispositivo, DNS e informações do servidor proxy.

**Definições de função**

Explica as definições para cada função do dispositivo.

**Definições básicas de segurança**

Explica as configurações para cada função, tais como impressão, digitalização e fax.

**Configurações de funcionamento e gestão**

Explica as operações após o início da utilização dos dispositivos, tais como verificação de informação e manutenção.

**Resolução de problemas**

Explica a inicialização de configurações e resolução de problemas da rede.

**Configurações de segurança avançada para empresas**

Explica o método de configurações para melhorar a segurança do dispositivo, por exemplo, usando o certificado da CA, comunicação SSL/TLS e filtragem IPsec/IP.

Dependendo do modelo, algumas funções neste capítulo não são suportadas.

## Definições de termos utilizados neste Guia

Segue-se uma lista dos termos utilizados neste Guia.

**Administrador**

A pessoa responsável pela instalação e configuração da rede ou o dispositivo num escritório ou organização. Em pequenas organizações, esta pessoa pode ser responsável pela administração dos dispositivos e da rede. Em organizações de maiores dimensões, os administradores têm autoridade sobre a rede ou dispositivos da unidade de

grupo de um departamento ou divisão, e os administradores de rede são responsáveis pelas configurações de comunicação para além da organização, como por exemplo a Internet.

### Administrador de rede

A pessoa responsável pelo controlo das comunicações de rede. A pessoa que configura o router, servidor proxy, servidor DNS e servidor de correio para controlo de comunicações através da Internet ou rede.

### Utilizador

A pessoa que usa dispositivos tais como impressoras ou scanners.

### Web Config (página Web do dispositivo)

O servidor Web incorporado no dispositivo. É designado Web Config. É possível verificar e alterar o estado do dispositivo no mesmo usando o navegador.

### Instrumento

Um termo genérico para software para configurar ou gerir um dispositivo, como por exemplo Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, etc.

### Digitalização de um toque (push scan)

Termo genérico para digitalização a partir do painel de controlo do dispositivo.

### ASCII (código-padrão americano para o intercâmbio de informações)

Um dos códigos de caracteres padrão. São definidos 128 caracteres, incluindo caracteres do alfabeto (a–z, A–Z), números árabes (0–9), símbolos, caracteres em branco e caracteres de controlo. Quando "ASCII" é descrito neste guia, refere-se a 0x20–0x7E (número hexadecimal) listado abaixo e não inclui caracteres de controlo.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SP* | ! | " | # | $ | % | & | ' | ( | ) | * | + | , | - | . | / |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | : | ; | < | = | > | ? |
| @ | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| P | Q | R | S | T | U | V | W | X | Y | Z | [ | \ | ] | ^ | _ |
| ` | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o |
| p | q | r | s | t | u | v | w | x | y | z | { | \| | } | ~ | |

* Espaço.

### Unicode (UTF-8)

Um código de padrão internacional, cobrindo as principais línguas globais. Quando "UTF-8" é descrito neste manual, refere-se à codificação de caracteres no formato UTF-8.

# Preparação

Este capítulo explica a função do administrador e a preparação antes de fazer ajustes.

## Fluxo das configurações e gestão do scanner

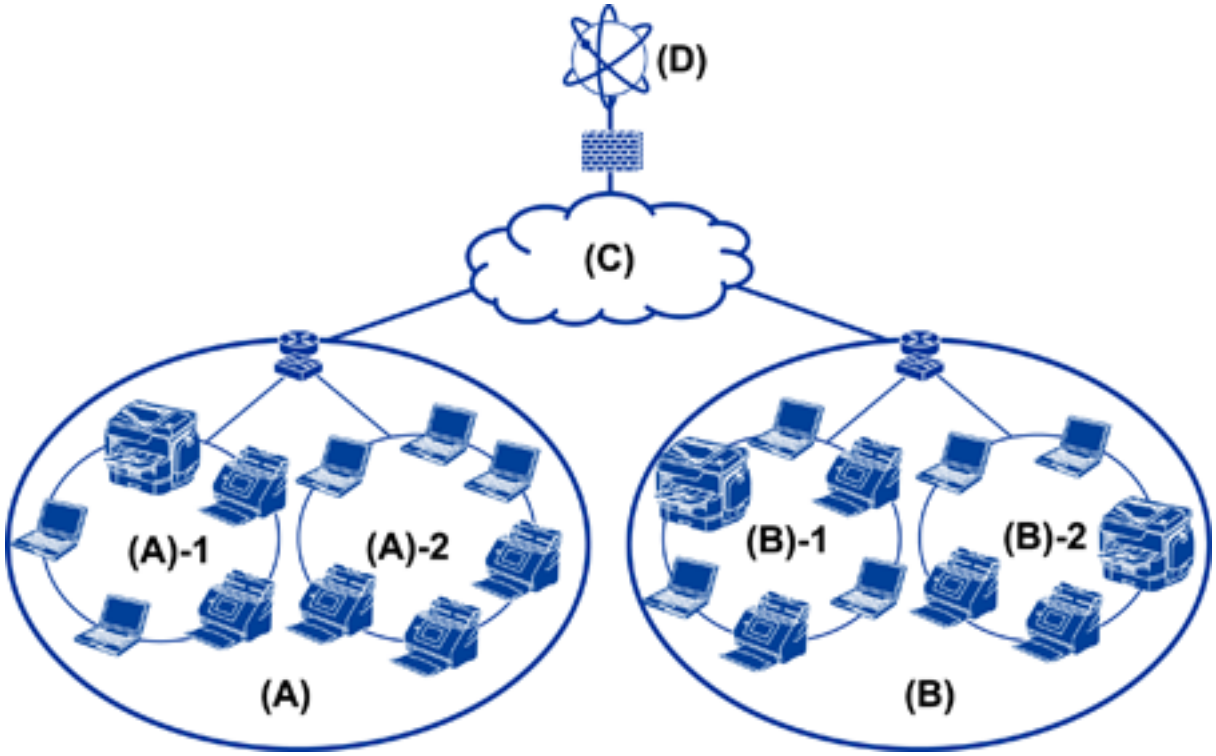
O administrador faz as configurações de ligação de rede, a configuração inicial e de manutenção do scanner ou o scanner para que possam estar disponíveis para os utilizadores.

1. Preparar
   - ❏ Recolher as informações de definição de ligação
   - ❏ Decisão do método de ligação
2. Em ligação
   - ❏ Ligação de rede a partir do painel de controlo do scanner
3. Definir as funções
   - ❏ Definições do controlador do scanner
   - ❏ Outras definições avançadas
4. Definições de segurança
   - ❏ Definições do administrador
   - ❏ SSL/TLS
   - ❏ Controlo de protocolo
   - ❏ Definições de segurança avançada (opção)
5. Funcionamento e gestão
   - ❏ Verificar o estado do dispositivo
   - ❏ Processamento do surgimento de eventos
   - ❏ Cópia de segurança das definições do dispositivo

**Informações relacionadas**

➡ “Preparação” na página 10
➡ “Ligação” na página 15
➡ “Definições de função” na página 22
➡ “Definições básicas de segurança” na página 32
➡ “Configurações de funcionamento e gestão” na página 40

# Exemplo de um ambiente de rede




(A): Office 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Office 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

## Introdução do exemplo de configuração de ligação do scanner

Existem principalmente dois tipos de ligação, dependendo de como usar o scanner. Ambos ligam o scanner à rede com o computador através do hub.

❏ Ligação servidor/cliente (scanner usando o servidor Windows, gestão da tarefa)

❏ Ligação ponto a ponto (ligação direta pelo computador do cliente)

### Informações relacionadas

➡ “Ligação servidor/cliente” na página 12

➡ “Ligação ponto a ponto” na página 12

## Ligação servidor/cliente

Centralizar a gestão de scanner e tarefa com Document Capture Pro Server instalado no servidor. É mais apropriado para o trabalho que usa vários scanners para digitalizar um grande número de documentos num determinado formato.

### Informações relacionadas

➡ "Definições de termos utilizados neste Guia" na página 8

## Ligação ponto a ponto

Use um scanner individual com um controlador de scanner como por exemplo Epson Scan 2 instalado no computador cliente. Instalar Document Capture Pro (Document Capture) no computador cliente permite-lhe executar tarefas nos computadores individuais cliente do scanner.

### Informações relacionadas

➡ "Definições de termos utilizados neste Guia" na página 8

# Preparar a ligação a uma rede

## Reunir informações sobre as informações de ligação

É necessário ter um endereço IP, endereço de gateway, etc., para ligação de rede. Verifique previamente o seguinte.

| Divisões | Itens | Nota |
|---|---|---|
| Método de ligação do dispositivo | ❏ Ethernet | Utilize um cabo de categoria 5e ou STP superior (cabo blindado de par trançado) para ligação Ethernet. |
| Informações de ligação LAN | ❏ Endereço IP<br>❏ Máscara de sub-rede<br>❏ Gateway predefinido | Se definir automaticamente o endereço IP, não é necessário utilizar a função DHCP do router. |
| Informações de servidor DNS | ❏ Endereço IP para DNS primário<br>❏ Endereço IP para DNS secundário | Se usar um endereço IP estático como o endereço IP, configurar o servidor DNS.<br>Configurar ao atribuir automaticamente utilizando a função DHCP e quando o servidor DNS não puder ser atribuído automaticamente. |
| Informações de servidor proxy | ❏ Nome de servidor proxy<br>❏ Número da porta | Configurar ao usar um servidor proxy para ligação Internet e ao usar o serviço Epson Connect ou a função de atualização automática de firmware. |

# Especificações do digitalizador

Para ver as especificação de compatibilidade do scanner com o modo padrão ou de ligação, consulte o *Guia do Utilizador*.

# Usar o número de porta

Consultar o "Índice" para o número de porta utilizado pelo scanner.

### Informações relacionadas

➡ "Usar a porta para o scanner" na página 60

# Atribuição dos tipos de endereço IP

Existem dois tipos para atribuir um endereço IP ao scanner.

### Endereço IP estático:

Atribua o endereço IP exclusivo predeterminado ao scanner.

O endereço IP não é alterado mesmo ao desligar o scanner ou o router, para que possa gerir o dispositivo por endereço IP.

Este tipo é adequado para uma rede onde muitos scanners são geridos, tais como um grande escritório ou escola.

### Atribuição automática por função DHCP:

O endereço IP correto é atribuído automaticamente quando a comunicação entre o scanner e um router que suporte a função DHCP bem-sucedida.

Se for inconveniente alterar o endereço IP para um determinado dispositivo, reserve previamente o endereço IP e em seguida, atribua-o.

# Servidor DNS e servidor Proxy

Se usa um serviço de ligação à Internet, configure o servidor DNS. Se não o configurar, é necessário especificar o endereço IP de acesso porque pode falhar a resolução de nome.

O servidor proxy é colocado no gateway entre a rede e a Internet, e comunica com o computador, scanner e Internet (servidor oposto), em nome de cada um deles. O servidor oposto comunica apenas com o servidor de proxy. Assim, as informações do scanner, tais como o endereço IP e o número da porta não podem ser lidas e é esperado um aumento de segurança.

É possível proibir o acesso a um URL específico, utilizando a função de filtragem, uma vez que o servidor proxy é capaz de verificar o conteúdo da comunicação.

# Método de definição de ligação de rede

Para configurações de ligação do endereço IP do scanner, máscara de sub-rede e gateway predefinido, proceda da seguinte forma.

### Utilizar o Painel de Controlo:

Configurar as definições usando o painel de controlo do scanner de cada scanner. Ligar à rede depois de configurar as configurações de ligação do scanner.

### Utilizar o instalador:

Se usar o instalador, a rede do scanner e o computador cliente são definidos automaticamente. A configuração está disponível seguindo as instruções do instalador, mesmo se não tiver um conhecimento profundo da rede.

### Usar um recurso:

Usar um recurso do computador do administrador. É possível localizar um scanner e, a seguir, definir o scanner, ou criar um ficheiro SYLK para fazer as configurações em lote para scanners. É possível configurar vários scanners, mas é necessário que estejam ligadas fisicamente pelo cabo Ethernet antes da configuração. Portanto, é recomendado caso consiga construir uma rede Ethernet para a configuração.

### Informações relacionadas

➡ “Ligar à rede a partir do painel de controlo” na página 15

➡ “Ligar à rede usando o instalador” na página 19

➡ “Atribua um endereço IP usando EpsonNet Config” na página 56

# Ligação

Este capítulo explica o ambiente ou o procedimento para ligar o scanner à rede.

## Ligar à rede

### Ligar à rede a partir do painel de controlo

Ligar o scanner à rede usando o painel de controlo do scanner.

Para o painel de controlo do scanner, consulte o *Guia do Utilizador* para obter mais informações.

#### Atribuir o endereço IP

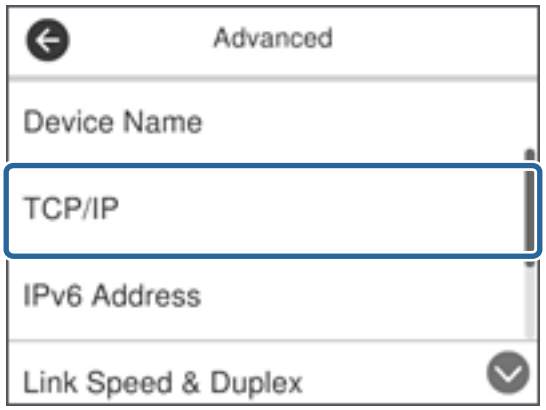
Definir itens básicos tais como Ender IP, Másc sub-rede, e Gateway predef..

1. Ligue o scanner.
2. Deslize o ecrã para a esquerda num movimento rápido no painel de controlo do scanner, e a seguir toque em **Definições**.

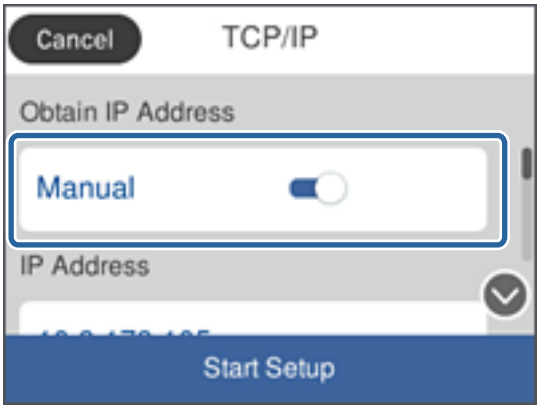

3. Toque em **Definições de rede** > **Alterar definições**.

   Se o item não for exibido, deslize o ecrã para cima num movimento rápido para cima.

4. Toque em **TCP/IP**.

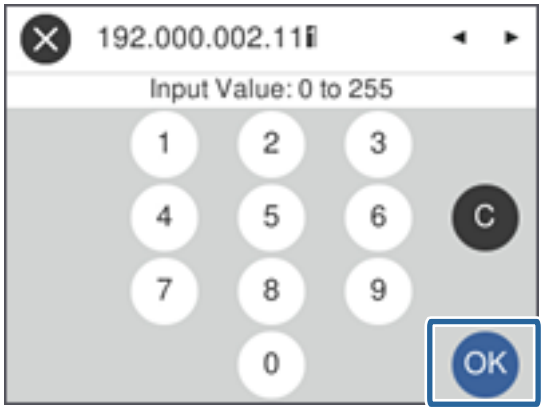



5. Seleccione **Manual** para **Obter ender IP**.




***Nota:***
*Ao definir o endereço IP automaticamente usando a função DHCP do router, selecione* ***Auto****. Nesse caso, o* ***Ender IP****,* ***Másc sub-rede****, e* ***Gateway predef.*** *no passo 6 a 7 também são definidos automaticamente, avance para o passo 8.*

6. Toque no campo **Ender IP**, introduza o endereço IP usando o teclado exibido no ecrã, e a seguir toque em **OK**.




Confirmar o valor refletido no ecrã anterior.

7. Configure a **Másc sub-rede** e **Gateway predef.**.

   Confirmar o valor refletido no ecrã anterior.

   ***Nota:***
   *Se a combinação do Ender IP, Másc sub-rede e Gateway predef. estiver errada, o **Iniciar Configuração** fica inativo e não pode continuar com as definições. Confirme que não existe erro na entrada.*

8. Toque no campo **DNS principal** do **Servidor DNS**, introduza o endereço IP do servidor primário DNS usando o teclado exibido no ecrã, e a seguir toque em **OK**.

   Confirmar o valor refletido no ecrã anterior.

   ***Nota:***
   *Ao selecionar **Auto** para as definições de atribuição de endereço IP, pode selecionar as definições de servidor DNS no **Manual** ou **Auto**. Se não conseguir obter o endereço de servidor DNS automaticamente, selecione **Manual** e introduza o endereço de servidor DNS. A seguir, introduza o endereço de servidor DNS diretamente. Se selecionar **Auto**, avance para o passo 10.*

9. Toque no campo **DNS secundário**, introduza o endereço IP para o servidor DNS secundário usando o teclado exibido no ecrã, e a seguir toque em **OK**.

   Confirmar o valor refletido no ecrã anterior.

10. Toque em **Iniciar Configuração**.

11. Toque em **Fechar** no ecrã de confirmação.

    O ecrã desliga-se automaticamente após um período de tempo específico se não tocar em **Fechar**.

## Ligação Ethernet

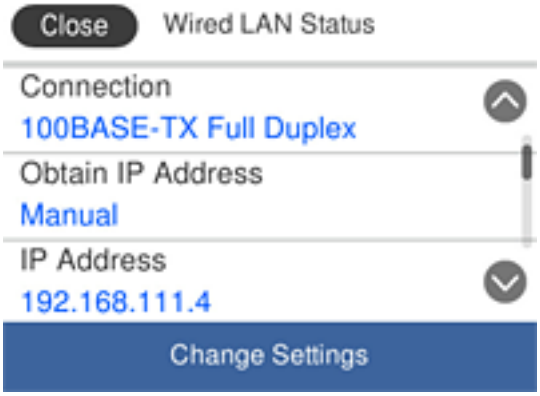
Ligar o scanner à rede usando o cabo Ethernet e verifique a ligação.

1. Ligue o scanner e o concentrador (interruptor L2) com o cabo Ethernet.

   O ícone no ecrã inicial muda para  .

2. Toque em  no ecrã inicial.

3. Volte a janela para cima e verifique se o estado de ligação e o endereço IP estão corretos.



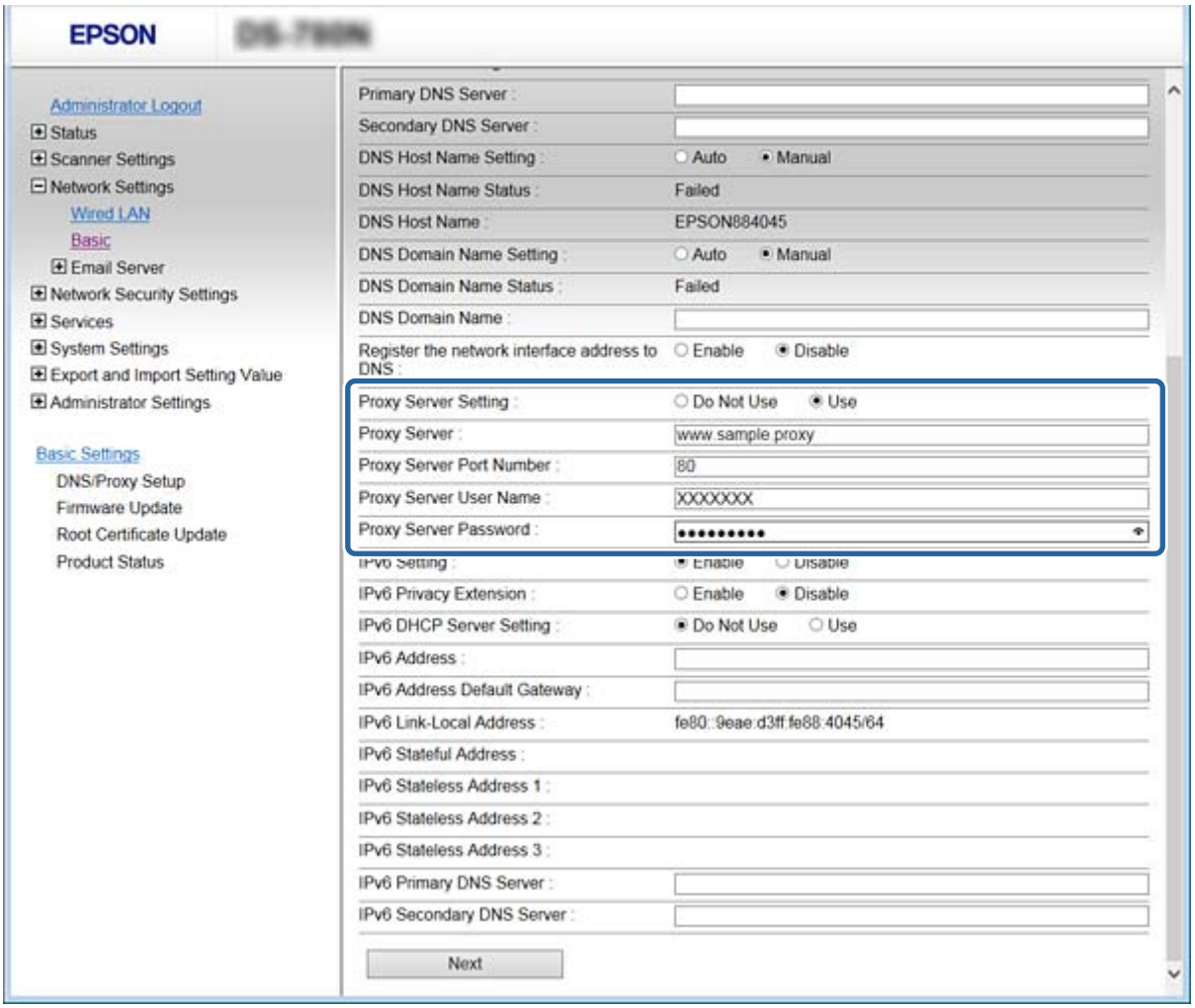

## Configurar o servidor Proxy

O servidor proxy não pode ser definido no painel. Configurar usando Web Config.

1. Aceder a Web Config e selecione **Definições de rede** > **Básico**.
2. Selecione **Utilizar** em **Configuração do Servidor proxy**.
3. Especifique o servidor proxy no endereço IPv4 ou formato FQDN em **Servidor proxy**, e a seguir introduza o número de porta em **Número da porta do servidor proxy**.

   Para servidores de proxy que exigem autenticação, digite o nome de utilizador de autenticação de servidor Proxy e a palavra-passe de autenticação do servidor Proxy.

4. Clique no botão **Seguinte**.




5. Confirme as definições e a seguir clique em **Definições**.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

## Ligar à rede usando o instalador

Recomendamos usar o instalador para ligar o scanner a um computador. Pode executar o instalador através dos seguintes métodos.

❏ Definir a partir do sítio Web

Aceder ao seguinte sítio Web e digitar o nome do produto. Aceda a **Configuração**, e comece a realizar a configuração.

http://epson.sn

❏ Realizar a configuração usando o disco de software (apenas nos modelos que vêm com um disco de software e utilizadores com computadores com unidade de disco.)

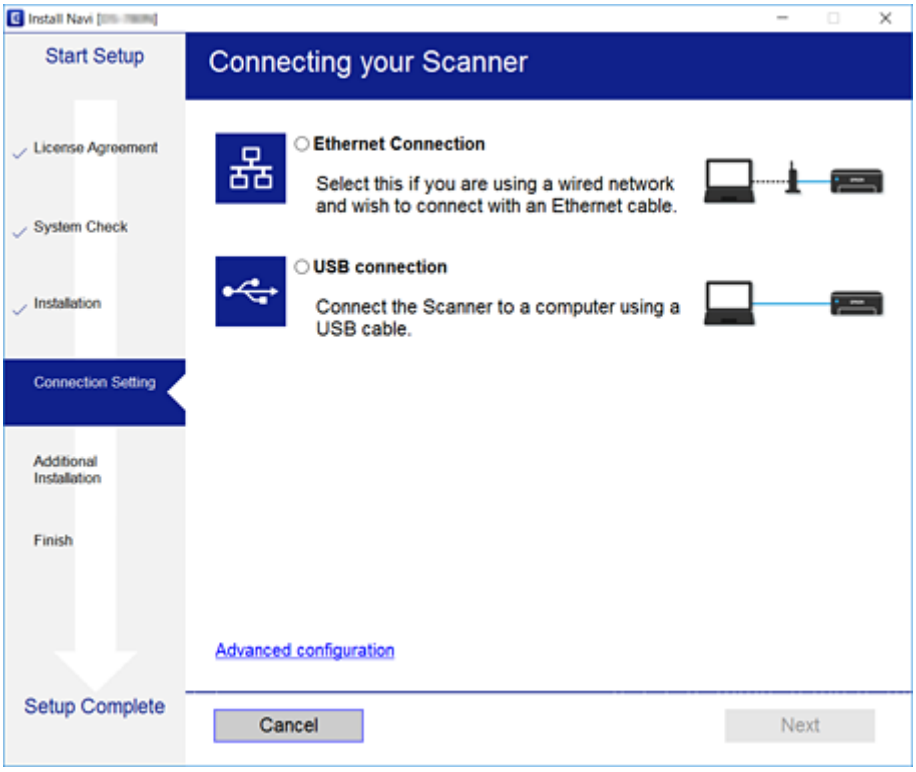
Inserir o disco de software no computador e siga as instruções apresentadas no ecrã.

## Selecionar os métodos de ligação

Siga as instruções apresentadas no ecrã até que a janela seguinte seja exibida e a seguir, selecione o método de ligação do scanner ao computador.

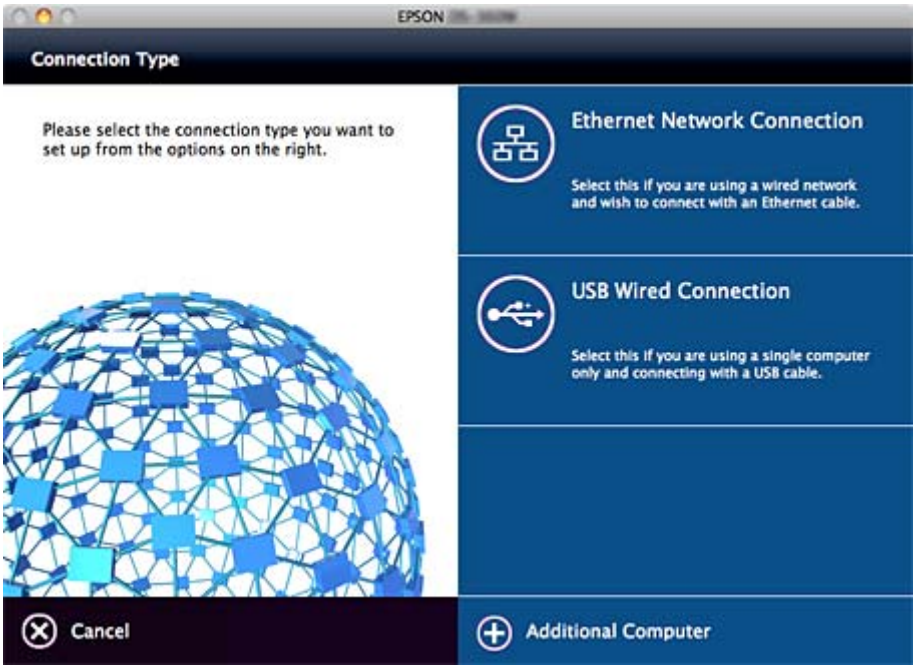
❏ Windows

Selecione o tipo de ligação e a seguir clique em **Seguinte**.




❏ Mac OS

Selecione o tipo de ligação.



**Ligação**

Siga as instruções apresentadas no ecrã. O software necessário está instalado.

# Definições de função

Este capítulo explica as primeiras configurações a realizar para utilizar cada função do dispositivo.

## Software para configuração

Neste tópico explicamos o procedimento para configurar definições a partir do computador do administrador usando o Web Config.

### Web Config (página Web para dispositivo)

#### Sobre a Web Config

O Web Config é uma aplicação que tem por base um browser para configurar as definições do scanner.

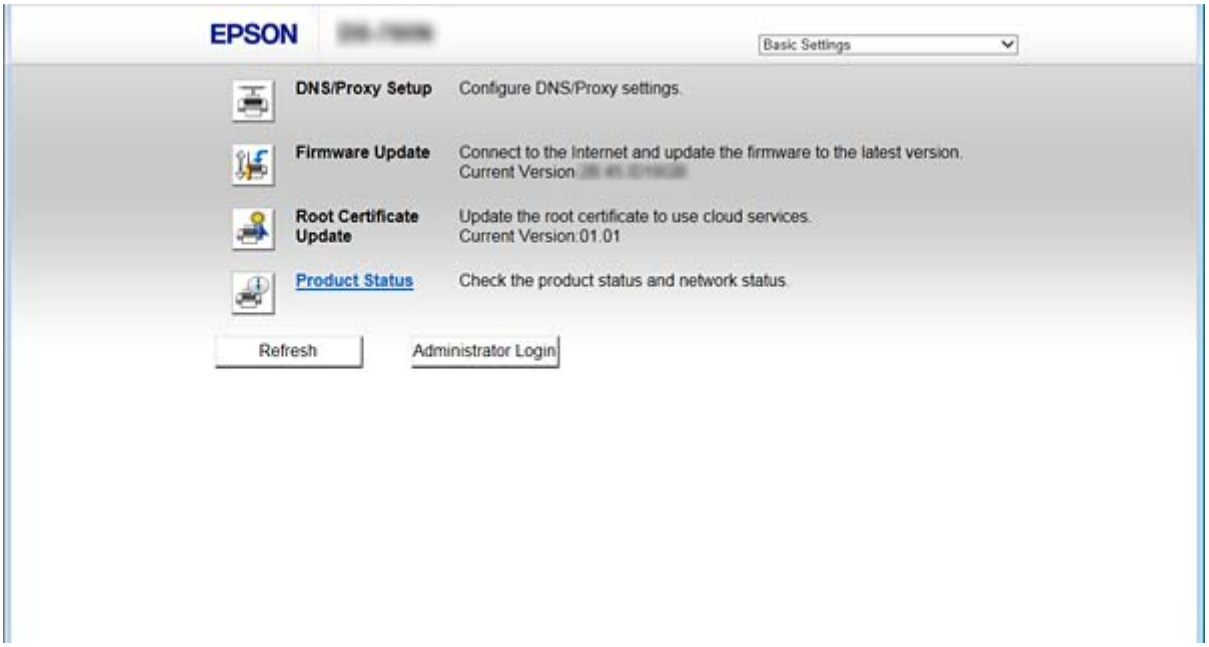
Para aceder ao Web Config, é necessário atribuir primeiro um endereço IP ao scanner.

***Nota:***
*Pode bloquear definições se configurar a palavra-passe do administrador no scanner.*

Existem duas páginas de configuração como se indica.

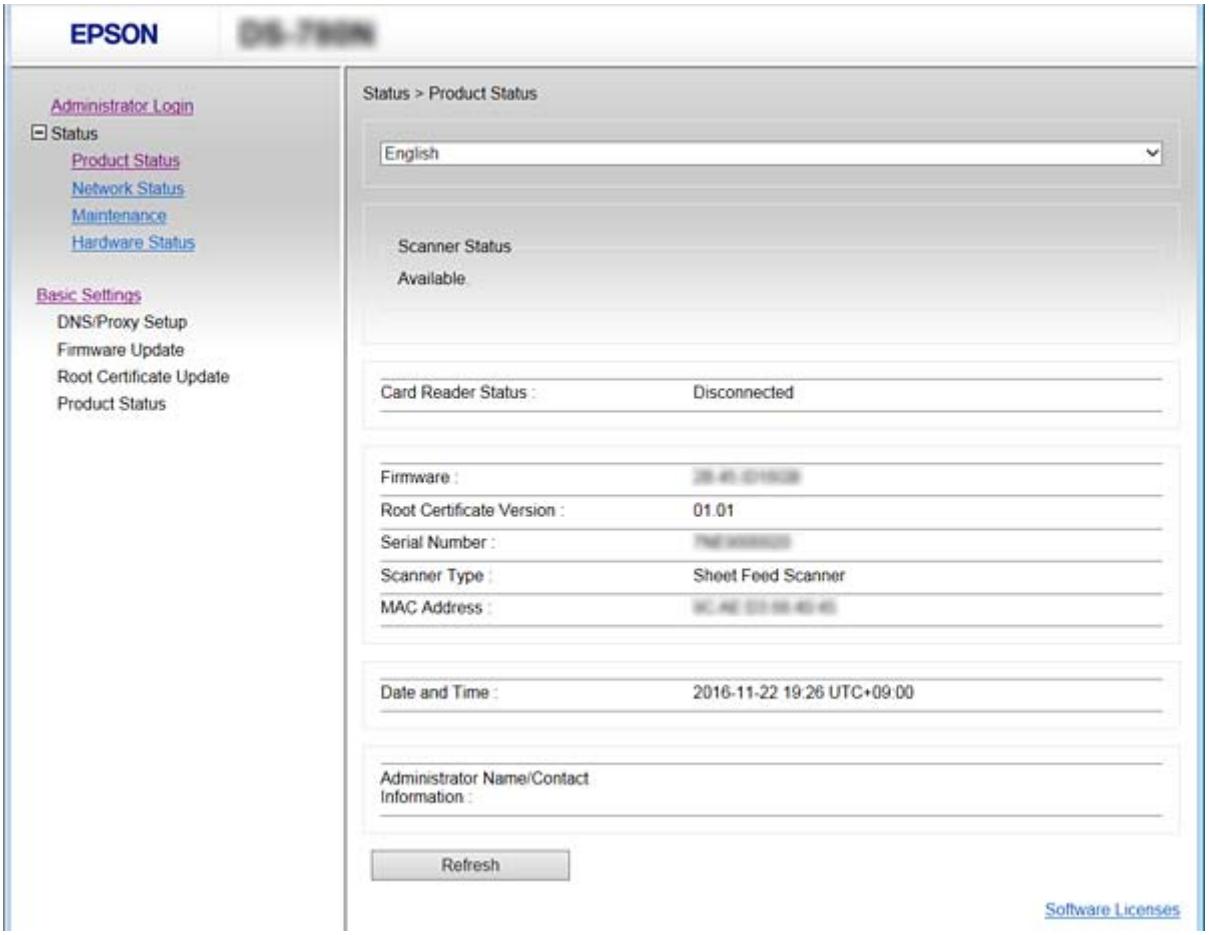
❏ **Definições básicas**

Pode configurar as definições básicas do scanner.



❏ **Definições avançadas**

Pode configurar as definições avançadas do scanner. Esta página destina-se sobretudo a um administrador.




## Aceder ao Web Config

Introduza o endereço IP do scanner num navegador Web. É necessário que o JavaScript esteja ativado. Ao aceder ao Web Config através de HTTPS, será exibida uma mensagem de aviso no navegador uma vez que é utilizado um certificado assinado automaticamente, armazenado no scanner.

❏ Acesso via HTTPS

IPv4: https://<endereço IP do scanner> (sem < >)

IPv6: https://[endereço IP do scanner]/ (com [ ])

❏ Acesso via HTTP

IPv4: http://<endereço IP do scanner> (sem < >)

IPv6: http://[endereço IP do scanner]/ (com [ ])

***Nota:***

❏ *Exemplos*

*IPv4:*

*https://192.0.2.111/*

*http://192.0.2.111/*

*IPv6:*

*https://[2001:db8::1000:1]/*

*http://[2001:db8::1000:1]/*

❏ *Se o nome do scanner for registado com o servidor DNS, pode utilizar o nome do scanner em vez do endereço IP do mesmo.*

### Informações relacionadas

➡ "Comunicações SSL/TLS com o scanner" na página 63

➡ "Informações sobre certificação digital" na página 63

# Usar as funções de digitalização

De acordo com a utilização que faz do scanner, instale o software que se segue e configure usando o mesmo.

❏ **Digitalizar para o computador**

❏ Confirmar a validade do serviço de digitalização de rede com Web Config (válido no envio de fábrica).

❏ Instale o Epson Scan 2 no computador e defina o endereço IP

❏ Ao digitalizar usando tarefas, instale o Document Capture Pro (Document Capture) e configure as definições da tarefa.

❏ **Digitalizar a partir do painel de funcionamento**

❏ Ao usar Document Capture Pro ou Document Capture Pro Server:

Instale o Document Capture Pro ou Document Capture Pro Server

Configuração DCP (modo servidor, modo cliente).

❏ Ao usar o protocolo WSD:

Confirmar a validade do WSD em Web Config ou painel de funcionamento (válido no envio de fábrica)

Configuração de dispositivo adicional (computador Windows).

## Digitalizar a partir de um computador

Instalar o software e verificar que o serviço de digitalização de rede está ativado para digitalizar através de uma rede a partir do computador.

### Informações relacionadas

➡ "Software a ser instalado" na página 25

➡ "Ativar a digitalização de rede" na página 25

## Software a ser instalado

❏ Epson Scan 2

Trata-se de um controlador de scanner. Se usar o dispositivo a partir de um computador, instale o controlador em cada computador cliente. Se Document Capture Pro/Document Capture estiver instalado, pode realizar as operações atribuídas aos botões do dispositivo.

Com o EpsonNet SetupManager, os controladores da impressora podem ser distribuídos juntamente em conjuntos.

❏ Document Capture Pro (Windows)/Document Capture (Mac OS)

Instalar no computador cliente. Pode aceder e executar tarefas registadas num computador com o Document Capture Pro/Document Capture instalado na rede a partir do painel de funcionamento do computador e do scanner.

Também pode digitalizar a partir do computador através da rede. Epson Scan 2 é necessário para digitalizar.

### Informações relacionadas

➡ "EpsonNet SetupManager" na página 56

## Definir o endereço IP do scanner em Epson Scan 2

Especificar o endereço IP do scanner para que o scanner possa ser utilizado na rede.

1. Inicie **Epson Scan 2 Utility** em **Início** > **Todos os programas** > **EPSON** > **Epson Scan 2**.

   Se já estiver registado outro scanner, avance para o passo 2.

   Se não estiver registado, avance para o passo 4.

2. Clique em ▼ em **Digitalizador**.

3. Clique em **Definições**.

4. Clique em **Activar Edição**, e a seguir clique em **Adicionar**.

5. Selecione o nome do modelo do scanner em **Modelo**.

6. Selecione o endereço IP do scanner que será utilizado em **Endereço** em **Procurar Rede**.

   Clique em  e cliqie em  para atualizar a lista. Se não conseguir encontrar o endereço IP do scanner, selecione **Inserir endereço** e introduza o endereço IP.

7. Clique em **Adicionar**.

8. Clique em **OK**.

## Ativar a digitalização de rede

É possível configurar o serviço de digitalização de rede ao realizar uma digitalização a partir de um computador cliente através da rede. A definição predefinida é ativada.

1. Aceda à configuração Web e selecione **Serviços** > **Pesquisa de rede**.

2. Certifique-se que seleciona **Activar digitalização** em **EPSON Scan**.

   Se estiver selecionado, a tarefa está terminada. Fechar o Web Config.

   Se estiver desmarcada, selecione e avance para o passo seguinte.

3. Clique em **Seguinte**.

4. Clique em **OK**.

   A rede é selecionada novamente, e a seguir as definições estão ativadas.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

# Digitalizar com o painel de controlo

A função digitalização para a pasta e a digitalização para a função de correio usando o painel de controlo do scanner, bem como a transferência de resultados de digitalização para o correio, pastas, etc., são realizadas pela execução de um trabalho a partir do computador.

Ao transferir resultados de digitalização, configure a tarefa com o Document Capture Pro Server ou Document Capture Pro.

Para mais informações sobre as definições e configurar uma tarefa, consulte os documentos ou a ajuda para Document Capture Pro Server ou Document Capture Pro.

### Informações relacionadas

➡ "Definições Document Capture Pro Server/Document Capture Pro" na página 26

➡ "Configuração de servidores e pastas" na página 27

## Software para instalar no computador

❏ **Document Capture Pro Server**

Esta é a versão servidor do Document Capture Pro. Instalar num servidor Windows. Diversos dispositivos e tarefas podem ser geridos centralmente pelo servidor. As tarefas podem ser executadas simultaneamente a partir de diversos scanners.

Ao usar a versão certificada do Document Capture Pro Server, é possível gerir tarefas e histórico de digitalizações ligados a utilizadores e grupos.

Para obter mais informações relativas ao Document Capture Pro Server, contacte o agente Epson local.

❏ **Document Capture Pro (Windows)/Document Capture (Mac OS)**

Assim como a digitalização a partir de um computador, é possível aceder a tarefas no computador a partir do painel de controle e executá-los. Não é possível executar tarefas do computador simultaneamente a partir de vários scanners.

## Definições Document Capture Pro Server/Document Capture Pro

Configurações para usar a função de digitalização a partir do painel de funcionamento do scanner.

1. Aceder a Web Config e selecione **Serviços** > **Document Capture Pro**.

2. Selecione **Modo Funcionam.**.

   ❏ Modo de servidor:

   Selecionar ao usar Document Capture Pro Server ou ao usar Document Capture Pro apenas para tarefas definidas para um computador específico.

   ❏ Modo de cliente:

   Definir ao selecionar as definições da tarefa de Document Capture Pro (Document Capture) instalado em cada computador de cliente na rede sem especificar o computador.

3. Definir de acordo com o modo selecionado.

   ❏ Modo de servidor:

   Em **Endereço do servidor**, especificar o servidor onde o Document Capture Pro Server está instalado. Pode ter entre 2 a 252 caracteres no formato IPv4, IPv6, nome do anfitrião, formato FQDN. No formato FQDN, podem ser usadas letras US-ASCII, números, alfabetos, e hifenes (exceto início e final).

   ❏ Modo de cliente:

   Especificar **Definições de grupo** para usar um grupo de scanner específico a partir de Document Capture Pro (Document Capture).

4. Clique em **Definições**.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

## Configuração de servidores e pastas

Document Capture Pro e Document Capture Pro Server guardam as informações digitalizadas no servidor ou computador do cliente e usam a função de transferência para executar a digitalização para a função de pasta e digitalizar para a função de correio.

É necessária a autoridade e informação para transferir a partir do computador onde Document Capture Pro, Document Capture Pro Server está instalado para o computador ou serviço nuvem.

Prepara as informações sobre a função que será utilizada, relativamente ao seguinte.

É possível realizar definições para estas funções usando Document Capture Pro ou Document Capture Pro Server. Para mais informações sobre as definições, consulte os documentos ou a ajuda para Document Capture Pro Server ou Document Capture Pro.

| Nome | Definições | Requisito |
|---|---|---|
| Digitalizar para a pasta de rede (SMB) | Criar e configurar a partilha da pasta guardar | A conta de utilizador administrativa para o computador que cria pastas guardar. |
| | Destino para digitalizar para pasta de rede (SMB) | Nome de utilizador e palavra-passe para iniciar sessão no computador onde se encontra a pasta guardar e o privilégio para atualizar a pasta guardar. |
| Digitalizar para a pasta de rede (FTP) | Configuração para iniciar sessão no servidor FTP | Informações de início de sessão para o servidor FTP e privilégio para atualizar a pasta guardar. |

| Nome | Definições | Requisito |
|---|---|---|
| Digitalizar para e-mail | Configurar para servidor e-mail | Informações de configuração para servidor e-mail |
| Digitalizar para Document Capture Pro (ao usar Document Capture Pro Server) | Configuração para iniciar sessão nos serviços nuvem | Ambiente de ligação à Internet<br>Registo da conta para serviços nuvem |

### Utilize a digitalização WSD (apenas Windows)

Se o computador usar Windows Vista ou posterior, poe usar a digitalização WSD.

Quando for possível usar o protocolo WSD, o menu **Computador (WSD)** será exibido no painel de controlo do scanner.

1. Aceder a Web Config e selecione **Serviços** > **Protocolo**.
2. Confirmar que o **Activar WSD** está selecionado em **Definições de WSD**.

   Se estiver selecionado, a sua tarefa será terminada e pode encerrar o Web Config.

   Se não estiver selecionado, selecione e avance para o passo seguinte.
3. Clique no botão **Seguinte**.
4. Confirme as definições e clique em **Definições**.

# Configuração do sistema

## Fazer configurações do sistema no Painel de Controlo

### Definir o brilho do ecrã

Definir o brilho do ecrã LCD.

1. Toque em **Definições** no ecrã de início.
2. Toque em **Definições comuns** > **Brilho do LCD**.
3. Toque em  ou  para ajustar o brilho.

   É possível ajustar de 1 a 9.
4. Toque em **OK**.

### Definir som

Definir o som do funcionamento do painel e som de erro.

1. Toque em **Definições** no ecrã de início.
2. Toque em **Definições comuns** > **Som**.
3. Defina os seguintes itens como necessário.
   - ❏ Som de funcionamento
     Defina o volume do som de funcionamento do painel de funcionamento.
   - ❏ Som de erro
     Defina o volume do som do erro.
4. Toque em **OK**.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

## Deteção de alimentação dupla de original

Determine a função de deteção de alimentação DUPLA do documento a ser digitalizado e para interromper a digitalização quando ocorrerem diversas alimentações.

Para digitalizar originais que são considerados alimentação múltipla, tais como envelopes ou papel com autocolantes, defina como desligado.

***Nota:***
*Também pode definir em Web Config ou Epson Scan 2.*

1. Toque em **Definições** no ecrã de início.
2. Toque em **Definições de Digitalização externas** > **Detec. aliment. dupla ultra-sónica**.
3. Toque em **Detec. aliment. dupla ultra-sónica** para ligar e desligar.
4. Toque em **Fechar**.

## Definir o modo de velocidade baixa

Definir para digitalizar a baixa velocidade, para evitar obstruções de papel durante a digitalização de documentos finos tais como deslizamentos.

1. Toque em **Definições** no ecrã de início.
2. Toque em **Definições de Digitalização externas** > **Lenta**.
3. Toque em **Lenta** para ligar e desligar.
4. Toque em **Fechar**.

# Fazer definições de sistema usando o Web Config

## Configurar a poupança de energia durante a inatividade

Faça a configuração de poupança de energia para o período de inatividade do scanner. Defina o tempo, dependendo do ambiente de utilização.

***Nota:***
*Pode também efetuar as definições de poupança de energia através do painel de controlo do scanner.*

1. Aceder a Web Config e selecione **Definições do sistema** > **Poupança de energia**.
2. Introduza a hora de **Temporizador** para mudar para o modo de poupança de energia em tempo de inatividade.

   É possível definir até 240 minutos um minuto de cada vez.
3. Selecione a hora para desligar para a **Temporizador para desligar**.
4. Clique em **OK**.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

## Configurar o painel de controlo

Configuração do painel de controlo do scanner. Pode fazer a seguinte configuração.

1. Aceder a Web Config e selecione **Definições do sistema** > **Painel de controlo**.
2. Defina os seguintes itens como necessário.
   - ❏ Língua

     Selecione o idioma exibido no painel de controlo.
   - ❏ Bloqueio do painel

     Se selecionar **ACT**, a palavra-passe de administrador é necessária ao realizar uma operação que exige a autoridade do administrador. Se a palavra-passe do administrador não for definida, é exibido o painel de bloqueio.
   - ❏ Tempo limite de operação

     Se selecionar **ACT**, quando iniciar sessão como administrador, termina sessão automaticamente e é reencaminhado para o ecrã inicial se não houver atividade durante um determinado período de tempo.

     Pode definir entre 10 segundos e 240 minutos ao segundo.
3. Clique em **OK**.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

## Configurar a restrição para a interface externa

Pode restringir a ligação USB a partir do computador. Configurar para limitar outra digitalização que não através da rede.

1. Aceder a Web Config e selecione **Definições do sistema** > **Interface externo**.
2. Selecione **Activar** ou **Desactivar**.

   Para restringir, selecione **Desactivar**.
3. Toque em **OK**.

## Sincronização dos dados e hora com o servidor de horário

Se usar um certificado CA, pode evitar problemas com a hora.

1. Aceda a Web Config e selecione **Definições do sistema** > **Data e Hora** > **Servidor de horas**.
2. Seleccione **Utilizar** para **Utilizar servidor de horas**.
3. Introduza a hora de endereço do servidor para **Endereço do servidor de horas**.

   Pode usar formato IPv4, IPv6 ou FQDN. Introduza 252 caracteres ou menos. Se não especificar, deixe em branco.
4. Introduza **Intervalo de actualização (min)**.

   É possível definir até 10.800 minutos um minuto de cada vez.
5. Clique em **OK**.

   ***Nota:***
   *Pode confirmar o estado da ligação com servidor de horário em **Estado do servidor de horas**.*

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

# Definições básicas de segurança

Este capítulo explica as definições básicas de segurança que não requerem um ambiente especial.

## Introdução de recursos de segurança básicos

Recursos básicos de segurança dos dispositivos Epson.

| Nome da funcionalidade | Tipo de funcionalidade | O que definir | O que evitar |
|---|---|---|---|
| Configuração da palavra-passe de administrador | Bloqueie as definições relacionadas com o sistema, tais como rede e definições de ligação USB, para que não possam ser alteradas exceto pelo administrador. | O administrador define uma palavra-passe para o dispositivo.<br>As configurações ou atualizações estão disponíveis em qualquer lugar em Web Config, o painel de controlo, Epson Device Admin, e EpsonNet Config. | Impedir a leitura e alteração das informações armazenadas no dispositivo, tais como a identificação, palavra-passe, configurações de rede, e os contactos de forma ilegal. Além disso, reduza uma ampla gama de riscos de segurança, tais como fuga de informações para o ambiente de rede ou política de segurança. |
| Comunicações SSL/TLS | Ao aceder a um servidor Epson na Internet através de um dispositivo, por exemplo uma comunicação com um computador através do navegador ou atualização de firmware, o conteúdo da comunicação é encriptado por comunicação SSL/TLS. | Obter um certificado assinado CA e, em seguida, importe-o para o scanner. | Eliminar uma identificação do dispositivo pela certificação assinada CA impede o roubo de identidade e acesso não autorizado. Além disso, o conteúdo da comunicação de SSL/TLS são protegidos, e impede que a fuga de conteúdos para a impressão de informações de dados e configuração. |
| Protocolos de controlos | Protocolos de controlos usados para comunicar entre dispositivos e computadores, e ativa/desativa funções. | Um protocolo ou serviço aplicado a recursos permitidos ou proibidos separadamente. | Reduzindo os riscos de segurança que podem ocorrer com a utilização não intencional, impedindo que os utilizadores usem funções desnecessárias. |

### Informações relacionadas

➡ “Sobre a Web Config” na página 22
➡ “Configuração EpsonNet” na página 55
➡ “Epson Device Admin” na página 55
➡ “Configurar a palavra-passe do administrador” na página 33
➡ “Protocolos de controlo” na página 35

# Configurar a palavra-passe do administrador

Quando definir a palavra-passe de administrador, os utilizadores que não sejam administradores não serão capazes de alterar as configurações para a administração do sistema. É possível definir e alterar a palavra-passe de administrador usando quer Web Config, o painel de controlo do scanner, ou software (Epson Device Admin ou EpsonNet Config). Ao usar o software, consulte a documentação para cada software.

### Informações relacionadas

➡ "Configurar a palavra-passe de administrador no painel de controlo" na página 33

➡ "Configurar a palavra-passe de Administrador usando Web Config" na página 33

➡ "Configuração EpsonNet" na página 55

➡ "Epson Device Admin" na página 55

## Configurar a palavra-passe de administrador no painel de controlo

É possível definir a palavra-passe de administrador no painel de controlo do scanner.

1. Toque em **Definições** no ecrã de início.
2. Toque em **Administração do sistema** > **Definições de administ.**.

   Se o item não for exibido, deslize o ecrã para cima num movimento rápido para cima para exibir o item.
3. Toque em **Senha de administrador** > **Registar**.
4. Introduza a palavra-passe nova e selecione **OK**.
5. Introduza a palavra-passe novamente e selecione **OK**.
6. Toque em **OK** no ecrã de confirmação.

   O ecrã das definições de administrador é exibido.
7. Toque em **Config. de bloqueio**, e a seguir toque em **OK** no ecrã de confirmação.

   Config. de bloqueio está definido como **Ativ.**, e a palavra-passe do administrador será solicitada para utilizar o item do menu bloqueado.

***Nota:***

❏ *Se definir **Definições** > **Definições comuns** > **Tempo limite de operação** para **Ativ.**, o scanner terminará a sua sessão após um período de inatividade no painel de controlo.*

❏ *É possível alterar ou eliminar a palavra-passe de administrador ao selecionar **Alterar** ou **Repor** no ecrã **Senha de administrador** e introduzir a palavra-passe de administrador.*

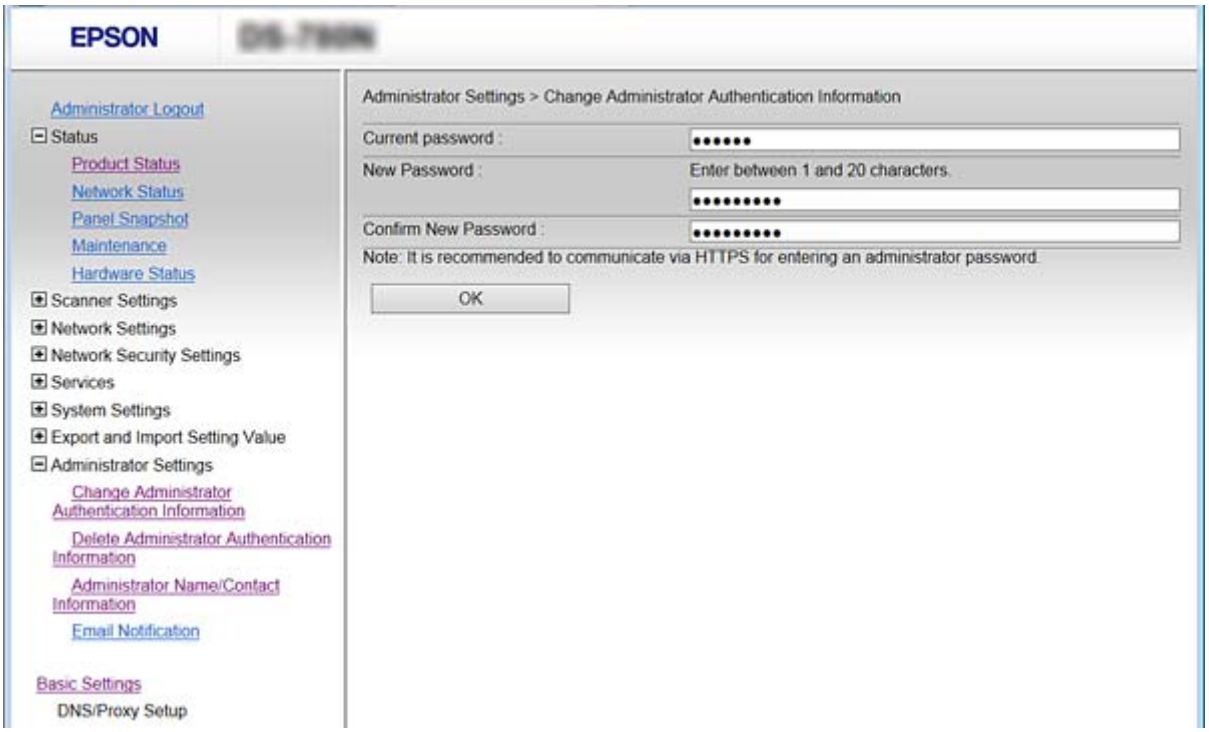
## Configurar a palavra-passe de Administrador usando Web Config

É possível definir a palavra-passe de Administrador usando Web Config.

1. Aceder a Web Config e selecione **Definições do administrador** > **Alterar informações de autenticação do administrador**.

2. Introduza uma palavra-passe para **Nova senha** e **Confirmar a nova senha**. Introduza o nome de utilizador, se necessário.

   Se deseja alterar a palavra-passe, digite a palavra-passe atual.




3. Selecione **OK**.

   ***Nota:***

   ❏ *Para definir ou alterar os itens de menu bloqueados, clique em* ***Início de sessão de administrador****, e a seguir introduza a palavra-passe de administrador.*

   ❏ *Para eliminar a palavra-passe de administrador, clique em* ***Definições do administrador*** *>* ***Eliminar informações de autenticação do administrador****, e a seguir introduza a palavra-passe do administrador.*

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

# Itens que são bloqueados pela palavra-passe de Administrador

Os administradores têm privilégios de configuração e alteração de todos os recursos dos dispositivos.

Se definir a palavra-passe de administrador no dispositivo, é possível bloquear para que não seja possível alterar itens relacionados com a gestão do dispositivo.

Seguem-se alguns dos itens que um administrador pode controlar.

| Item | Descrição |
|---|---|
| Configuração do scanner | Definição da deteção de alimentação duplicada e modo de velocidade baixa. |

**Definições básicas de segurança**

| Item | Descrição |
|---|---|
| Configuração de ligação Ethernet | Alterar o nome dos dispositivos e endereços IP, configuração do servidor DNS ou servidor proxy, e definição de alterações relacionadas com ligações de rede. |
| Configuração dos serviços de utilizador | Configuração para controlo de protocolos de comunicação, digitalização de rede, e serviços Document Capture Pro. |
| Definições do servidor de e-mail | Configurar um servidor de e-mail com o qual os dispositivos comunicam diretamente. |
| Configuração de segurança | Configuração da segurança de rede, como por exemplo comunicação SSL/TLS, filtro IPsec/IP e IEEE802.1X. |
| Atualização do certificado de raíz | Atualização de certificados de raíz necessários para autenticação Document Capture Pro Server e atualização de firmware a partir de Web Config. |
| Atualização do firmware | Verifique e atualize o firmware dos dispositivos. |
| Hora, configuração da hora | Hora de transição para modo de suspensão, desligar automático, data/hora, hora de inatividade, outras definições relacionadas com uma hora. |
| Repor as definições predefinidas | Configurar o scanner para a reposição da configuração de fábrica. |
| Configuração de administrador | Configurar o bloqueio de administrador ou palavra-passe de administrador. |
| Configuração do dispositivo certificado | Configuração da identificação do dispositivo de autenticação. Definir ao utilizar o scanner num sistema de autenticação compatível com sistemas de autenticação. |

# Protocolos de controlo

Pode digitalizar utilizando uma variedade de protocolos e caminhos. Também pode usar a digitalização de rede a partir de um número indeterminado de computadores em rede. Por exemplo, é permitido digitalizar usando apenas caminhos e protocolos específicos. Pode reduzir os riscos de segurança não previstos restringindo a digitalização a partir de caminhos específicos, ou controlando as funções disponíveis.

Configuração das definições de protocolos.

1. Aceder a Web Config e selecione **Serviços** > **Protocolo**.
2. Configure cada um dos itens.
3. Clique em **Seguinte**.
4. Clique em **OK**.

   As definições são aplicadas ao scanner.

### Informações relacionadas

➡ “Aceder ao Web Config” na página 23
➡ “Protocolos que pode Activar ou Desactivar” na página 36
➡ “Itens de definição de protocolos” na página 37

# Protocolos que pode Activar ou Desactivar

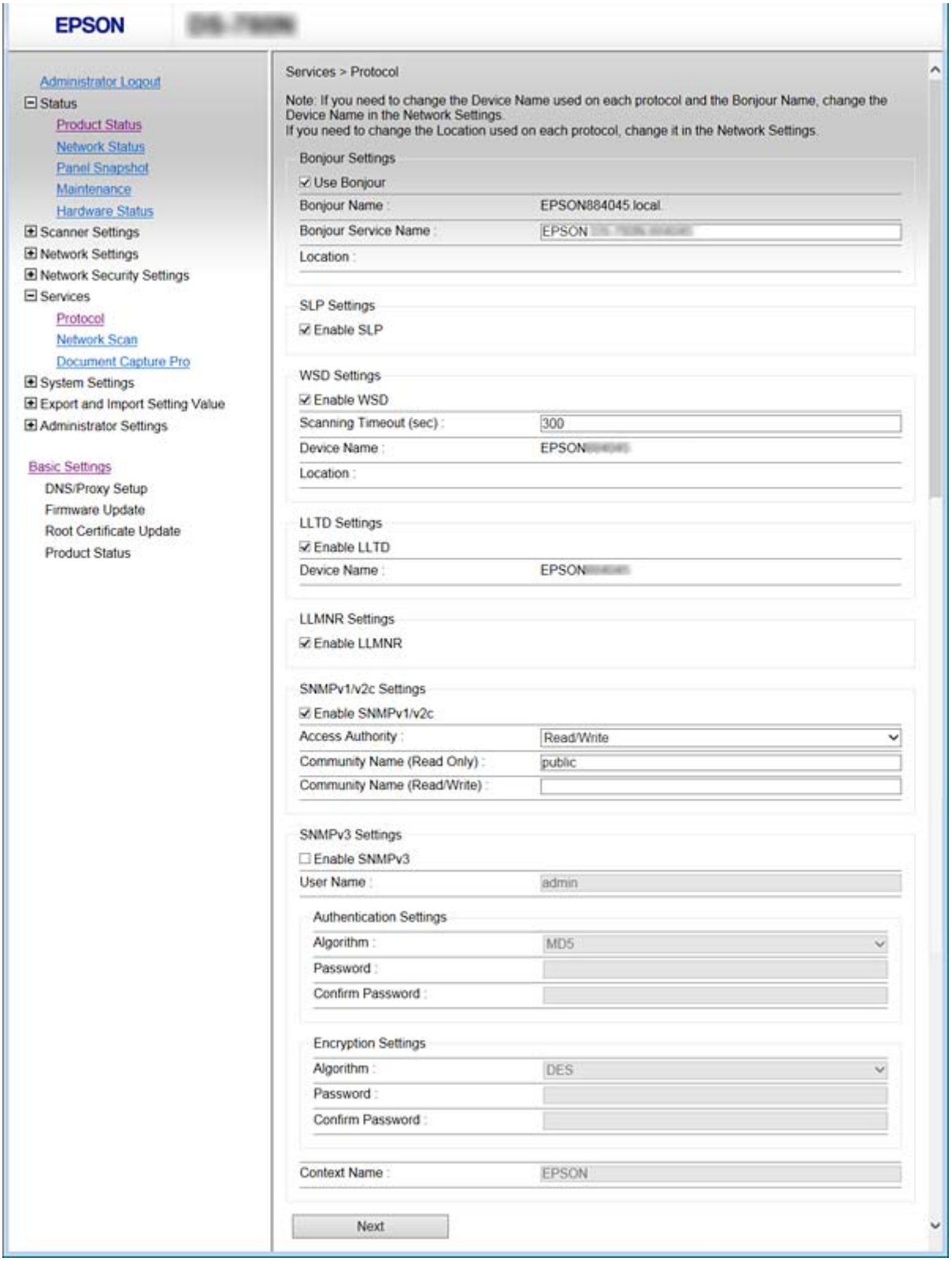
| Protocolo | Descrição |
|---|---|
| Definições Bonjour | Pode especificar se pretende usar o Bonjour. O Bonjour é usado para procurar dispositivos, digitalizar, etc. |
| Definições de SLP | Pode ativar ou desativar a função SLP. O SLP é usado para Epson Scan 2 e pesquisa de rede em EpsonNet Config. |
| Definições de WSD | Pode ativar ou desativar a função WSD. Quando ativada, pode adicionar dispositivos WSD ou digitalizar a partir da porta WSD. |
| Definições de LLTD | Pode activar ou desactivar a função LLTD. Quando activada, é apresentada no mapa de rede do Windows. |
| Definições de LLMNR | Pode activar ou desactivar a função LLMNR. Quando activada, pode usar a resolução de nome sem NetBIOS, mesmo que não possa usar DNS. |
| Definições de SNMPv1/v2c | Pode especificar se pretende ativar ou não ativar a função SNMPv1/v2c. Isto é usado para configurar dispositivos, monitorização, etc. |
| Definições de SNMPv3 | Pode especificar se pretende ativar ou não ativar a função SNMPv3. É usado para configurar dispositivos encriptados, monitorização, etc. |

### Informações relacionadas

➡ “Protocolos de controlo” na página 35

➡ “Itens de definição de protocolos” na página 37

# Itens de definição de protocolos




| Itens | Valor e descrição da definição |
|---|---|
| Definições Bonjour | |

## Definições básicas de segurança

| Itens | Valor e descrição da definição |
|---|---|
| Utilizar Bonjour | Selecione esta opção para procurar ou utilizar dispositivos por meio do Bonjour. |
| Nome Bonjour | Apresenta o nome do Bonjour. |
| Nome do Serviço Bonjour | É possível exibir e definir o nome do serviço Bonjour. |
| Localização | Apresenta o nome do localização do Bonjour. |
| Definições de SLP | |
| Activar SLP | Selecione esta opção para ativar a função SLP. Utilizado para encontrar a rede em Epson Scan 2 e EpsonNet Config. |
| Definições de WSD | |
| Activar WSD | Selecione esta opção para ativar a adição de dispositivos usando WSD e a impressão e digitalização a partir da porta WSD. |
| Tempo limite de digitalização (seg) | Introduza um valor de tempo limite de comunicação para a digitalização WSD, entre 3 e 3600 segundos. |
| Nome do dispositivo | Apresenta o nome do dispositivo WSD. |
| Localização | Apresenta o nome do localização do WSD. |
| Definições de LLTD | |
| Activar LLTD | Selecione esta opção para ativar LLTD. O scanner é apresentado no mapa de rede Windows. |
| Nome do dispositivo | Apresenta o nome do dispositivo LLTD. |
| Definições de LLMNR | |
| Activar LLMNR | Selecione esta opção para ativar LLMNR. Pode usar a resolução de nome sem NetBIOS, mesmo que não possa usar DNS. |
| Definições de SNMPv1/v2c | |
| Ativar SNMPv1/v2c | Selecione para ativar SNMPv1/v2c. Só são apresentados scanners impressoras que suportem SNMPv3. |
| Autoridade de acesso | Defina a autoridade de acesso quando o SNMPv1/v2c estiver ativado. Selecione **Só ler** ou **Ler/Escrever**. |
| Nome da comunidade (Apenas leitura) | Introduza entre 0 a 32 caracteres ASCII (0x20 a 0x7E). |
| Nome da comunidade (Escrita/leitura) | Introduza entre 0 a 32 caracteres ASCII (0x20 a 0x7E). |
| Definições de SNMPv3 | |
| Ativar SNMPv3 | SNMPv3 está ativado quando a caixa é selecionada. |
| Nome de Util. | Introduza entre 1 e 32 caracteres utilizando caracteres de 1 byte. |
| Definições de autenticação | |
| Algoritmo | Selecione um algoritmo para uma autenticação para SNMPv3. |

**Definições básicas de segurança**

| Itens | Valor e descrição da definição |
|---|---|
| Palavra-passe | Introduza a palavra-passe para uma autenticação SNMPv3.<br>Introduza entre 8 e 32 caracteres em ASCII (0x20–0x7E). Se não especificar, deixe em branco. |
| Confirmar palavra-passe | Introduza a palavra-passe que configurou para confirmação. |
| Definições de encriptação | |
| Algoritmo | Selecione um algoritmo para uma encriptação para SNMPv3. |
| Palavra-passe | Introduza a palavra-passe para uma encriptação SNMPv3.<br>Introduza entre 8 e 32 caracteres em ASCII (0x20–0x7E). Se não especificar, deixe em branco. |
| Confirmar palavra-passe | Introduza a palavra-passe que configurou para confirmação. |
| Nome do contexto | Introduza 32 caracteres ou menos em Unicode (UTF-8). Se não especificar, deixe em branco. O número de caracteres que podem ser inseridos varia dependendo do idioma. |

### Informações relacionadas

➡ "Protocolos de controlo" na página 35

➡ "Protocolos que pode Activar ou Desactivar" na página 36

# Configurações de funcionamento e gestão

Este capítulo explica os itens relacionados com as operações diárias e de gestão do dispositivo.

## Confirmar a informação de um dispositivo

Consegue verificar as informações que se seguem do dispositivo de funcionamento de **Estado** utilizando Web Config.

❏ Estado do produto

Verifique o idioma, estado, número de produto, endereço MAC, etc.

❏ Estado da rede

Verifique as informações do estado de ligação de rede, endereço IP, servidor DNS, etc.

❏ Instantâneo de painel

Exibe um instantâneo da imagem do ecrã que é exibido no painel de controlo do dispositivo.

❏ Manutenção

Verifique a data de início, informações de digitalização, etc.

❏ Estado do hardware

Verifique o estado do scanner.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

## Gerir dispositivos (Epson Device Admin)

Pode gerir e utilizar vários dispositivos usando Epson Device Admin. Epson Device Admin permite-lhe gerir dispositivos que se encontrem numa rede diferente. Segue-se uma descrição dos principais recursos de gestão.

Para mais informações sobre funções e a utilização do software, consulte a bibliografia ou a ajuda do recurso Epson Device Admin.

❏ Encontrar dispositivos

Pode encontrar dispositivos na rede e registá-los numa lista. Se os dispositivos Epson como impressoras e scanners estão ligados ao mesmo segmento de rede que o computador do administrador, pode encontrá-los, mesmo se não lhes tiver sido atribuído um endereço IP.

Também pode encontrar dispositivos que estão ligados a computadores na rede através de cabos USB. É necessário instalar o Epson Device USB Agent no computador.

❏ Configurar os dispositivos

Pode criar um modelo com os itens de configuração como a interface de rede e a fonte de papel e aplicá-lo a outros dispositivos como configurações partilhadas. Quando estiver ligado à rede, pode atribuir um endereço IP a um dispositivo ao qual não tenha sido atribuído um endereço IP.

❏ Dispositivos de monitorização

Pode adquirir regularmente o estado e informações detalhadas para dispositivos na rede. Também pode monitorizar dispositivos que estão ligados a computadores na rede por cabos USB e dispositivos de outras empresas que foram registados na lista de dispositivos. Para monitorizar dispositivos ligados por cabos USB, é necessário instalar o recurso Epson Device USB Agent.

❏ Gestão de alertas

Pode monitorizar alertas sobre o estado de dispositivos e consumíveis. O sistema envia automaticamente e-mails de notificação ao administrador com base nas condições definidas.

❏ Gestão de relatórios

Pode criar relatórios regulares à medida que o sistema acumula dados sobre a utilização do dispositivo e consumíveis. A seguir pode salvar estes relatórios criados e enviá-los por e-mail.

**Informações relacionadas**

➡ "Epson Device Admin" na página 55

# Receber Notificações por E-mail Quando Ocorrem Eventos

## Sobre as notificações de e-mail

Pode usar este recurso para receber alertas por e-mail quando ocorrem eventos. Pode registar até 5 endereços de e-mail e escolher sobre quais eventos deseja receber notificações.

O servidor de email deve ser configurado para usar esta função.

**Informações relacionadas**

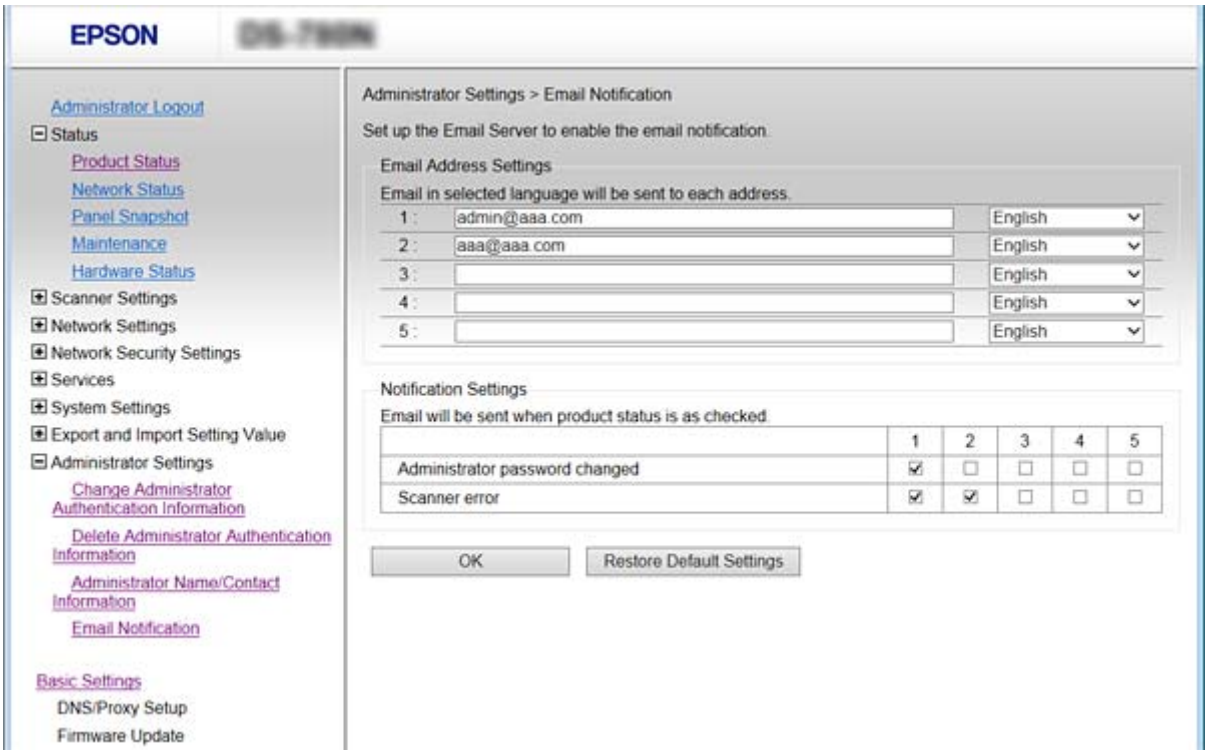
➡ "Configurar um servidor de correio" na página 42

## Configurar a notificação por e-mail

Para utilizar a funcionalidade, terá de configurar um servidor de correio.

1. Selecionar Web Config e **Definições do administrador** > **Notificação por e-mail**.
2. Introduza o endereço de e-mail onde deseja receber as notificações por e-mail.
3. Selecione o idioma para das notificações de e-mail.

4. Marque as caixas para as notificações que deseja receber.




5. Clique em **OK**.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23
➡ "Configurar um servidor de correio" na página 42

## Configurar um servidor de correio

Verifique o seguinte antes de configurar.

❏ O scanner está ligado a uma rede.

❏ As informações do servidor de correio eletrónico do computador.

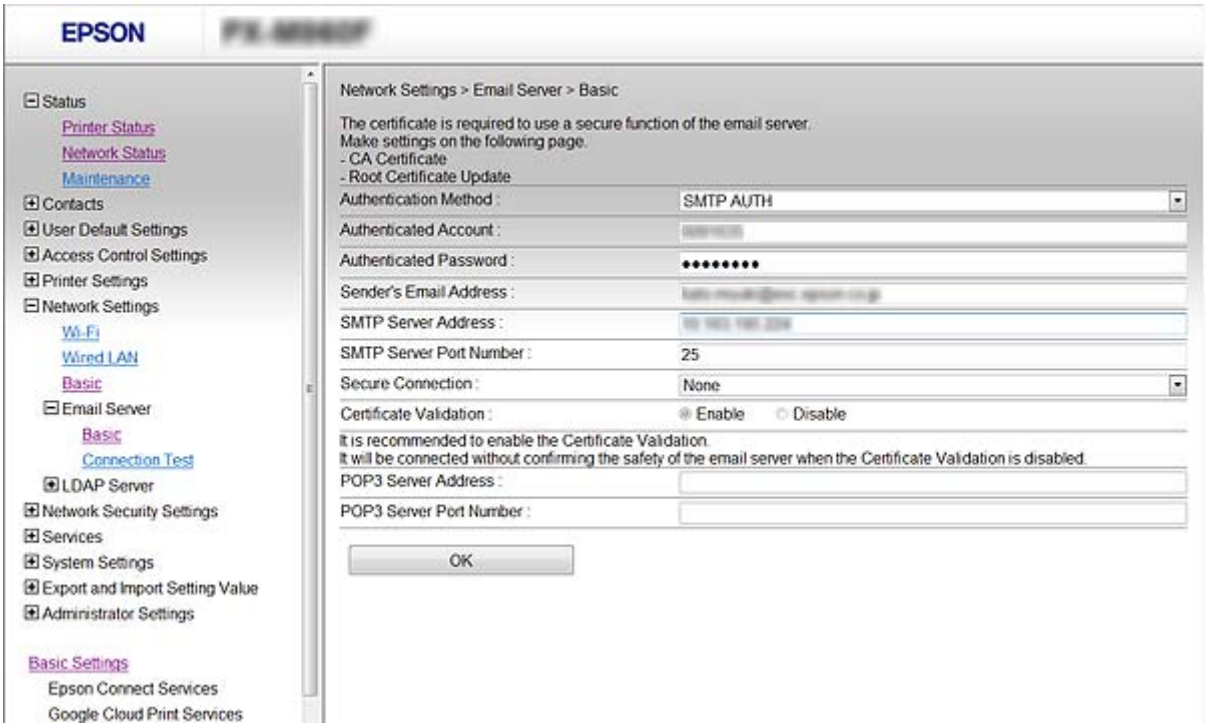
1. Selecionar Web Config e **Definições de rede** > **Servidor de e-mail** > **Básico**.
2. Introduza um valor para cada item.
3. Selecione **OK**.

   São apresentadas as definições que seleccionou.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23
➡ "Itens de definição do servidor de correio" na página 43

# Itens de definição do servidor de correio




| Itens | Definições e explicação | |
|---|---|---|
| Método de autenticação | Especifique o método de autenticação para que o scanner aceda ao servidor de correio. | |
| | Desactivar | A autenticação é desativada ao comunicar com um servidor de e-mail. |
| | Autentic. SMTP | Requer que um servidor de correio suporte autenticação SMTP. |
| | POP antes de SMTP | Configure o servidor POP3 quando selecionar este método. |
| Conta autenticada | Se selecionar **Autentic. SMTP** ou **POP antes de SMTP** como **Método de autenticação**, introduza o nome de conta autenticada entre 0 e 255 caracteres em ASCII (0x20 a 0x7E). | |
| Palavra-passe autenticada | Se selecionar **Autentic. SMTP** ou **POP antes de SMTP** como **Método de autenticação**, introduza a palavra-chave autenticada entre 0 e 20 caracteres usando A-Z a-z 0-9 ! # $ % & ' * + - . / = ? ^ _ { \| } ~ @. | |
| Ender. de e-mail do remetente | Introduza o endereço de e-mail do remetente. Introduzir entre 0 e 255 caracteres em ASCII (0x20 a 0x7E) exceto: ( ) < > [ ] ; ¥. O primeiro carácter não pode ser um ponto final ("."). | |
| Endereço do servidor SMTP | Introduza entre 0 e 255 caracteres utilizando A-Z a-z 0-9 . - . Pode utilizar o formato IPv4 ou FQDN. | |
| Número da porta do serv. SMTP | Introduza um número entre 1 e 65535. | |

| Itens | Definições e explicação | |
|---|---|---|
| Ligação segura | Especifique o método de ligação segura para o servidor de correio eletrónico. | |
| | Inexistente | Se selecionar **POP antes de SMTP** no **Método de autenticação**, o método de ligação encontra-se definido para **Inexistente**. |
| | SSL/TLS | Isto está disponível quando o **Método de autenticação** estiver definido para **Desactivar** ou **Autentic. SMTP**. |
| | STARTTLS | Isto está disponível quando o **Método de autenticação** estiver definido para **Desactivar** ou **Autentic. SMTP**. |
| Validação do certificado | O certificado é validado quando esta opção está ativada. Recomendamos que defina para **Activar**. | |
| Endereço do servidor POP3 | Se selecionar **POP antes de SMTP** como **Método de autenticação**, introduza o endereço de servidor POP3 entre 0 e 255 caracteres usando A-Z a-z 0-9 . - . Pode utilizar o formato IPv4 ou FQDN. | |
| Número da porta do serv. POP3 | Se selecionar **POP antes de SMTP** como **Método de autenticação**, introduzir um número entre 1 e 65535. | |

### Informações relacionadas

➡ "Configurar um servidor de correio" na página 42

## Verificar uma ligação do servidor de correio

1. Selecionar Web Config e **Definições de rede** > **Servidor de e-mail** > **Teste de ligação**.
2. Selecione **Iniciar**.

   É iniciado o teste de ligação ao servidor de correio electrónico. Após o teste, é apresentado o relatório de verificação.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

➡ "Referências do teste de ligação do servidor de correio" na página 44

## Referências do teste de ligação do servidor de correio

| Mensagens | Explicação |
|---|---|
| O teste de ligação foi concluído com sucesso. | Esta mensagem aparece quando a ligação ao servidor é bem-sucedida. |

**Configurações de funcionamento e gestão**

| Mensagens | Explicação |
|---|---|
| Erro de comunicação do servidor SMTP. Verifique o seguinte. - Definições de rede | Esta mensagem é apresentada quando<br>❏ O scanner não está ligado a uma rede<br>❏ O servidor SMTP está inativo<br>❏ A ligação de rede é desativada durante a comunicação<br>❏ Foram recebidos dados incompletos |
| Erro de comunicação do servidor POP3. Verifique o seguinte. - Definições de rede | Esta mensagem é apresentada quando<br>❏ O scanner não está ligado a uma rede<br>❏ O servidor POP3 está inativo<br>❏ A ligação de rede é desativada durante a comunicação<br>❏ Foram recebidos dados incompletos |
| Ocorreu um erro ao ligar ao servidor SMTP. Verifique o seguinte. - Endereço do servidor SMTP - Servidor DNS | Esta mensagem é apresentada quando<br>❏ A ligação a um servidor DNS falhou<br>❏ A resolução de nome para um servidor SMTP |
| Ocorreu um erro ao ligar ao servidor POP3. Verifique o seguinte. - Endereço do servidor POP3 - Servidor DNS | Esta mensagem é apresentada quando<br>❏ A ligação a um servidor DNS falhou<br>❏ A resolução de nome para um servidor POP3 |
| Erro de autenticação do servidor SMTP. Verifique o seguinte. - Método de autenticação - Conta autenticada - Palavra-passe autenticada | Esta mensagem é apresentada quando a autenticação no servidor SMTP falha. |
| Erro de autenticação do servidor POP3. Verifique o seguinte. - Método de autenticação - Conta autenticada - Palavra-passe autenticada | Esta mensagem é apresentada quando a autenticação no servidor POP3 falha. |
| Método de comunicação não suportado. Verifique o seguinte. - Endereço do servidor SMTP - Número da porta do serv. SMTP | Esta mensagem é apresentada quando tenta comunicar com protocolos não suportados. |
| A ligação ao servidor SMTP falhou. Mude Ligação segura para Inexistente. | Esta mensagem é apresentada quando ocorre uma discrepância entre um servidor SMTP e um cliente, ou quando o servidor não suporta ligações SMTP segura (ligação SSL). |
| A ligação ao servidor SMTP falhou. Mude Ligação segura para SSL/TLS. | Esta mensagem é apresentada quando ocorre uma discrepância entre um servidor SMTP e um cliente, ou quando o servidor solicita a utilização de uma ligação SSL/TLS para uma ligação SMTP segura. |
| A ligação ao servidor SMTP falhou. Mude Ligação segura para STARTTLS. | Esta mensagem é apresentada quando ocorre uma discrepância entre um servidor SMTP e um cliente, ou quando o servidor solicita a utilização de uma ligação STARTTLS para uma ligação SMTP segura. |
| A ligação não é fiável. Verifique o seguinte. - Data e Hora | Esta mensagem é apresentada quando as definições de data e hora do scanner não estão corretas ou o certificado expirou. |
| A ligação não é fiável. Verifique o seguinte. - Certificado CA | Esta mensagem é apresentada quando o scanner não tem um certificado de raiz correspondente ao servidor, ou não foi importado um Certificado CA. |
| A ligação não é fiável. | Esta mensagem é apresentada quando o certificado obtido está danificado. |

| Mensagens | Explicação |
|---|---|
| A autenticação do servidor SMTP falhou. Mude Método de autenticação para Autentic. SMTP. | Esta mensagem é apresentada quando ocorre uma discrepância no método de autenticação entre um servidor e o cliente. O servidor suporta Autentic. SMTP. |
| A autenticação do servidor SMTP falhou. Mude Método de autenticação para POP antes de SMTP. | Esta mensagem é apresentada quando ocorre uma discrepância no método de autenticação entre um servidor e o cliente. O servidor não suporta Autentic. SMTP. |
| Ender. de e-mail do remetente está incorreto. Mude para o endereço de e-mail do seu serviço de e-mail. | Esta mensagem é apresentada quando o endereço de correio eletrónico do remetente especificado está errado. |
| Não é possível aceder ao produto até o processamento estar concluído. | Esta mensagem aparece quando o scanner está ocupado. |

### Informações relacionadas

➡ "Verificar uma ligação do servidor de correio" na página 44

# Atualizar o firmware

## Atualizar o firmware usando Web Config

Atualizar o firmware usando Web Config. O dispositivo deve estar ligado à Internet.

1. Aceder a Web Config e selecione **Definições básicas** > **Actualização do firmware**.
2. Clique em **Iniciar**.

   A confirmação de firmware é iniciada, e a informação de firmware é exibida se existir um firmware atualizado.
3. Clique em **Iniciar**, e siga as instruções exibidas no ecrã.

***Nota:***
*Também pode atualizar o firmware usando o Epson Device Admin. Pode confirmar visualmente as informações de firmware na lista de dispositivo. É útil quando quiser atualizar o firmware de vários dispositivos. Consulte o guia Epson Device Admin ou a ajuda para obter mais informações.*

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23
➡ "Epson Device Admin" na página 55

## Atualizar o Firmware usando Epson Firmware Updater

Pode transferir o firmware do dispositivo a partir do sítio Web da Epson no computador e, em seguida, ligue o dispositivo e o computador através de um cabo USB para atualizar o firmware. Se não for possível atualizar através da rede, tente este método.

1. Aceder ao sítio Web da Epson e transfira o firmware.

2. Ligue o computador que contém o firmware transferido para o dispositivo pelo cabo USB.
3. Clique duas vezes no ficheiro .exe transferido.

   O Epson Firmware Updater inicia.
4. Siga as instruções apresentadas no ecrã.

# Fazer cópia de segurança das configurações

Ao exportar os itens das definições em Web Config, pode copiar os itens a outros scanners.

## Exportar as definições

Exporte cada item das definições do scanner.

1. Selecione Web Config e, em seguida, **Exportar e importar valor de definição** > **Exportar**.
2. Selecione as definições que pretende exportar.

   Selecione as definições que pretende exportar. Se tiver selecionado uma categoria superior, as subcategorias também são selecionadas. No entanto, as subcategorias que causam erros devido a duplicação na mesma rede (como os endereços de IP, etc.) não podem ser selecionadas.
3. Introduza uma palavra-passe para encriptar o ficheiro exportado.

   É necessária a palavra-passe para importar o ficheiro. Deixe em branco se não quiser encriptar o ficheiro.
4. Clique em **Exportar**.

   ***Importante:***

   *Se quiser exportar as definições de rede do scanner, como o nome do scanner e o endereço de IP, selecione* ***Ative para selecionar as definições individuais do dispositivo*** *e selecione mais itens. Utilize apenas os valores selecionados para o scanner de substituição.*

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

## Importar as definições

Importe o ficheiro do Web Config exportado para o scanner.

***Importante:***

*Aquando da importação de valores que incluam informações individuais, como o nome do scanner ou endereço de IP, certifique-se de que o endereço de IP não existe já na mesma rede. Se o endereço de IP for repetido, o scanner não reflete o valor.*

1. Selecione Web Config e, em seguida, **Exportar e importar valor de definição** > **Importar**.

2. Selecione o ficheiro exportado e introduza a palavra-passe de encriptação.
3. Clique em **Seguinte**.
4. Selecione as definições que deseja importar e clique em **Seguinte**.
5. Clique em **OK**.

As definições são aplicadas ao scanner.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

# Resolver problemas

## Sugestões para a resolução de problemas

Pode encontrar mais informações no seguinte manual.

❏ Guia do Utilizador

Oferece instruções sobre a utilização do scanner, manutenção e resolução de problemas.

## Verificando o registo do servidor e o dispositivo de rede

Em caso de problema com a ligação de rede, é possível identificar a causa confirmando o registo do servidor de e-mail, servidor LDAP, etc., verificando o estado usando o registo de comandos como roteadores e registos de equipamentos do sistema de rede.

## Inicializar as definições de rede

### Recuperar as configurações de Wi-Fi a partir do Painel de Controlo

Pode restaurar todas as predefinições de rede.

1. Toque em **Definições** no ecrã de início.
2. Toque em **Administração do sistema** > **Restaurar predefinições** > **Definições de rede**.
3. Verifique a mensagem e toque em **Sim**.
4. Quando for apresentada uma mensagem de conclusão, toque em **Fechar**.

   O ecrã desliga-se automaticamente após um período de tempo específico se não tocar em **Fechar**.

## Verifique a comunicação entre computadores e os dispositivos

### Verificação da ligação utilizando um comando Ping - Windows

Pode usar um comando Ping para verificar se o computador está ligado ao scanner. Siga os passos abaixo para verificar a ligação usando um comando Ping.

**Resolver problemas**

1. Verifique o endereço IP do scanner para a ligação pretendida.

   Pode verificar usando o Epson Scan 2.

2. Aceda ao ecrã de linha de comandos do computador.

   ❏ Windows 10

   Clique com o botão do lado direito do rato no botão iniciar ou mantenha premido e selecione **Linha de Comandos**.

   ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

   Aceda ao ecrã de aplicações e selecione **Linha de Comandos**.

   ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 ou anterior

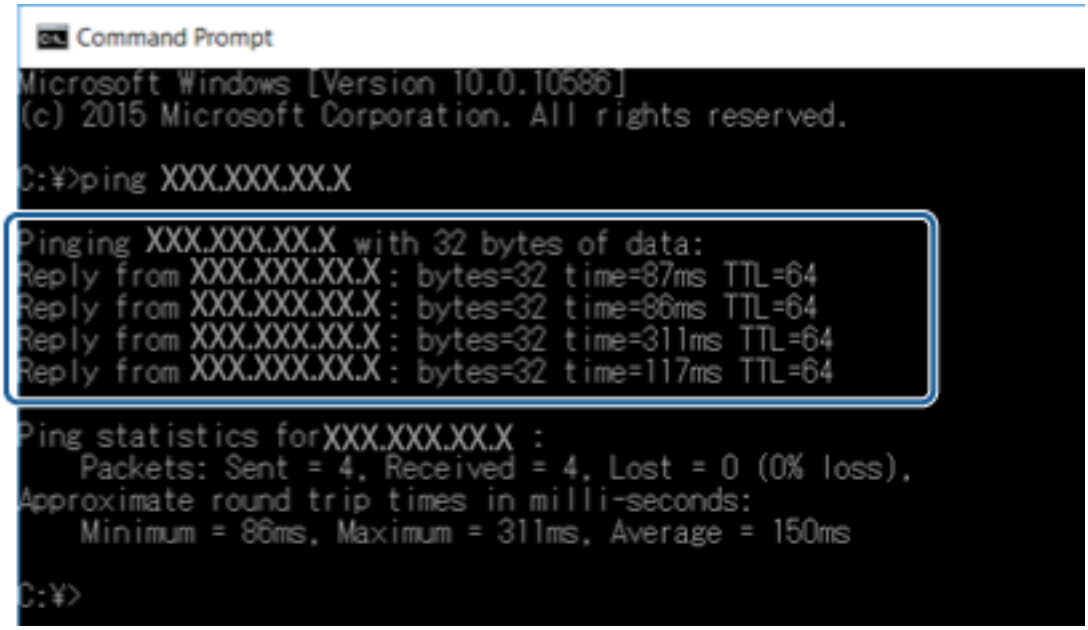
   Clique no botão Iniciar, selecione **Todos os Programas** ou **Programas** > **Acessórios** > **Linha de Comandos**.

3. Introduza "ping xxx.xxx.xxx.xxx" e prima a tecla Enter.

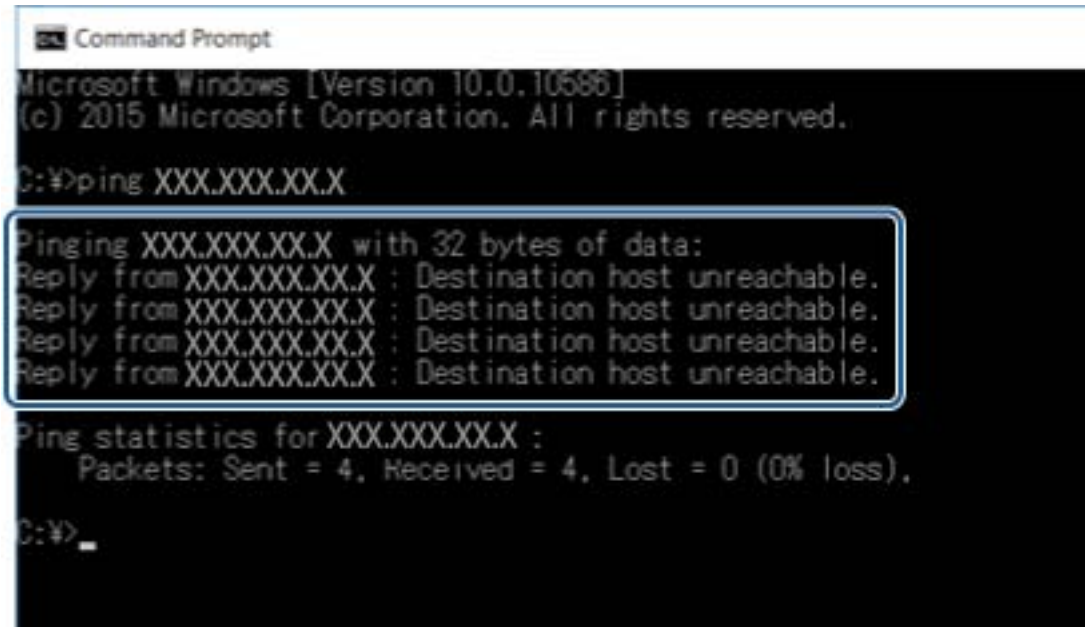
   Introduza o endereço IP do scanner em xxx.xxx.xxx.xxx.

4. Verifique o estado da comunicação.

   Se existir comunicação entre o scanner e o computador, é apresentada a mensagem abaixo.



Se não existir comunicação entre o scanner e o computador, é apresentada a mensagem abaixo.




## Verificação da ligação utilizando um comando Ping — Mac OS

Pode usar um comando Ping para verificar se o computador está ligado ao scanner. Siga os passos abaixo para verificar a ligação usando um comando Ping.

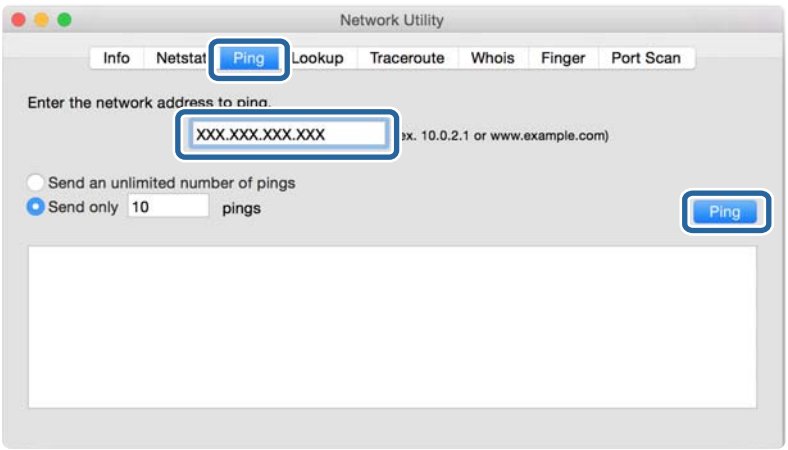
1. Verifique o endereço IP do scanner para a ligação pretendida.

   Pode verificar usando o Epson Scan 2.

2. Execute o Network Utility.

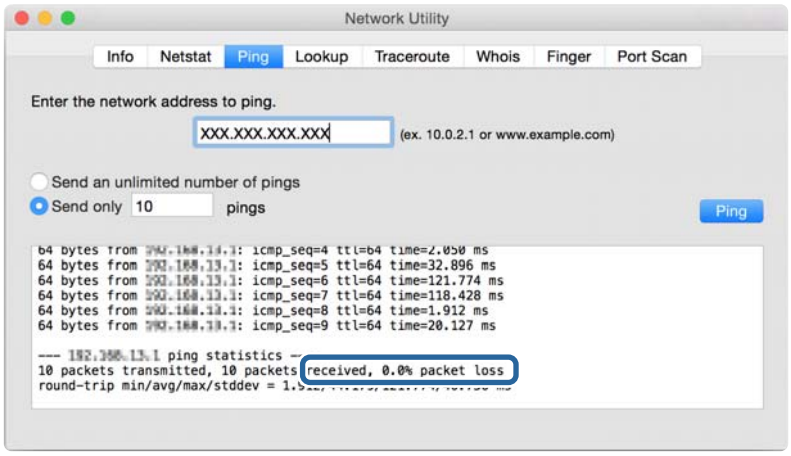
   Introduza "Network Utility" no **Spotlight**.

3. Clique no separador **Ping**, introduza o endereço IP que verificou no passo 1 e clique em **Ping**.

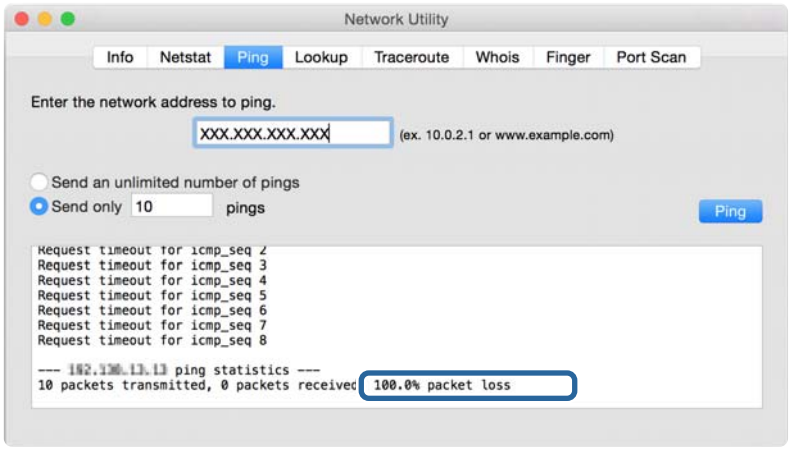


4. Verifique o estado da comunicação.

   Se existir comunicação entre o scanner e o computador, é apresentada a mensagem abaixo.




   Se não existir comunicação entre o scanner e o computador, é apresentada a mensagem abaixo.




# Problemas de utilização do software de rede

## Não é possível aceder ao Web Config

### O endereço IP do scanner está configurado adequadamente?

Configure o endereço IP usando Epson Device Admin ou EpsonNet Config.

### O seu navegador suporta as encriptações em série para o Força da encriptação para SSL/TLS?

As encriptações em série para a Força da encriptação para SSL/TLS são as seguintes. Web Config só pode ser acedida num navegador compatível com as seguintes codificações em série. Verifique o suporte de encriptação do seu navegador.

- ❏ 80bit: AES256/AES128/3DES
- ❏ 112bit: AES256/AES128/3DES
- ❏ 128bit: AES256/AES128

❏ 192bit: AES256

❏ 256bit: AES256

### Aparece a mensagem "Fora de prazo" quando acede ao Web Config utilizando a comunicação SSL (https).

Se o certificado estiver fora de prazo, volte a obter o certificado. Se a mensagem aparecer antes da data da validade, certifique-se de que a data do scanner está configurada corretamente.

### Aparece a mensagem "O nome do certificado de segurança não corresponde…" quando acede ao Web Config utilizando a comunicação SSL (https).

O endereço IP do scanner introduzido em **Nome comum** para criar um certificado assinado automaticamente ou CSR não corresponde ao endereço introduzido no browser. Obtenha e importe novamente um certificado ou altere o nome do scanner.

### O scanner está a ser acedido através de um servidor proxy.

Se estiver a utilizar um servidor proxy com o scanner, terá de configurar as definições proxy do navegador.

❏ Windows:

Selecione **Painel de Controlo** > **Rede e Internet** > **Opções da Internet** > **Ligações** > **Definições de LAN** > **Servidor proxy** e configure a não utilização do servidor proxy para endereços locais.

❏ Mac OS:

Selecione **Preferências do Sistema** > **Rede** > **Avançadas** > **Proxies** e registe o endereço local em **Ignorar especificações do proxy para estes Servidores & Domínios**.

Exemplo:

192.168.1.*: endereço local 192.168.1.XXX, máscara de sub-rede 255.255.255.0

192.168.*.*: endereço local 192.168.XXX.XXX, máscara de sub-rede 255.255.0.0

### Informações relacionadas

➡ “Aceder ao Web Config” na página 23

➡ “Atribuir o endereço IP” na página 15

➡ “Atribua um endereço IP usando EpsonNet Config” na página 56

## O nome do modelo e/ou o endereço IP não aparecem no EpsonNet Config

### Seleccionou Bloquear, Cancelar ou Encerrar quando apareceu um ecrã de segurança do Windows ou um ecrã de firewall?

Se seleccionar **Bloquear**, **Cancelar** ou **Encerrar**, o endereço IP e o nome do modelo não são apresentados no EpsonNet Config ou no EpsonNet Setup.

Para corrigir esta situação, registe o EpsonNet Config como excepção utilizando a firewall do Windows e software de segurança comercial. Se utilizar um programa antivírus ou de segurança, feche-o e, em seguida, experimente utilizar o EpsonNet Config.

## Resolver problemas

### A definição de tempo excedido para erros de comunicação é demasiado curta?

Execute o EpsonNet Config, seleccione **Tools** > **Options** > **Timeout**, e aumente o período de tempo na definição **Communication Error**. Tenha em atenção que ao fazê-lo o EpsonNet Config poderá ser executado mais lentamente.

### Informações relacionadas

➡ "Executar o EpsonNet Config — Windows" na página 56

➡ "Executar o EpsonNet Config — Mac OS" na página 56

# Apêndice

## Introdução de software de rede

A seguir descrevemos o software que configura e gestão de dispositivos.

### Epson Device Admin

A Epson Device Admin é uma aplicação que permite instalar dispositivos na rede, e a seguir configurar e gerir os dispositivos. É possível adquirir informações detalhadas para dispositivos tais como estado e consumíveis, enviar notificações de alertas, e criar relatórios para uso do dispositivo. Pode fazer um modelo com itens de configuração e aplicar a outros dispositivos como definições partilhadas. Pode transferir o Epson Device Admin a partir do sítio Web de suporte Epson. Para mais informações, consulte a documentação ou a ajuda do Epson Device Admin.

#### Executar Epson Device Admin (apenasWindows)

Selecionar **Todos os Programas** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

***Nota:***
*Se aparecer o alerta da firewall, permita o acesso aoEpson Device Admin.*

### Configuração EpsonNet

O EpsonNet Config permite ao administrador configurar as definições de rede do scanner, como atribuir um endereço IP e alterar o modo de ligação. A funcionalidade de definições de série é compatível com Windows. Para mais informações, consulte a documentação ou a ajuda do EpsonNet Config.

### Executar o EpsonNet Config — Windows

Selecionar **Todos os programas** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

***Nota:***
*Se aparecer o alerta da firewall, permita o acesso aoEpsonNet Config.*

### Executar o EpsonNet Config — Mac OS

Selecione **Ir** > **Aplicações** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

## EpsonNet SetupManager

EpsonNet SetupManager é um software para criar um pacote para uma instalação simples de scanner, tais como instalar e configurar o controlador do scanner e instalar Document Capture Pro. Este software permite ao administrador criar pacotes de software únicos e distribuí-los entre grupos.

Para mais informações, visite o seu sítio Web regional Epson.

# Atribua um endereço IP usando EpsonNet Config

Pode atribuir um endereço IP ao scanner usando o EpsonNet Config. EpsonNet Config permite-lhe atribuir um endereço IP a outro scanner que não tenha sido atribuído após ligar o cabo Ethernet.

## Atribua um endereço IP usando as definições em lote

### Criar o ficheiro para definições de lote

Ao usar o endereço MAC e nome do modelo como palavras-passe, pode criar um novo ficheiro SYLK para definir o endereço IP.

1. Abra um editor de folha de cálculo ou (como o Microsoft Excel) ou um editor de texto.

2. Introduza "Info_MACAddress", "Info_ModelName", e "TCPIP_IPAddress" na primeira linha como definições de nomes de itens.

   Introduza os itens das definições para as seguintes linhas de texto. Para distinguir entre maiúsculas e minúsculas e caracteres de duplo byte ou byte único, caso apenas um caracter seja diferente, o item não será reconhecido.

   Introduza o nome do item de definição como descrito abaixo; se não o fizer, EpsonNet Config não pode reconhecer os itens de definição.

| Info_MACAddress | Info_ModelName | TCPIP_IPAddress |
|---|---|---|
| | | |
| | | |

3. Introduza o endereço MAC, nome de modelo, e endereço IP para cada interface de rede.

| Info_MACAddress | Info_ModelName | TCPIP_IPAddress |
|---|---|---|
| 0000XXXX0001 | ALC-XXXXX | 192.168.100.102 |
| 0000XXXX0002 | ALC-XXXXX | 192.168.100.103 |
| 0000XXXX0003 | ALC-XXXXX | 192.168.100.104 |

4. Introduza um nome e guarde como ficheiro SYLK (*.slk).

## Realizar definições de lote usando o ficheiro de configuração

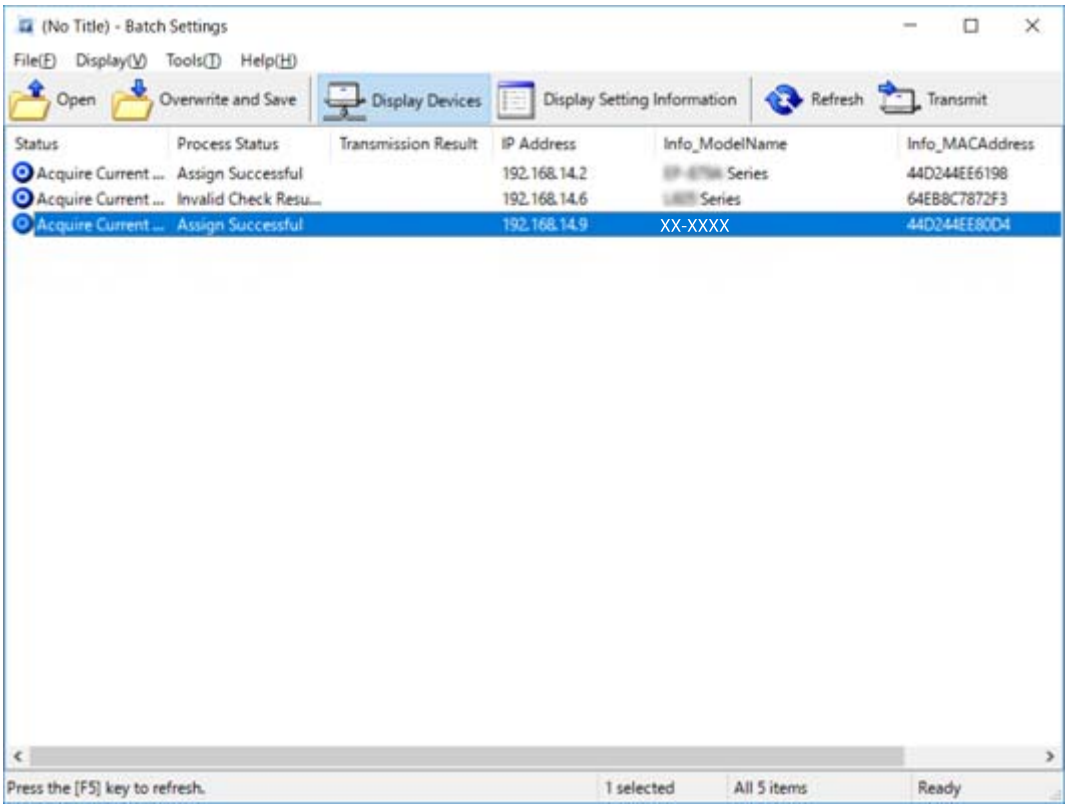
Atribuir o endereço IP no ficheiro de configuração (SYLK file) de uma vez. É necessário criar o ficheiro de configuração antes de atribuir.

1. Ligue todos os dispositivos à rede usando cabos Ethernet.
2. Ligue o scanner.
3. Inicie o EpsonNet Config.

   É exibida uma lista dos scanners na rede. Pode demorar algum tempo até serem exibidas.
4. Clique em **Tools** > **Batch Settings**.
5. Clique em **Open**.
6. No ecrã de seleção de ficheiro, selecione o ficheiro SYLK (*.slk) com as configurações, e a seguir clique em **Open**.

7. Selecione os dispositivos nos quais pretende realizar as definições em lote com a coluna **Status** definida como **Unassigned**, e o **Process Status** definido como **Assign Successful**.

   Ao fazer várias seleções, pressione Ctrl ou Shift e clique ou arraste com o rato.




8. Clique em **Transmit**.

9. Quando for exibida a janela para introduzir a palavra-passe, introduzir a palavra-passe, e a seguir clique em **OK**.

   Transmitir as configurações.

   ***Nota:***
   *As informações são transmitidas para a interface de rede até que seja concluída a barra de progresso. Não desligue o dispositivo ou o adaptador sem fios e não envie dados para o dispositivo.*

10. No ecrã **Transmitting Settings**, clique em **OK**.

11. Verifique o estado do dispositivo definido.

    No caso dos dispositivos que exibem  ou  , verifique o conteúdo do ficheiro de definição, ou se o dispositivo foi reiniciado normalmente.

| Ícone | Status | Process Status | Explicação |
|---|---|---|---|
|  | Setup Complete | Setup Successful | Configuração concluída normalmente. |
|  | Setup Complete | Rebooting | Quando as informações forem transmitidas, os dispositivos devem ser reiniciados para implementar as definições. É realizada uma verificação para determinar se o dispositivo pode ou não ser ligado após ser reiniciado. |
|  | Setup Complete | Reboot Failed | Não é possível confirmar o dispositivo após transmitir as configurações. Verifique se o dispositivo está ligado, ou se reiniciou normalmente. |
|  | Setup Complete | Searching | Procurar o dispositivo indicado no ficheiro de definições.* |
|  | Setup Complete | Search Failed | Não é possível verificar os dispositivos que já foram configurados. Verifique se o dispositivo está ligado, ou se reiniciou normalmente.* |

    * Apenas quando as informações de configuração são exibidas.

### Informações relacionadas

➡ "Executar o EpsonNet Config — Windows" na página 56
➡ "Executar o EpsonNet Config — Mac OS" na página 56

## Atribuir um endereço IP a cada dispositivo

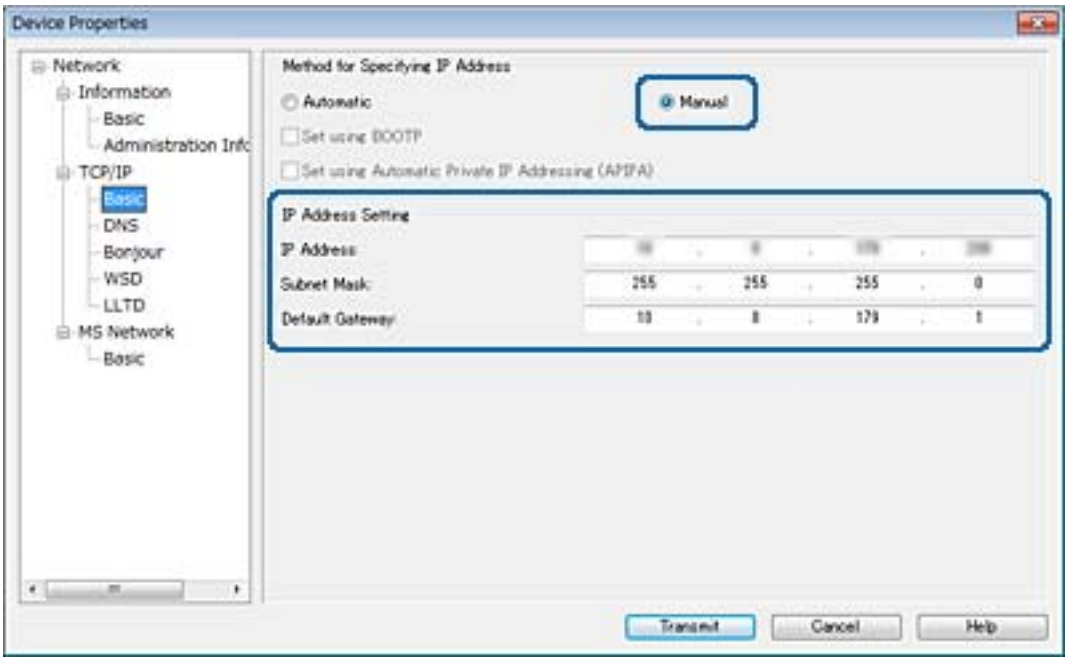
Atribuir um endereço IP a scanner utilizando EpsonNet Config.

1. Ligue o scanner.
2. Ligue o scanner à rede usando um cabo Ethernet.
3. Inicie o EpsonNet Config.

   É exibida uma lista dos scanners na rede. Pode demorar algum tempo até serem exibidas.
4. Clique duas vezes no scanner ao qual pretende atribuir.

   ***Nota:***
   *Se tiver ligados vários scanners do mesmo modelo, pode identificar a impressora usando o endereço MAC.*
5. Seleccione **Network** > **TCP/IP** > **Basic**.

6. Introduza os endereços para **IP Address**, **Subnet Mask**, e **Default Gateway**.




***Nota:***
*Digite um endereço estático quando ligar o scanner a uma rede segura.*

7. Clique em **Transmit**.

   É exibida uma janela que confirma a transmissão das informações.

8. Clique em **OK**.

   É exibida a janela de finalização da transmissão.

   ***Nota:***
   *As informações são transmitidas para o dispositivo, e a seguir é exibida a mensagem "Configuração terminada com sucesso.". Não desligue o dispositivo e não envie dados para o dispositivo.*

9. Clique em **OK**.

### Informações relacionadas

➡ "Executar o EpsonNet Config — Windows" na página 56
➡ "Executar o EpsonNet Config — Mac OS" na página 56

# Usar a porta para o scanner

O scanner usa a seguinte porta. Estas portas devem tornar-se disponíveis pelo administrador da rede, conforme necessário.

## Apêndice

| Remetente (Cliente) | Utilizar | Destino (Servidor) | Protocolo | Número da porta |
|---|---|---|---|---|
| Scanner | Envio de e-mail (notificação e-mail) | Servidor SMPT | SMTP (TCP) | 25 |
| | | | SMTP SSL/TLS (TCP) | 465 |
| | | | SMTP STARTTLS (TCP) | 587 |
| | POP antes de ligação SMTP (notificação e-mail | Servidor POP | POP3 (TCP) | 110 |
| | Controlar WSD | Computador cliente | WSD (TCP) | 5357 |
| | Procurar o computador ao digitalizar em push a partir do Document Capture Pro | Computador cliente | Descoberta da rede de digitalização push | 2968 |
| | Recolha de informações da tarefa ao digitalizar em push a partir do Document Capture Pro | Computador cliente | Digitalização de rede em push | 2968 |
| Computador cliente | Descobrir o scanner a partir de uma aplicação como por exemplo EpsonNet Config e controlador de scanner. | Scanner | ENPC (UDP) | 3289 |
| | Recolha e configuração das informações MIB de uma aplicação como por exemplo EpsonNet Config e controlador de scanner. | Scanner | SNMP (UDP) | 161 |
| | Procurar scanner WSD | Scanner | Descoberta WS (UDP) | 3702 |
| | Reencaminhar os dados digitalizados a partir do Document Capture Pro | Scanner | Digitalização de rede (TCP) | 1865 |

# Configurações de segurança avançada para empresas

Neste capítulo, descrevemos os recursos de segurança avançados.

## Definições de segurança e prevenção de perigo

Quando um dispositivo é ligado a uma rede, é possível aceder ao mesmo a partir de um local remoto. Para além disso, o dispositivo pode ser partilhado por várias pessoas, uma funcionalidade útil para melhorar a conveniência e eficiência operacional. No entanto, aumentam os riscos tais como acesso ilegal, utilização ilegal e adulteração de dados. Se usar o dispositivo num ambiente onde pode aceder à Internet, os riscos são ainda maiores.

Para evitar este risco, os dispositivos Epson dispõem de uma variedade de tecnologias de segurança.

Definir o dispositivo como necessário de acordo com as condições ambientais que foram construídas com informações sobre o ambiente do cliente.

| Nome | Tipo de funcionalidade | O que definir | O que evitar |
|---|---|---|---|
| Comunicação SSL/TLS | O percurso de comunicação de um computador e um dispositivo é encriptado utilizando comunicação SSL/TLS. O conteúdo da comunicação através do navegador é protegido. | Definir um certificado de AC para o servidor certificado assinado por uma AC (autoridade de certificação) para o dispositivo. | Evitar a fuga de informações de configuração e o conteúdo dos dados transferidos para o scanner a partir do computador. Aceder ao servidor Epson na Internet a partir do dispositivo também pode ser protegido usando uma atualização de firmware, etc. |
| Filtragem IPsec/IP | É possível definir para permitir cortando e eliminando dados de um determinado cliente ou de um tipo específico. Uma vez que o IPsec protege os dados por unidade de pacotes IP (criptografia e autenticação), é possível comunicar com segurança com protocolos de digitalização não seguros. | Crie uma política básica e política individual para definir o cliente ou tipo de dados que podem aceder ao dispositivo. | Proteger o acesso não autorizado e adulteração e interceção de dados de comunicação enviados para o dispositivo. |
| SNMPv3 | São adicionados recursos tais como monitorização de dispositivos ligados em rede, integridade dos dados para o protocolo SNMP para controlar, criptografia, autenticação de utilizador, etc. | Ativar o SNMPv3, e a seguir definir o método de encriptação e autenticação. | Certifique-se de alterar as configurações através da rede, confidencialidade no modo de monitorização. |

| Nome | Tipo de funcionalidade | O que definir | O que evitar |
|---|---|---|---|
| IEEE802.1X | Permite apenas um usuário que é autenticado para ligar por Ethernet. Permite que apenas um utilizador autorizado use o dispositivo. | Definição de autenticação para o servidor RADIUS (servidor de autenticação). | Protege contra o acesso não autorizado e utilização do dispositivo. |
| Leitura do cartão de identificação | É possível utilizar o dispositivo através de um cartão de identificação para o dispositivo autenticado que está ligado. É possível limitar a aquisição dos registos de cada utilizador e dispositivo e limitar a utilização de dispositivos disponíveis e os recursos disponíveis de cada utilizador e grupo. | Ligar um dispositivo de autenticação ao dispositivo e a seguir, defina as informações de um utilizador no sistema de autenticação. | Prevenir a utilização não autorizada e spoofing do dispositivo. |

**Informações relacionadas**

➡ "Comunicações SSL/TLS com o scanner" na página 63

➡ "Comunicações encriptada usando filtro IPsec/IP" na página 71

➡ "Utilizar o protocolo SNMPv3" na página 83

➡ "Ligar o scanner a uma rede IEEE802.1X" na página 85

## Definições do recurso de segurança

Ao definir a filtragem IPsec/IP ou IEEE802.1X, recomendamos aceder a Web Config usando SSL/TLS para transmitir as informações de definições para reduzir os riscos de segurança tais como a manipulação e a interceção.

# Comunicações SSL/TLS com o scanner

Quando o certificado do servidor é definido usando a comunicação SSL/TLS (Secure Sockets Layer/Transport Layer Security) para o scanner, pode encriptar o percurso de comunicação entre computadores. Proceda desta forma se pretende evitar acesso remoto e não autorizado.

## Informações sobre certificação digital

❏ Certificado assinado por uma CA

Um certificado assinado por uma CA (Autoridade de Certificação) tem de ser obtido através de uma autoridade de certificação. Pode garantir comunicações seguras através da utilização de um certificado CA assinado. Pode utilizar um certificado CA assinado para cada função de segurança.

❏ Certificado CA

Um certificado CA indica que uma terceira parte verificou a identidade de um servidor. Este é um componente-chave para uma web de confiança segura. Necessita de obter um certificado CA para autenticação de servidor através de uma CA que o emita.

❏ Certificado assinado automaticamente

O certificado assinado automaticamente é um certificado que o scanner emite e assina. Este certificado não é fiável e não consegue evitar o spoofing. Se utilizar este certificado para um certificado SSL/TLS, poderá aparecer um alerta de segurança num browser. Apenas pode utilizar este certificado para uma comunicação SSL/TLS.

### Informações relacionadas

➡ "Obter e importar um certificado CA assinado" na página 64

➡ "Apagar um certificado CA assinado" na página 67

➡ "Atualizar um certificado assinado automaticamente" na página 68

# Obter e importar um certificado CA assinado

## Obter um certificado CA assinado

Para obter um certificado CA assinado, crie um CSR (Pedido de Assinatura de Certificado) e aplique-o para certificar a autoridade. Pode criar um CSR utilizando o Web Config e um computador.

Siga as instruções para criar um CSR e obter um certificado CA assinado utilizando o Web Config. Quando criar um CSR com o Web Config, o certificado tem o formato PEM/DER.

1. Selecione Web Config e, em seguida, **Definições de segurança de rede**. A seguir, selecione **SSL/TLS** > **Certificado** ou **IPsec/Filtro de IP** > **Certificado do cliente** ou **IEEE802.1X** > **Certificado do cliente**.

2. Clique em **Gerar** de **CSR**.

   Abre uma página de criação de CSR.

3. Introduza um valor para cada item.

   ***Nota:***
   *O comprimento da chave e as abreviaturas disponíveis variam em função da autoridade de certificação. Crie um pedido de acordo com as regras de cada autoridade de certificação.*

4. Clique em **OK**.

   É apresentada uma mensagem de finalização.

5. Selecione **Definições de segurança de rede**. A seguir, selecione **SSL/TLS** > **Certificado**, ou **IPsec/Filtro de IP** > **Certificado do cliente** ou **IEEE802.1X** > **Certificado do cliente**.

6. Clique num dos botões de transferência de **CSR**, de acordo com um formato especificado por cada autoridade de certificação, para transferir um CSR para um computador.

   ***Importante:***
   *Não gere um CSR novamente. Se o fizer, poderá não conseguir importar um Certificado CA assinado emitido.*

7. Envie o CSR para uma autoridade de certificação e obtenha um Certificado CA assinado.

   Siga as regras de cada autoridade de certificação em relação ao método e à forma de envio.

8. Guarde o Certificado CA assinado num computador ligado ao scanner.

   A obtenção de um Certificado CA assinado fica concluída quando guarda o certificado num destino.

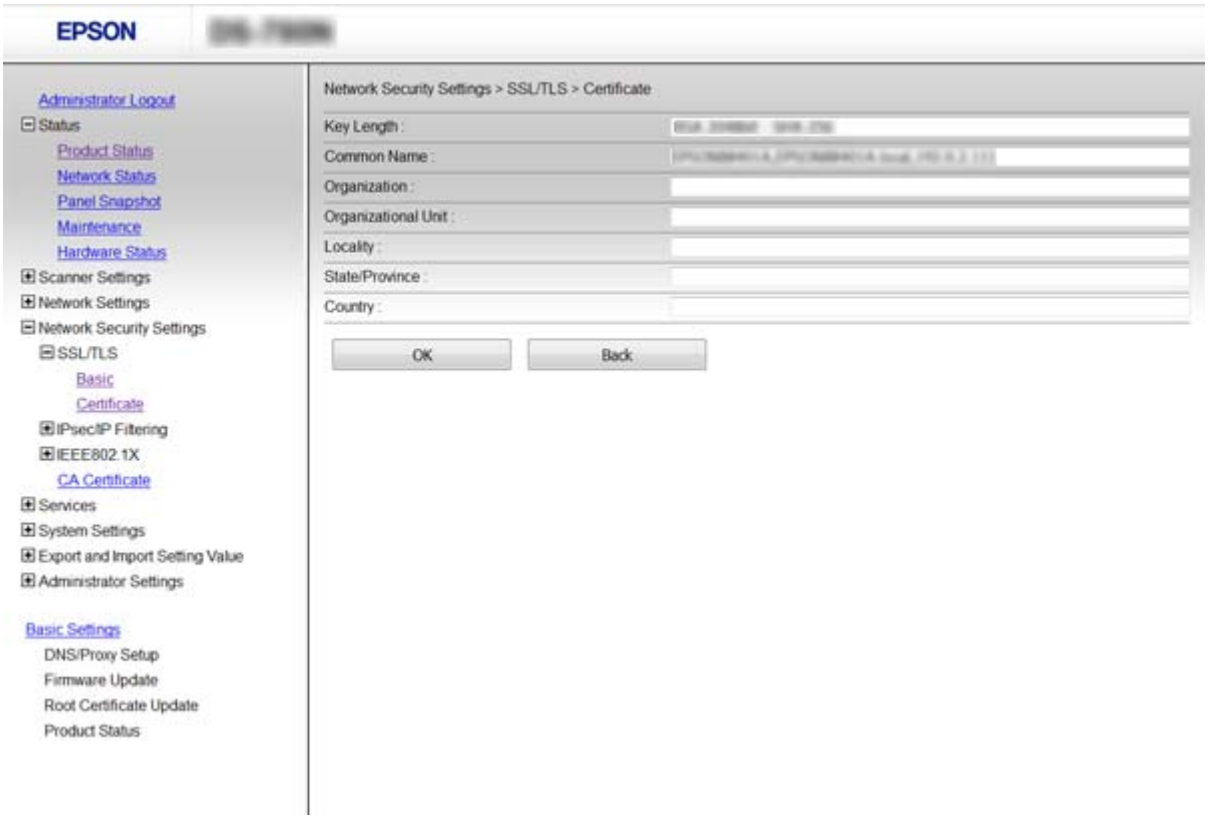
### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

➡ "Itens de definição de CSR" na página 65

➡ "Importar um certificado CA assinado" na página 66

## *Itens de definição de CSR*




| Itens | Definições e explicação |
|---|---|
| Comprimento da chave | Seleccione um comprimento de chave para um CSR. |
| Nome comum | Pode introduzir entre 1 e 128 caracteres. Se se tratar de um endereço IP, deverá ser um endereço IP estático.<br>Exemplo:<br>URL para aceder ao Web Config: https://10.152.12.225<br>Nome comum: 10.152.12.225 |
| Organização/ Unidade organizacional/ Localidade/ Estado/Província | Introduza entre 0 e 64 caracteres em ASCII (0x20–0x7E). Pode separar nomes distintos com vírgulas. |
| País | Introduza um código de país com um número de dois dígitos especificado pela ISO-3166. |

### Informações relacionadas

➡ "Obter um certificado CA assinado" na página 64

## Importar um certificado CA assinado

***Importante:***

❏ *Certifique-se de que a data e a hora do scanner estão corretamente definidas.*

❏ *Se obtiver um certificado utilizando um CSR criado através do Web Config, pode importar um certificado uma vez.*

1. Selecione Web Config e a seguir selecione **Definições de segurança de rede**. A seguir, selecione **SSL/TLS** > **Certificado**, ou **IPsec/Filtro de IP** > **Certificado do cliente** ou **IEEE802.1X** > **Certificado do cliente**.

2. Clique em **Importar**.

   Abre uma página de importação de certificados.

3. Introduza um valor para cada item.

   As definições necessárias podem variar em função de onde cria um CSR e do formato de ficheiro do certificado. Introduza valores para os itens necessários de acordo com o seguinte:

   ❏ Um certificado de formato PEM/DER obtido através do Web Config

   ❏ **Chave privada**: Não configure porque o scanner contém uma chave privada.

   ❏ **Palavra-passe**: Não configure.

   ❏ **Certificado CA 1/Certificado CA 2**: Opcional

   ❏ Um certificado de formato PEM/DER obtido através de um computador

   ❏ **Chave privada**: É necessário definir.

   ❏ **Palavra-passe**: Não configure.

   ❏ **Certificado CA 1/Certificado CA 2**: Opcional

   ❏ Um certificado de formato PKCS#12 obtido através de um computador

   ❏ **Chave privada**: Não configure.

   ❏ **Palavra-passe**: Opcional

   ❏ **Certificado CA 1/Certificado CA 2**: Não configure.

4. Clique em **OK**.

   É apresentada uma mensagem de finalização.

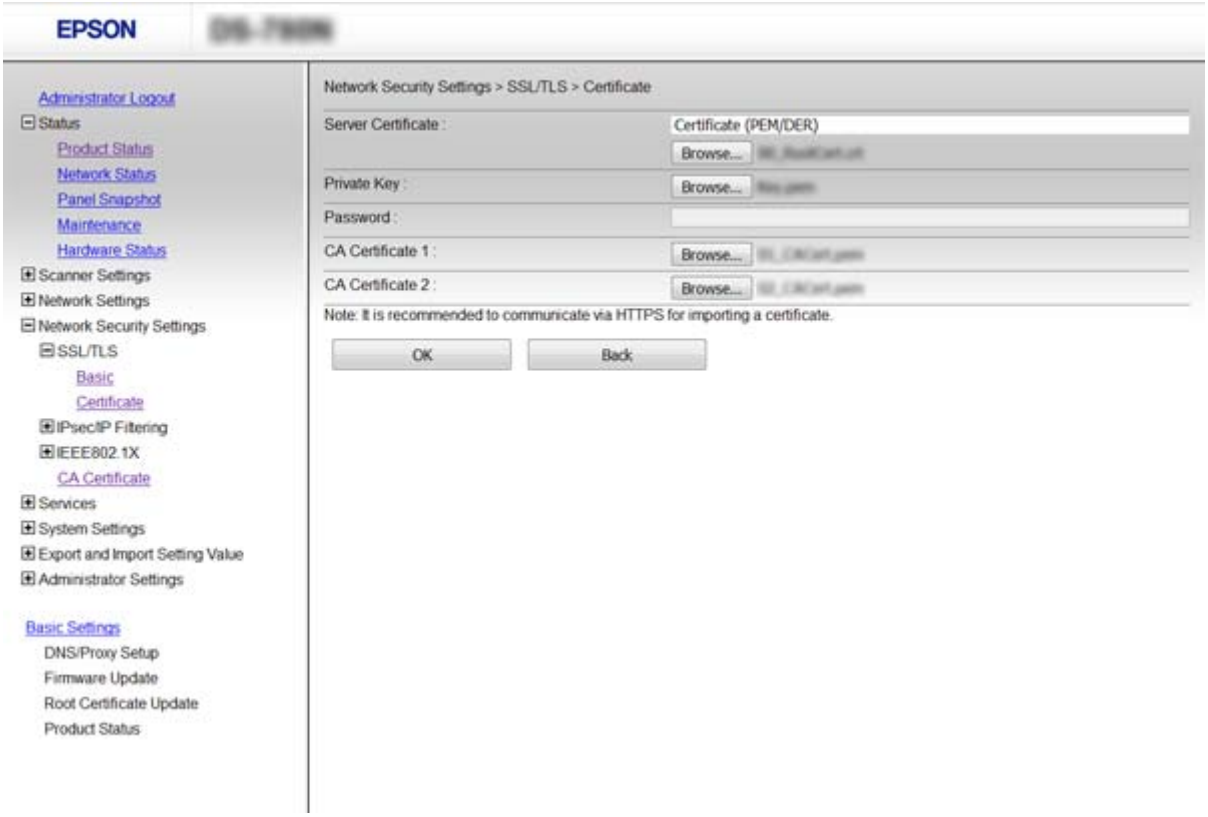
***Nota:***
*Clique em **Confirmar** para verificar as informações do certificado.*

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

➡ "Itens de definição da importação de um certificado CA assinado" na página 67

### *Itens de definição da importação de um certificado CA assinado*




| Itens | Definições e explicação |
|---|---|
| Certificado de servidor ou Certificado do cliente | Seleccione o formato de um certificado. |
| Chave privada | Se obtiver um certificado de formato PEM/DER utilizando um CSR criado através de um computador, especifique um ficheiro de chave privada que corresponda a um certificado. |
| Palavra-passe | Introduza uma palavra-passe para encriptar uma chave privada. |
| Certificado CA 1 | Se o formato do seu certificado for **Certificado (PEM/DER)**, importe um certificado de uma autoridade de certificação que emita um certificado de servidor. Especifique um ficheiro se for necessário. |
| Certificado CA 2 | Se o formato do seu certificado for **Certificado (PEM/DER)**, importe um certificado de uma autoridade de certificação que emita **Certificado CA 1**. Especifique um ficheiro se for necessário. |

#### Informações relacionadas

➡ "Importar um certificado CA assinado" na página 66

## Apagar um certificado CA assinado

Pode apagar um certificado importado quando o certificado tiver expirado ou quando uma ligação encriptada deixar de ser necessária.

> ***Importante:***
> *Se obtiver um certificado utilizando um CSR criado através do Web Config, não pode importar novamente um certificado apagado. Neste caso, crie um CSR e volte a obter um certificado.*

1. Selecione Web Config e, em seguida, **Definições de segurança de rede**. A seguir, selecione **SSL/TLS** > **Certificado**, ou **IPsec/Filtro de IP** > **Certificado do cliente** ou **IEEE802.1X** > **Certificado do cliente**.
2. Clique em **Eliminar**.
3. Confirme que pretende eliminar o certificado na mensagem apresentada.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

## Atualizar um certificado assinado automaticamente

Se o scanner suportar a função de servidor HTTPS, pode atualizar um certificado assinado automaticamente. Quando aceder ao Web Config utilizando um certificado assinado automaticamente, aparece uma mensagem de aviso.

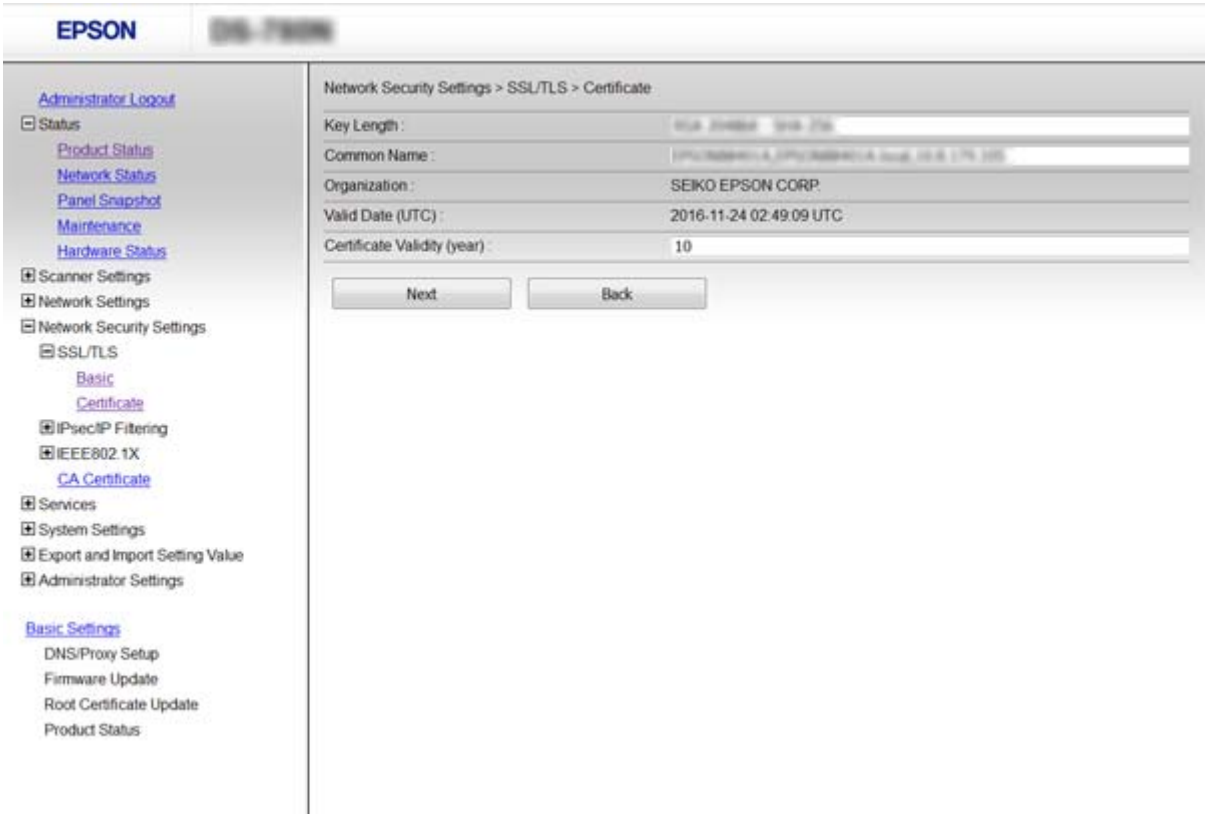
Utilize um certificado assinado automaticamente temporariamente até obter e importar um certificado CA assinado.

1. Selecionar Web Config e **Definições de segurança de rede** > **SSL/TLS** > **Certificado**.
2. Clique em **Actualizar**.
3. Introduza **Nome comum**.

   Introduza um endereço IP ou um identificador, como um nome FQDN, para o scanner. Pode introduzir entre 1 e 128 caracteres.

   ***Nota:***
   *Pode separar um nome distinto (CN) com vírgulas.*

4. Especifique um prazo de validade para o certificado.




5. Clique em **Seguinte**.

   É apresentada uma mensagem de confirmação.

6. Clique em **OK**.

   O scanner está atualizado.

***Nota:***
*Clique em **Confirmar** para verificar as informações do certificado.*

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

# Configurar o Certificado CA

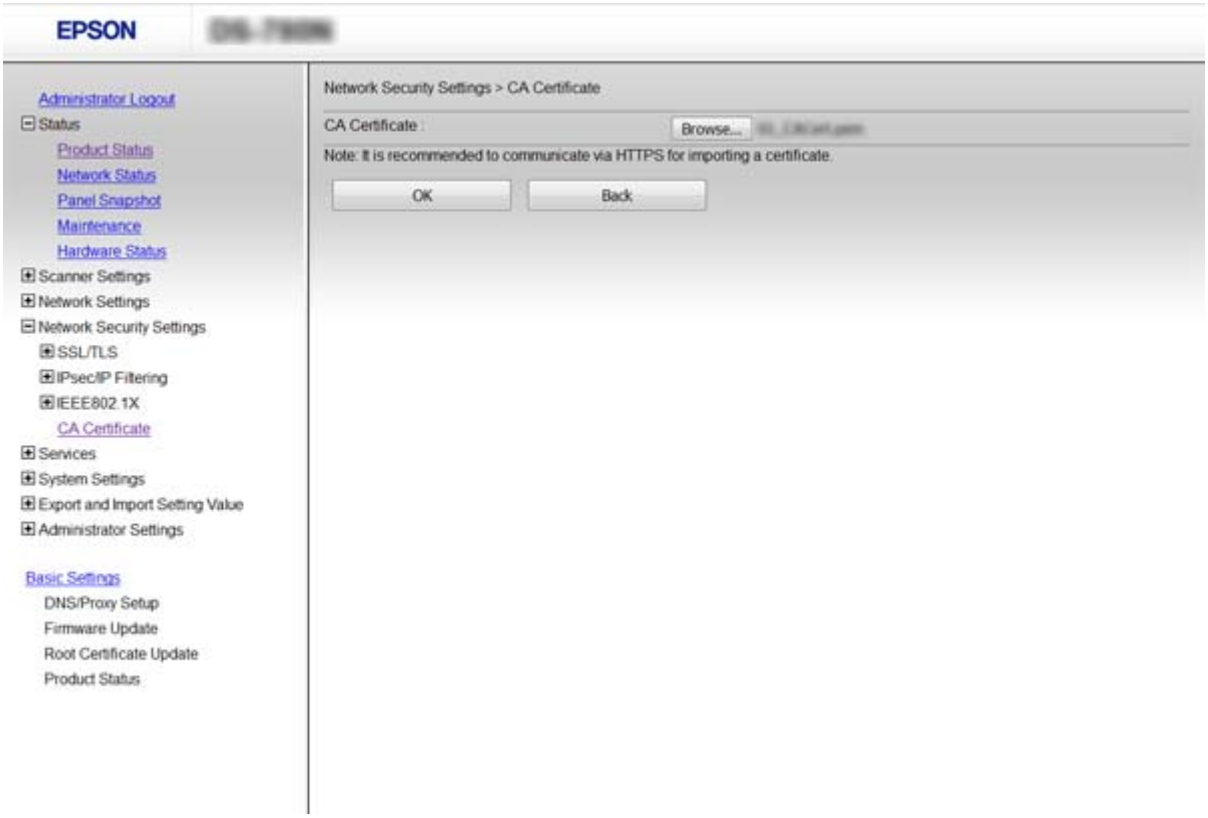
Pode importar, apresentar, eliminar um Certificado CA.

## Importar um Certificado CA

1. Selecione Web Config e, em seguida, **Definições de segurança de rede** > **Certificado CA**.

2. Clique em **Importar**.

3. Especifique o Certificado CA que pretende importar.




4. Clique em **OK**.

Quando a importação estiver concluída, regressa ao ecrã do **Certificado CA** e o Certificado CA é apresentado importado.

### Informações relacionadas

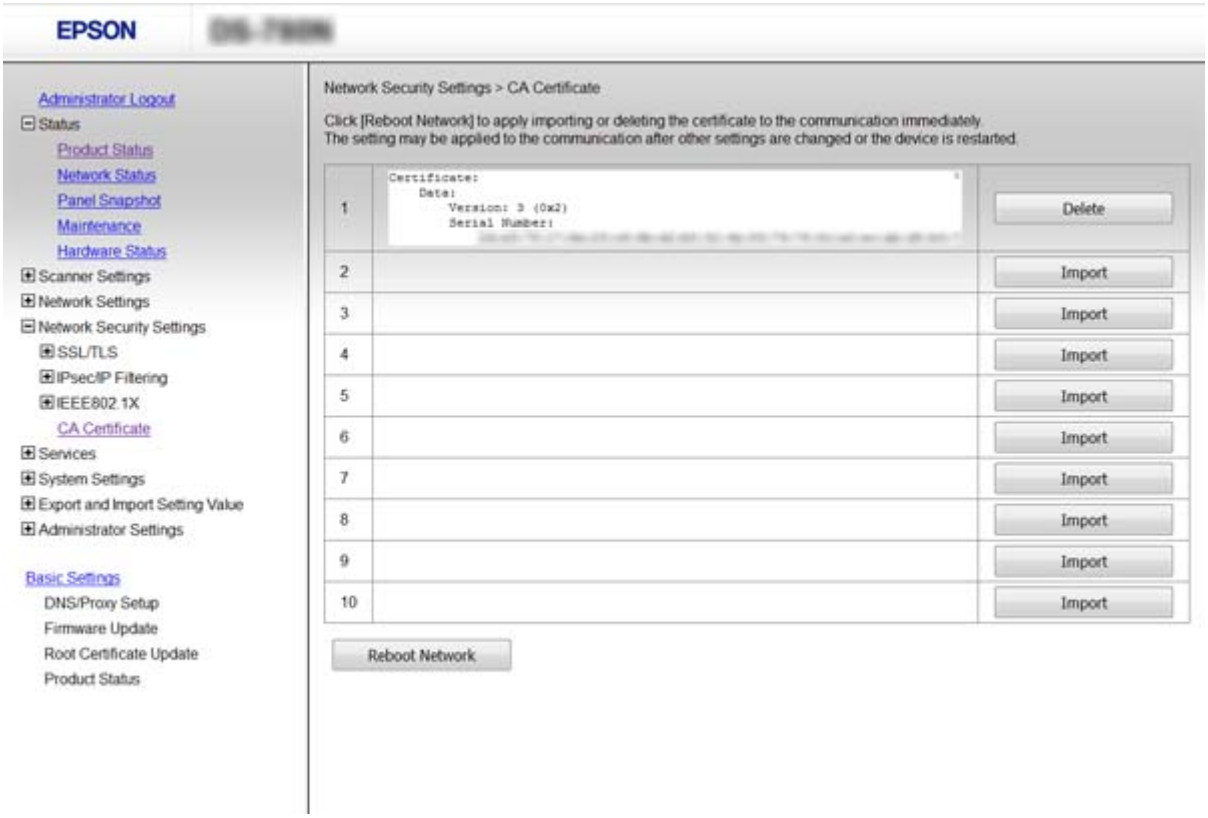
➡ "Aceder ao Web Config" na página 23

## Eliminar um Certificado CA

Pode eliminar o Certificado CA importado.

1. Selecione Web Config e, em seguida, **Definições de segurança de rede** > **Certificado CA**.

2. Clique em **Eliminar** junto ao Certificado CA que pretende eliminar.




3. Confirme que pretende eliminar o certificado na mensagem apresentada.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

# Comunicações encriptada usando filtro IPsec/IP

## Sobre a IPsec/Filtro de IP

Se o scanner suportar a filtragem IPsec/IP, pode filtrar o tráfego com base em endereços IP, serviços e porta. Através da combinação da filtragem, pode configurar o scanner para aceitar ou bloquear clientes especificados e dados especificados. Além disso, pode melhor o nível de segurança utilizando um IPsec.

Para filtrar o tráfego, configure a política predefinida. A política predefinida aplica-se a todos os utilizadores ou grupos que estabelecem ligação com o scanner. Para exercer um controlo mais preciso sobre os utilizadores e grupos de utilizadores, configure políticas de grupo. Uma política de grupo consiste em uma ou mais regras que se aplicam a um utilizador ou grupo de utilizadores. O scanner controla pacotes IP que correspondem a políticas configuradas. Os pacotes IP são autenticados pela ordem de uma política de grupo de 1 a 10 e, depois, uma política predefinida.

***Nota:***
*Computadores com Windows Vista ou posterior ou Windows Server 2008 ou posterior são compatíveis com IPsec.*

# Configurar a Política predefinida

1. Selecionar Web Config e **Definições de segurança de rede** > **IPsec/Filtro de IP** > **Básico**.
2. Introduza um valor para cada item.
3. Clique em **Seguinte**.

   É apresentada uma mensagem de confirmação.
4. Clique em **OK**.

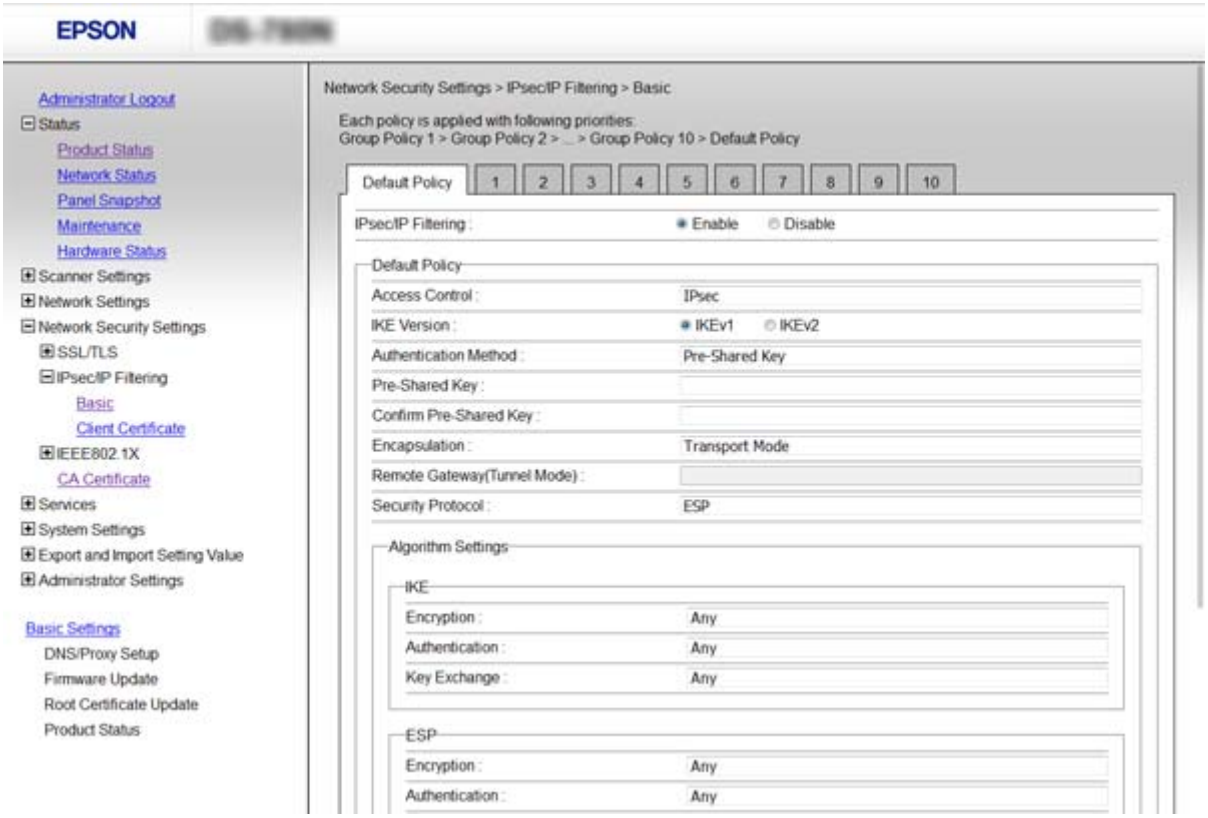
   O scanner está atualizado.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

➡ "Itens de definição da Política predefinida" na página 72

## Itens de definição da Política predefinida




| Itens | Definições e explicação |
|---|---|
| IPsec/Filtro de IP | Pode ativar ou desativar uma função de filtragem IPsec/IP. |

## Configurações de segurança avançada para empresas

| Itens | Definições e explicação | |
|---|---|---|
| Controlo de acesso | Configure um método de controlo para o tráfego de pacotes IP. | |
| | Permitir acesso | Selecione para permitir que os pacotes IP configurados sejam transmitidos. |
| | Recusar acesso | Selecione para não permitir que os pacotes IP configurados sejam transmitidos. |
| | IPsec | Selecione para permitir que os pacotes IPsec configurados sejam transmitidos. |
| Versão de IKE | Selecione IKEv1 ou IKEv2 para a versão IKE.<br>Selecione um deles de acordo com o dispositivo ao qual o scanner está ligado. | |
| IKEv1 | Os itens que se seguem são exibidos ao selecionar **IKEv1** para **Versão de IKE**. | |
| | Método de autenticação | Para selecionar **Certificado**, terá de obter e importar um certificado CA assinado antecipadamente. |
| | Chave pré-partilhada | Se selecionar **Chave pré-partilhada** para **Método de autenticação**, introduza uma chave pré-partilhada com entre 1 e 127 caracteres. |
| | Confirmar chave pré-partilhada | Introduza o código que configurou para confirmação. |
| IKEv2 | Os itens que se seguem são exibidos ao selecionar **IKEv2** para **Versão de IKE**. | |
| Local | Método de autenticação | Para selecionar **Certificado**, terá de obter e importar um certificado CA assinado antecipadamente. |
| | Tipo de ID | Selecione o tipo de ID para o scanner. |
| | ID | Introduza o ID do scanner que corresponde ao tipo de ID.<br>Não é possível usar "@", "#", e "=" como primeiro caracter.<br>**Nome distinto**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). É necessário incluir "=".<br>**Endereço IP**: Introduza o formato IPv4 ou IPv6.<br>**FQDN**: Introduza uma combinação entre 1 e 255 caracteres utilizando A–Z, a–z, 0–9, "-" e ponto final (.).<br>**Ender. de E-mail**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). É necessário incluir "@".<br>**ID da chave**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). |
| | Chave pré-partilhada | Se selecionar **Chave pré-partilhada** para **Método de autenticação**, introduza uma chave pré-partilhada com entre 1 e 127 caracteres. |
| | Confirmar chave pré-partilhada | Introduza o código que configurou para confirmação. |

**Configurações de segurança avançada para empresas**

| Itens | Definições e explicação | |
|---|---|---|
| Remota | Método de autenticação | Para selecionar **Certificado**, terá de obter e importar um certificado CA assinado antecipadamente. |
| | Tipo de ID | Selecione o tipo de ID para o dispositivo que pretende autenticar. |
| | ID | Introduza o ID do scanner que corresponde ao tipo de ID.<br>Não é possível usar "@", "#", e "=" como primeiro caracter.<br>**Nome distinto**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). É necessário incluir "=".<br>**Endereço IP**: Introduza o formato IPv4 ou IPv6.<br>**FQDN**: Introduza uma combinação entre 1 e 255 caracteres utilizando A–Z, a–z, 0–9, "-" e ponto final (.).<br>**Ender. de E-mail**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). É necessário incluir "@".<br>**ID da chave**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). |
| | Chave pré-partilhada | Se selecionar **Chave pré-partilhada** para **Método de autenticação**, introduza uma chave pré-partilhada com entre 1 e 127 caracteres. |
| | Confirmar chave pré-partilhada | Introduza o código que configurou para confirmação. |
| Encapsulamento | Se selecionar **IPsec** para **Controlo de acesso**, terá de configurar um modo de encapsulamento. | |
| | Modo de transporte | Se utilizar apenas o scanner na mesma LAN, selecione esta opção. Os pacotes IP de camada 4 ou posterior são encriptados. |
| | Modo de túnel | Se usa o scanner na rede com ligação à Internet através de, por exemplo, IPsec-VPN, selecione esta opção. O cabeçalho e os dados dos pacotes IP são encriptados. |
| Endereço gateway remoto | Se selecionar **Modo de túnel** para **Encapsulamento**, introduza um endereço de gateway com entre 1 e 39 caracteres. | |
| Protocolo de segurança | **IPsec** para **Controlo de acesso**, selecione uma opção. | |
| | ESP | Selecione para garantir a integridade de uma autenticação e dados, e de dados encriptados. |
| | AH | Selecione para garantir a integridade de uma autenticação e dados. Mesmo que encriptar dados seja proibido, pode utilizar o IPsec. |
| Definições de algoritmo | | |
| IKE | Encriptação | Selecione o algoritmo de encriptação para IKE.<br>Os itens variam de acordo com a versão de IKE. |
| | Autenticação | Selecione o algoritmo de autenticação para IKE. |
| | Intercâmbio de chaves | Selecione o algoritmo de troca palavra-passe para IKE.<br>Os itens variam de acordo com a versão de IKE. |

| Itens | Definições e explicação | |
|---|---|---|
| ESP | Encriptação | Selecione o algoritmo de encriptação para ESP.<br>Disponível quando **ESP** estiver selecionado para **Protocolo de segurança**. |
| | Autenticação | Selecione o algoritmo de autenticação para ESP.<br>Disponível quando **ESP** estiver selecionado para **Protocolo de segurança**. |
| AH | Autenticação | Selecione o algoritmo de encriptação para AH.<br>Disponível quando **AH** estiver selecionado para **Protocolo de segurança**. |

### Informações relacionadas

➡ "Configurar a Política predefinida" na página 72

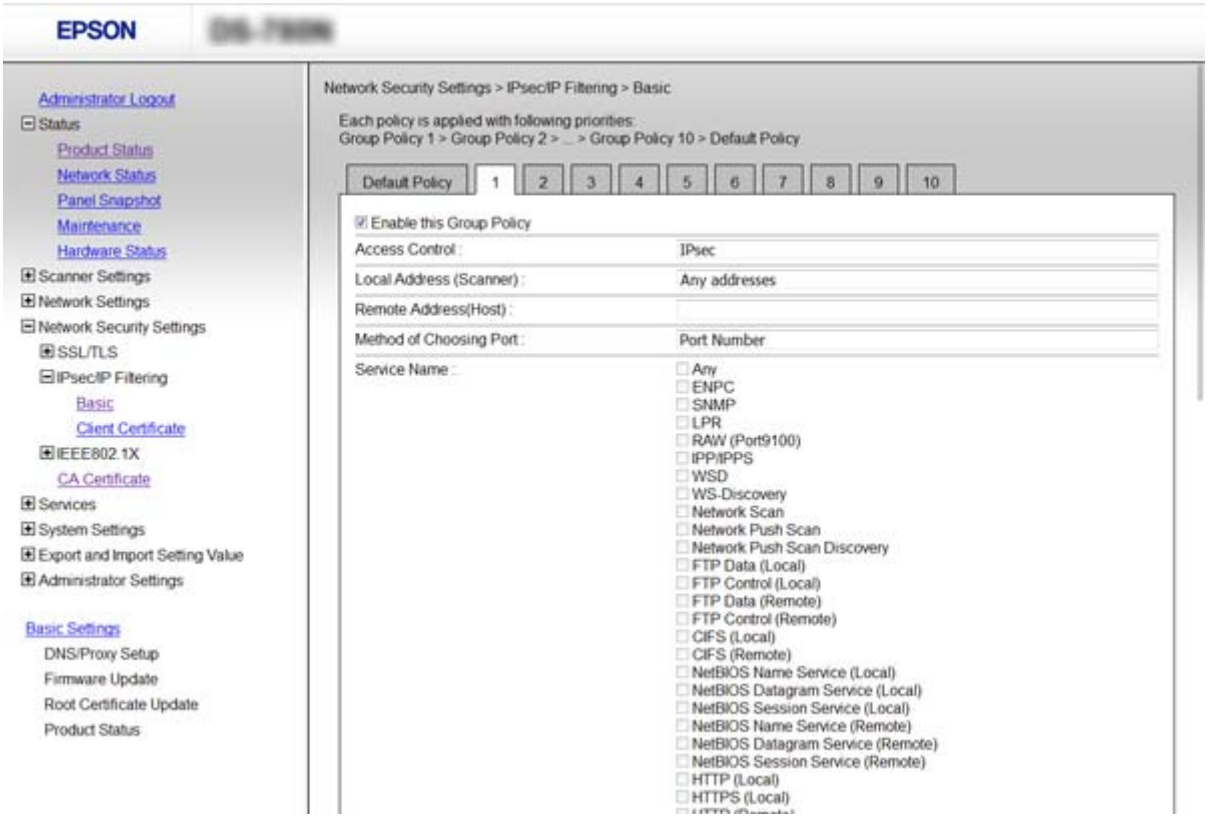
## Configurar a Política do grupo

1. Selecionar Web Config e **Definições de segurança de rede** > **IPsec/Filtro de IP** > **Básico**.
2. Clique num guia numerado que deseja configurar.
3. Introduza um valor para cada item.
4. Clique em **Seguinte**.
   É apresentada uma mensagem de confirmação.
5. Clique em **OK**.
   O scanner está atualizado.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23
➡ "Itens de definição da Política do grupo" na página 76

# Itens de definição da Política do grupo




| Itens | Definições e explicação | |
|---|---|---|
| Ativar esta Política de Grupo | Pode ativar ou desativar uma política de grupo. | |
| Controlo de acesso | Configure um método de controlo para o tráfego de pacotes IP. | |
| | Permitir acesso | Selecione para permitir que os pacotes IP configurados sejam transmitidos. |
| | Recusar acesso | Selecione para não permitir que os pacotes IP configurados sejam transmitidos. |
| | IPsec | Selecione para permitir que os pacotes IPsec configurados sejam transmitidos. |
| Endereço local (Digitalizador) | Selecione um endereço IPv4 ou IPv6 que corresponde ao seu ambiente de rede. Se o endereço de IP for atribuído automaticamente, pode selecionar **Utilizar endereço IPv4 obtido automaticamente**. | |
| Endereço remoto (Anfitrião) | Introduza o endereço IP de um dispositivo para controlar o acesso. O endereço IP deve ter 43 caracteres ou menos. Se não introduzir um endereço IP válido, todos os endereços são controlados.<br>***Nota:***<br>*Se um endereço IP for atribuído automaticamente (ou seja, atribuído pelo DHCP), a ligação pode não estar disponível. Configure um endereço IP estático.* | |
| Método de selecção da porta | Selecione um método para definir as portas. | |
| Nome do serviço | Se selecionar **Nome do serviço** para **Método de selecção da porta**, selecione uma opção. | |

**Configurações de segurança avançada para empresas**

| Itens | Definições e explicação | |
|---|---|---|
| Protocolo de transporte | Se selecionar **Número da porta** para **Método de selecção da porta**, terá de configurar um modo de encapsulamento. | |
| | Qualquer protocolo | Selecione essa opção para controlar todos os tipos de protocolo. |
| | TCP | Selecione para controlar os dados de unicast. |
| | UDP | Selecione para controlar os dados de difusão e multicast. |
| | ICMPv4 | Selecione para controlar o comando ping. |
| Porta local | Se selecionou **Número da porta** para **Método de selecção da porta** e se selecionou **TCP** ou **UDP** para **Protocolo de transporte**, introduza os números de porta para controlar os pacotes recebidos, separados por vírgulas. Pode introduzir um máximo de 10 números de portas.<br>Exemplo: 20,80,119,5220<br>Se não introduzir um número de porta, todas as portas são controladas. | |
| Porta remota | Se selecionou **Número da porta** para **Método de selecção da porta** e se selecionar **TCP** ou **UDP** para **Protocolo de transporte**, introduza os números de porta para controlar os pacotes enviados, separados por vírgulas. Pode introduzir um máximo de 10 números de portas.<br>Exemplo: 25,80,143,5220<br>Se não introduzir um número de porta, todas as portas são controladas. | |
| Versão de IKE | Selecione IKEv1 ou IKEv2 para a versão IKE.<br>Selecione um deles de acordo com o dispositivo ao qual o scanner está ligado. | |
| IKEv1 | Os itens que se seguem são exibidos ao selecionar **IKEv1** para **Versão de IKE**. | |
| | Método de autenticação | Se selecionar **IPsec** para **Controlo de acesso**, selecione uma opção. O certificado utilizado está de acordo com uma política predefinida. |
| | Chave pré-partilhada | Se selecionar **Chave pré-partilhada** para **Método de autenticação**, introduza uma chave pré-partilhada com entre 1 e 127 caracteres. |
| | Confirmar chave pré-partilhada | Introduza o código que configurou para confirmação. |
| IKEv2 | Os itens que se seguem são exibidos ao selecionar **IKEv2** para **Versão de IKE**. | |

## Configurações de segurança avançada para empresas

| Itens | Definições e explicação | |
|---|---|---|
| Local | Método de autenticação | Se selecionar **IPsec** para **Controlo de acesso**, selecione uma opção. O certificado utilizado está de acordo com uma política predefinida. |
| | Tipo de ID | Selecione o tipo de ID para o scanner. |
| | ID | Introduza o ID do scanner que corresponde ao tipo de ID.<br>Não é possível usar "@", "#", e "=" como primeiro caracter.<br>**Nome distinto**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). É necessário incluir "=".<br>**Endereço IP**: Introduza o formato IPv4 ou IPv6.<br>**FQDN**: Introduza uma combinação entre 1 e 255 caracteres utilizando A–Z, a–z, 0–9, "-" e ponto final (.).<br>**Ender. de E-mail**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). É necessário incluir "@".<br>**ID da chave**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). |
| | Chave pré-partilhada | Se selecionar **Chave pré-partilhada** para **Método de autenticação**, introduza uma chave pré-partilhada com entre 1 e 127 caracteres. |
| | Confirmar chave pré-partilhada | Introduza o código que configurou para confirmação. |
| Remota | Método de autenticação | Se selecionar **IPsec** para **Controlo de acesso**, selecione uma opção. O certificado utilizado está de acordo com uma política predefinida. |
| | Tipo de ID | Selecione o tipo de ID para o dispositivo que pretende autenticar. |
| | ID | Introduza o ID do scanner que corresponde ao tipo de ID.<br>Não é possível usar "@", "#", e "=" como primeiro caracter.<br>**Nome distinto**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). É necessário incluir "=".<br>**Endereço IP**: Introduza o formato IPv4 ou IPv6.<br>**FQDN**: Introduza uma combinação entre 1 e 255 caracteres utilizando A–Z, a–z, 0–9, "-" e ponto final (.).<br>**Ender. de E-mail**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). É necessário incluir "@".<br>**ID da chave**: Introduza 1 a 128 caracteres de 1-byte ASCII (0x20 a 0x7E). |
| | Chave pré-partilhada | Se selecionar **Chave pré-partilhada** para **Método de autenticação**, introduza uma chave pré-partilhada com entre 1 e 127 caracteres. |
| | Confirmar chave pré-partilhada | Introduza o código que configurou para confirmação. |

**Configurações de segurança avançada para empresas**

| Itens | Definições e explicação | |
|---|---|---|
| Encapsulamento | Se selecionar **IPsec** para **Controlo de acesso**, terá de configurar um modo de encapsulamento. | |
| | Modo de transporte | Se utilizar apenas o scanner na mesma LAN, selecione esta opção. Os pacotes IP de camada 4 ou posterior são encriptados. |
| | Modo de túnel | Se usa o scanner na rede com ligação à Internet através de, por exemplo, IPsec-VPN, selecione esta opção. O cabeçalho e os dados dos pacotes IP são encriptados. |
| Endereço gateway remoto | Se selecionar **Modo de túnel** para **Encapsulamento**, introduza um endereço de gateway com entre 1 e 39 caracteres. | |
| Protocolo de segurança | Se selecionar **IPsec** para **Controlo de acesso**, selecione uma opção. | |
| | ESP | Selecione para garantir a integridade de uma autenticação e dados, e de dados encriptados. |
| | AH | Selecione para garantir a integridade de uma autenticação e dados. Mesmo que encriptar dados seja proibido, pode utilizar o IPsec. |
| Definições de algoritmo | | |
| IKE | Encriptação | Selecione o algoritmo de encriptação para IKE.<br>Os itens variam de acordo com a versão de IKE. |
| | Autenticação | Selecione o algoritmo de autenticação para IKE. |
| | Intercâmbio de chaves | Selecione o algoritmo de troca palavra-passe para IKE.<br>Os itens variam de acordo com a versão de IKE. |
| ESP | Encriptação | Selecione o algoritmo de encriptação para ESP.<br>Disponível quando **ESP** estiver selecionado para **Protocolo de segurança**. |
| | Autenticação | Selecione o algoritmo de autenticação para ESP.<br>Disponível quando **ESP** estiver selecionado para **Protocolo de segurança**. |
| AH | Autenticação | Selecione o algoritmo de autenticação para AH.<br>Disponível quando **AH** estiver selecionado para **Protocolo de segurança**. |

## Informações relacionadas

➡ “Configurar a Política do grupo” na página 75

➡ “Combinação de Endereço local (Digitalizador) e Endereço remoto (Anfitrião) em Política do grupo” na página 80

➡ “Referências do nome do serviço da política de grupo” na página 80

## Combinação de Endereço local (Digitalizador) e Endereço remoto (Anfitrião) em Política do grupo

| | | Definir Endereço local (Digitalizador) | | |
|---|---|---|---|---|
| | | IPv4 | IPv6*2 | Quaisquer endereços*3 |
| **Definir Endereço remoto (Anfitrião)** | IPv4*1 | ✓ | – | ✓ |
| | IPv6*1*2 | – | ✓ | ✓ |
| | Blank | ✓ | ✓ | ✓ |

*1 Se **IPsec** for selecionado para **Controlo de acesso**, não pode especificar na extensão de um prefixo.

*2 Se **IPsec** for selecionado para **Controlo de acesso**, pode selecionar um endereço de ligação local (fe80::) mas a política de grupo será desativada.

*3 Exceto endereços de ligações locais IPv6.

## Referências do nome do serviço da política de grupo

***Nota:***
*Os serviços não disponíveis são exibidos, mas não podem ser selecionados.*

| Nome de Serviço | Tipo de protocolo | Número de porta local | Número de porta remota | Funcionalidades controladas |
|---|---|---|---|---|
| Quaisquer | – | – | – | Todos os serviços |
| ENPC | UDP | 3289 | Qualquer porta | Procurar um scanner a partir de aplicações tais como EpsonNet Config e controlador do scanner |
| SNMP | UDP | 161 | Qualquer porta | Adquirir e configurar o MIB a partir de aplicações tais como EpsonNet Config e controlador do scanner Epson |
| WSD | TCP | Qualquer porta | 5357 | Controlo do WSD |
| WS-Discovery | UDP | 3702 | Qualquer porta | Procurar um scanner a partir do WSD |
| Network Scan | TCP | 1865 | Qualquer porta | Reencaminhar dados de digitalização a partir do Document Capture Pro |
| Network Push Scan Discovery | UDP | 2968 | Qualquer porta | Procurar um computador a partir do scanner. |
| Network Push Scan | TCP | Qualquer porta | 2968 | Adquirir informações da tarefa de digitalização push a partir de Document Capture Pro ou Document Capture |
| HTTP (Local) | TCP | 80 | Qualquer porta | Servidor HTTP(S) (reencaminhar dados de Web Config e WSD) |
| HTTPS (Local) | TCP | 443 | Qualquer porta | |

| Nome de Serviço | Tipo de protocolo | Número de porta local | Número de porta remota | Funcionalidades controladas |
|---|---|---|---|---|
| HTTP (Remoto) | TCP | Qualquer porta | 80 | Cliente HTTP(S) (comunicação entre a atualização de firmware e atualização de certificado root) |
| HTTPS (Remoto) | TCP | Qualquer porta | 443 | |

# Exemplos de configuração da IPsec/Filtro de IP

### Receber apenas pacotes IPsec

Este exemplo ilustra apenas a configuração de uma política predefinida.

**Política predefinida**:

❏ **IPsec/Filtro de IP**: **Activar**

❏ **Controlo de acesso**: **IPsec**

❏ **Método de autenticação**: **Chave pré-partilhada**

❏ **Chave pré-partilhada**: introduza até 127 caracteres.

**Política do grupo**:

Não configure.

### Aceitar a digitalização usando Epson Scan 2 e definições do scanner

Este exemplo permite comunicações de dados da digitalização e configuração do scanner de serviços especificados.

**Política predefinida**:

❏ **IPsec/Filtro de IP**: **Activar**

❏ **Controlo de acesso**: **Recusar acesso**

**Política do grupo**:

❏ **Ativar esta Política de Grupo**: selecione a caixa.

❏ **Controlo de acesso**: **Permitir acesso**

❏ **Endereço remoto (Anfitrião)**: endereço IP de um cliente

❏ **Método de selecção da porta**: **Nome do serviço**

❏ **Nome do serviço**: assinale a caixa **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** e **HTTPS (Local)**.

### Receber acesso apenas de um endereço IP especificado

Este exemplo permite que um endereço IP especificado aceda ao scanner.

**Política predefinida**:

❏ **IPsec/Filtro de IP**: **Activar**

❏ **Controlo de acesso**:**Recusar acesso**

**Política do grupo**:

❏ **Ativar esta Política de Grupo**: selecione a caixa.

❏ **Controlo de acesso**: **Permitir acesso**

❏ **Endereço remoto (Anfitrião)**: endereço IP do cliente de um administrador

***Nota:***
*Independentemente da configuração da política, o cliente conseguirá aceder e configurar o scanner.*

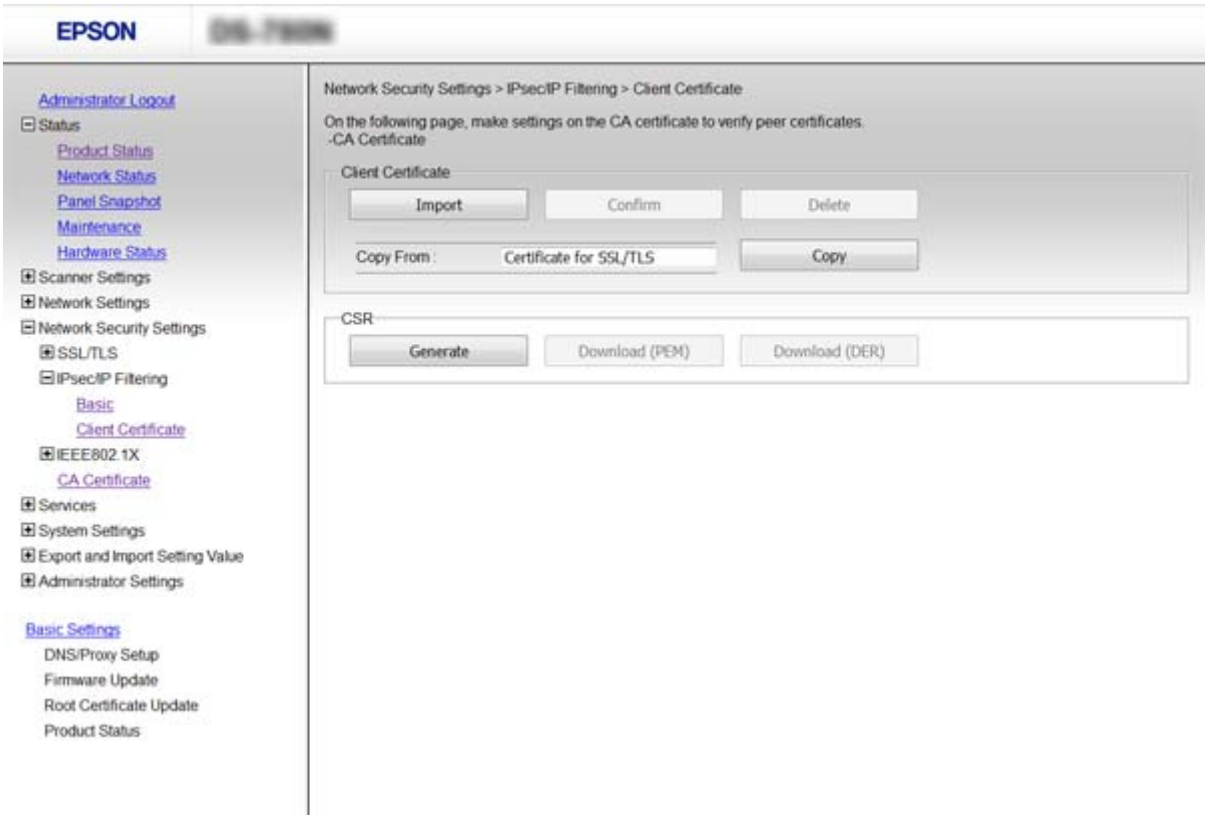
# Configurar um certificado para IPsec/Filtro de IP

Configurar o Certificado de Cliente para Filtragem IPsec/IP. Se quiser configurar a autoridade de certificação, aceda a **Certificado CA**.

1. Selecionar Web Config e **Definições de segurança de rede** > **IPsec/Filtro de IP** > **Certificado do cliente**.

2. Importe o certificado no **Certificado do cliente**.

   Se já tiver importado um certificado publicado por uma Autoridade de Certificação em IEEE802.1X ou SSL/TLS, pode copiar o certificado e usá-lo na Filtragem IPsec/IP. Para copiar, selecione o certificado em **Copiar de** e clique em **Copiar**.




### Informações relacionadas

➡ “Aceder ao Web Config” na página 23

➡ “Obter e importar um certificado CA assinado” na página 64

# Utilizar o protocolo SNMPv3

## Sobre o SNMPv3

O SNMP é um protocolo que realiza a monitorização e controlo da recolha de informações dos dispositivos que estão ligados na rede. O SNMPv3 é a versão melhorada do recurso de segurança de gestão.

Ao usar o SNMPv3, a monitorização do estado e alterações das definições da comunicação SNMP (pacote) podem ser autenticadas e encriptadas para proteger a comunicação SNMP (pacote) de riscos de rede, tais como escutas telefónicas, falsificação e manipulação.

## Configurar o SNMPv3

Se o scanner for compatível com o protocolo SNMPv3, pode monitorizar e controlar os acessos ao scanner.

1. Selecionar Web Config e **Serviços** > **Protocolo**.
2. Introduza um valor para cada item **Definições de SNMPv3**.
3. Clique em **Seguinte**.

   É apresentada uma mensagem de confirmação.
4. Clique em **OK**.

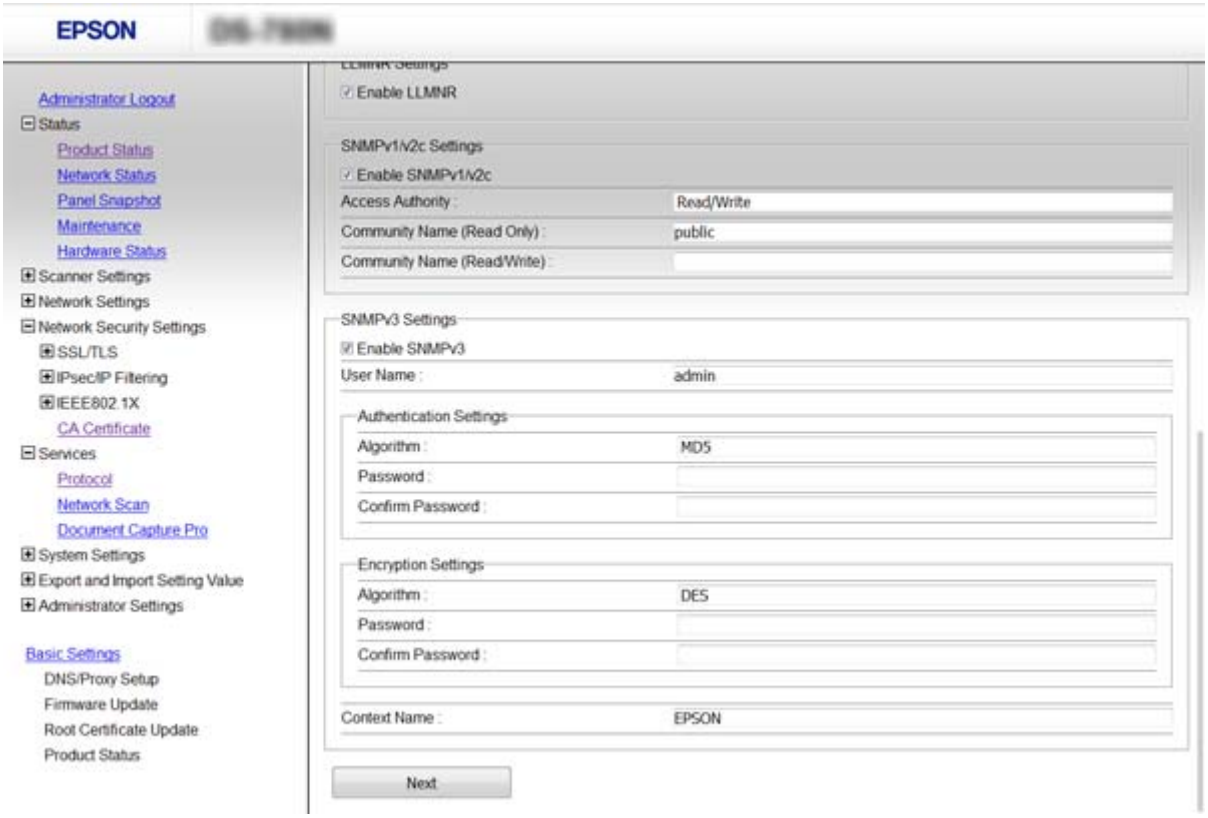
   O scanner está atualizado.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

➡ "Itens de definição SNMPv3" na página 84

# Itens de definição SNMPv3




| Itens | Definições e explicação |
|---|---|
| Ativar SNMPv3 | O protocolo SNMPv3 é activado quando a caixa é seleccionada. |
| Nome de Util. | Introduza entre 1 e 32 caracteres utilizando caracteres de 1 byte. |
| Definições de autenticação | |
| Algoritmo | Seleccione um algoritmo para uma autenticação. |
| Palavra-passe | Introduza entre 8 e 32 caracteres em ASCII (0x20-0x7E). |
| Confirmar palavra-passe | Introduza a palavra-passe que configurou para confirmação. |
| Definições de encriptação | |
| Algoritmo | Seleccione um algoritmo para uma encriptação. |
| Palavra-passe | Introduza entre 8 e 32 caracteres em ASCII (0x20-0x7E). |
| Confirmar palavra-passe | Introduza a palavra-passe que configurou para confirmação. |
| Nome do contexto | Introduza entre 1 e 32 caracteres utilizando caracteres de 1 byte. |

### Informações relacionadas

➡ “Configurar o SNMPv3” na página 83

# Ligar o scanner a uma rede IEEE802.1X

## Configurar uma rede IEEE802.1X

Se o scanner suportar IEEE802.1X, pode utilizá-lo numa rede com autenticação que esteja ligada a um servidor RADIUS e a um concentrador como autenticador.

1. Selecionar Web Config e **Definições de segurança de rede** > **IEEE802.1X** > **Básico**.
2. Introduza um valor para cada item.
3. Clique em **Seguinte**.

   É apresentada uma mensagem de confirmação.
4. Clique em **OK**.

   O scanner está atualizado.

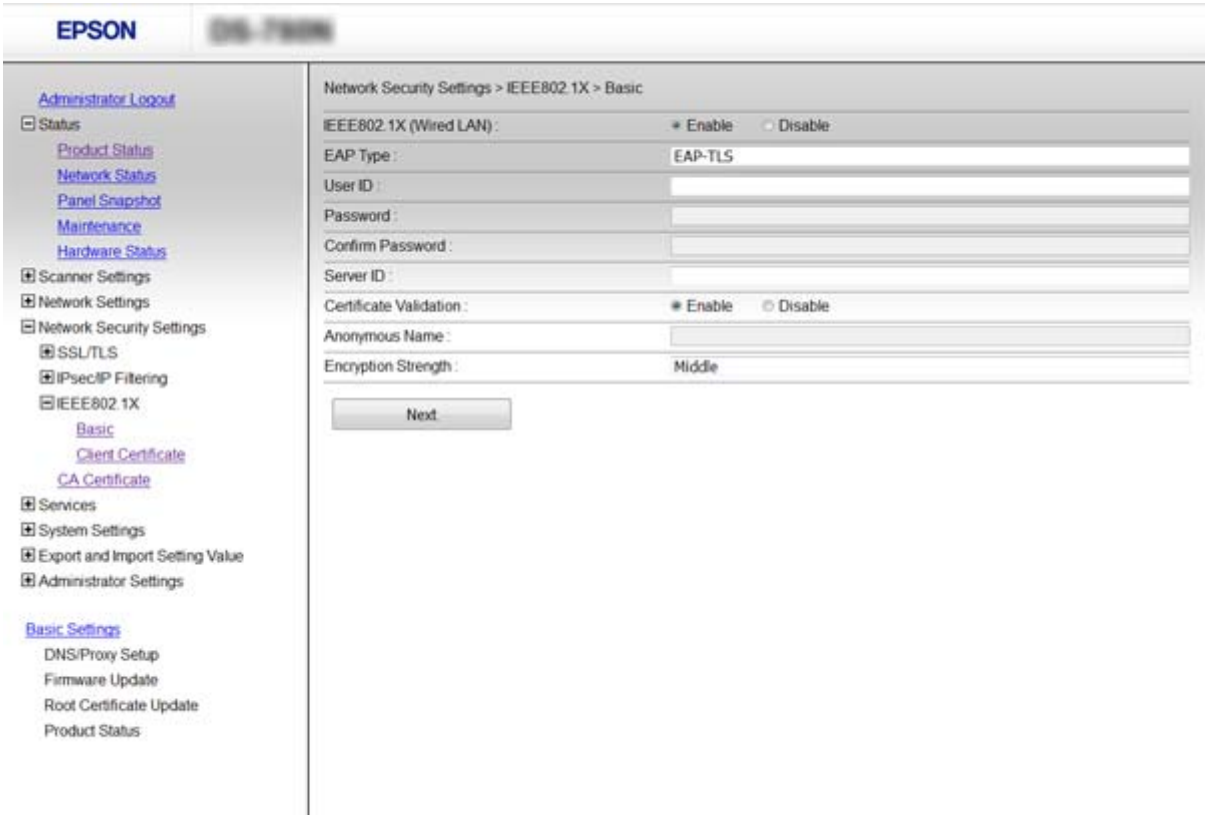
### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

➡ "Itens de definição da rede IEEE802.1X" na página 85

➡ "Não é possível aceder à impressora ou ao scanner após configurar IEEE802.1X" na página 90

## Itens de definição da rede IEEE802.1X



**Configurações de segurança avançada para empresas**

| Itens | Definições e explicação | |
|---|---|---|
| IEEE802.1X (LAN com fios) | Pode ativar ou desativar definições na página (**IEEE802.1X** > **Básico**) para IEEE802.1X (LAN com fios). | |
| Tipo EAP | Selecione uma opção para um método de autenticação entre o scanner e um servidor RADIUS. | |
| | EAP-TLS | Necessita de obter e importar um certificado CA assinado. |
| | PEAP-TLS | |
| | PEAP/MSCHAPv2 | Terá de configurar uma palavra-passe. |
| ID do utilizador | Configure uma ID (identificação) a utilizar numa autenticação de um servidor RADIUS.<br>Introduza entre 1 a 128 caracteres ASCII (0x20 a 0x7E) de 1 byte. | |
| Palavra-passe | Configure uma palavra-passe para autenticar o scanner.<br>Introduza entre 1 a 128 caracteres ASCII (0x20 a 0x7E) de 1 byte. Se estiver a utilizar um servidor Windows como servidor RADIUS, pode introduzir até 127 caracteres. | |
| Confirmar palavra-passe | Introduza a palavra-passe que configurou para confirmação. | |
| ID do servidor | Pode configurar uma ID do servidor para autenticar junto de um servidor RADIUS. O autenticador verifica se está ou não incluída uma ID de servidor no campo subject/subjectAltName de um certificado de servidor que é enviado por um servidor RADIUS.<br>Introduza entre 1 a 128 caracteres ASCII (0x20 a 0x7E) de 0 byte. | |
| Validação do certificado | Pode definir a validação do certificado independentemente do método de autenticação. Importe o certificado no **Certificado CA**. | |
| Nome anónimo | Se selecionar **PEAP-TLS** ou **PEAP/MSCHAPv2** para **Método de autenticação**, pode configurar um nome anónimo em vez de uma ID de utilizador para uma fase 1 de uma autenticação PEAP.<br>Introduza entre 1 a 128 caracteres ASCII (0x20 a 0x7E) de 0 byte. | |
| Força da encriptação | Pode selecionar uma das opções seguintes: | |
| | Alta | AES256/3DES |
| | Médio | AES256/3DES/AES128/RC4 |

### Informações relacionadas

➡ "Configurar uma rede IEEE802.1X" na página 85

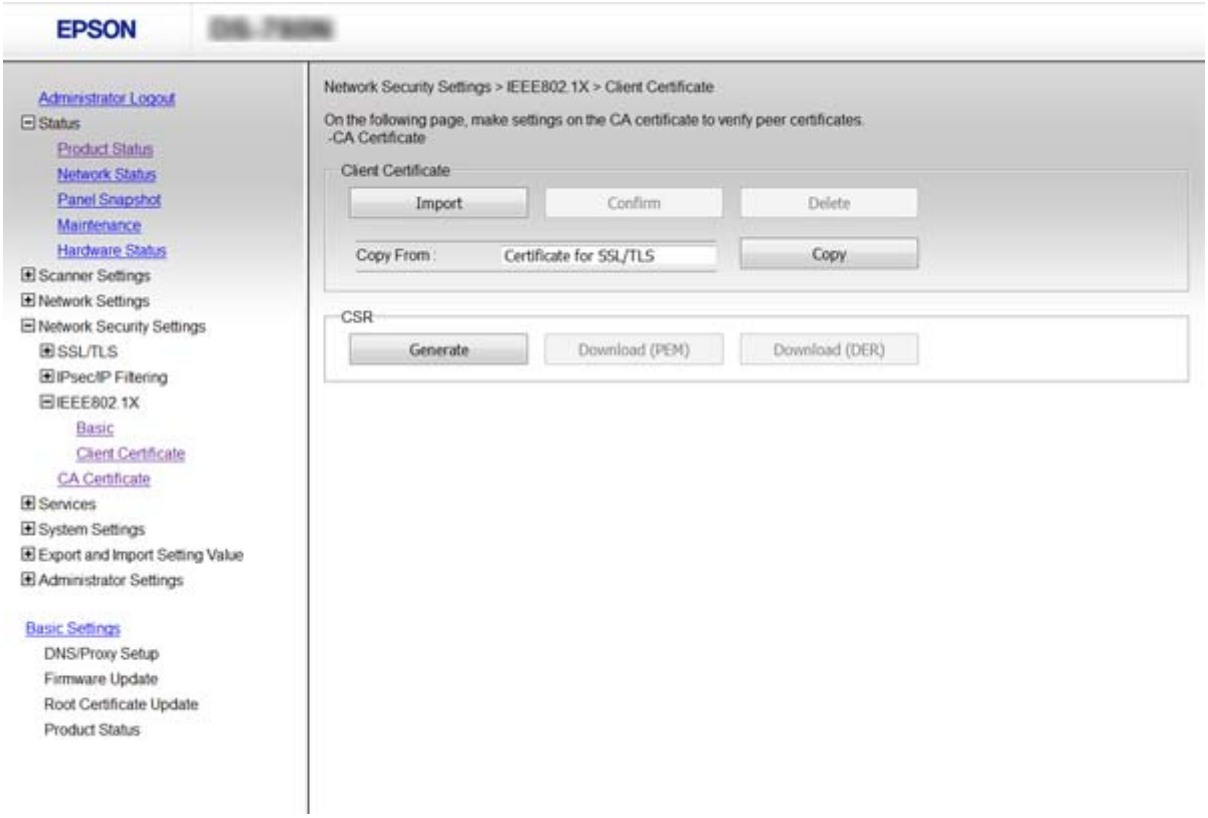
# Configurar um certificado para IEEE802.1X

Configurar o Certificado de Cliente para IEEE802.1X. Se quiser configurar a autoridade de certificação, aceda a **Certificado CA**.

1. Selecionar Web Config e **Definições de segurança de rede** > **IEEE802.1X** > **Certificado do cliente**.

2. Introduza um certificado no **Certificado do cliente**.

   Pode copiar o certificado se este tiver sido publicado por uma Autoridade de Certificação. Para copiar, selecione o certificado em **Copiar de** e clique em **Copiar**.




**Informações relacionadas**

➡ "Aceder ao Web Config" na página 23

➡ "Obter e importar um certificado CA assinado" na página 64

# Resolução de problemas para segurança avançada

## Recuperação de definições de segurança

Ao estabelecer um ambiente altamente seguro como a filtragem IPsec/IP ou IEEE802.1X, pode não ser capaz de comunicar com dispositivos devido a configurações incorretas ou problemas com o dispositivo ou servidor. Neste caso, restaure as configurações de segurança para fazer as configurações para o dispositivo novo ou para permitir a utilização temporária.

### Desativar a função de segurança usando o painel de controlo

É possível desativar o filtro IPsec/IP ou IEEE802.1X usando o painel de controlo do scanner.

1. Toque em **Definições** > **Definições de rede**.

2. Toque em **Alterar definições**.
3. Selecione os itens que pretende desativar.
   - ❏ **IPsec/Filtro de IP**
   - ❏ **IEEE802.1X**
4. Quando for apresentada uma mensagem de conclusão, toque em **Avan**.

## Restaurar a função de segurança usando o Web Config

Em IEEE802.1X, os dispositivos podem não ser reconhecidos na rede. Nesse caso, desative a função usando o painel de controlo do scanner.

Para filtragem IPsec/IP, pode desativar a função se conseguir aceder ao dispositivo a partir do computador.

### *Desativar o filtro IPsec/IP usando Web Config*

1. Aceda a Web Config e selecione **Definições de segurança de rede** > **IPsec/Filtro de IP** > **Básico**.
2. Selecione **Desactivar** para **IPsec/Filtro de IP** em **Política predefinida**.
3. Clique em **Seguinte**, e a seguir elimine **Ativar esta Política de Grupo** para todas as políticas de grupo.
4. Clique em **OK**.

#### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

# Problemas de utilização de funções de segurança da rede

## Não se lembra de uma chave pré-partilhada

#### Volte a configurar a chave utilizando o Web Config.

Para mudar a chave, aceda a Web Config e selecione **Definições de segurança de rede** > **IPsec/Filtro de IP** > **Básico** > **Política predefinida** ou **Política do grupo**.

Ao alterar a chave pré-partilhada, configure a chave pré-partilhada para computadores.

#### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

## Não consegue comunicar com a comunicação IPsec

### Estará a utilizar um algoritmo não compatível com as definições do computador?

O scanner é compatível com os seguintes algoritmos.

| Métodos de segurança | Algoritmos |
|---|---|
| Algoritmo de encriptação IKE | AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES |
| Algoritmo de autenticação IKE | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |
| Algoritmo de troca de chave IKE | Grupo DH 1, Grupo DH 2, Grupo DH 5, Grupo DH 14, Grupo DH 15, Grupo DH 16, Grupo DH 17, Grupo DH 18, Grupo DH 19, Grupo DH 20, Grupo DH 21, Grupo DH 22, Grupo DH 23, Grupo DH 24, Grupo DH 25, Grupo DH 26, Grupo DH 27*, Grupo DH 28*, Grupo DH 29*, Grupo DH 30* |
| Algoritmo de encriptação ESP | AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES |
| Algoritmo de autenticação ESP | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |
| Algoritmo de autenticação AH | SHA-1, SHA-256, SHA-384, SHA-512, MD5 |

* disponível apenas para IKEv2

### Informações relacionadas

➡ "Comunicações encriptada usando filtro IPsec/IP" na página 71

## Deixa de poder comunicar de repente

### O endereço IP do scanner é inválido ou foi alterado?

Desative o IPsec através do painel de controlo do scanner.

Se o DHCP estiver desatualizado, reiniciar ou se o endereço IPv6 estiver desatualizado ou não tenha sido obtido, o endereço IP registado para o scanner Web Config (**Definições de segurança de rede** > **IPsec/Filtro de IP** > **Básico** > **Política do grupo** > **Endereço local (Digitalizador)**) pode não ser encontrado.

Utilize um endereço IP estático.

### O endereço IP do computador é inválido ou foi alterado?

Desative o IPsec através do painel de controlo do scanner.

Se o DHCP estiver desatualizado, reiniciar ou se o endereço IPv6 estiver desatualizado ou não tenha sido obtido, o endereço IP registado para o scanner Web Config (**Definições de segurança de rede** > **IPsec/Filtro de IP** > **Básico** > **Política do grupo** > **Endereço remoto (Anfitrião)**) pode não ser encontrado.

Utilize um endereço IP estático.

### Informações relacionadas

➡ "Aceder ao Web Config" na página 23

➡ "Comunicações encriptada usando filtro IPsec/IP" na página 71

## Não é possível ligar depois de configurar a filtragem IPsec/IP

### O valor definido pode estar incorreto.

Desative a filtragem IPsec/IP no painel de controlo do scanner. Ligue o scanner e o computador e configure novamente as definições de Filtragem IPsec/IP.

### Informações relacionadas

➡ "Comunicações encriptada usando filtro IPsec/IP" na página 71

## Não é possível aceder à impressora ou ao scanner após configurar IEEE802.1X

### As definições podem estar erradas.

Desative IEEE802.1X no painel de controlo do scanner. Ligue o scanner e um computador, e a seguir configure IEEE802.1X novamente.

### Informações relacionadas

➡ "Configurar uma rede IEEE802.1X" na página 85

# Problemas de utilização de um certificado digital

## Não é possível importar um certificado CA assinado

### O certificado CA assinado e as informações sobre o CSR correspondem?

Se o certificado CA assinado e o CSR não contiverem as mesmas informações, o CSR não pode ser importado. Verifique o seguinte:

❏ Estará a tentar importar o certificado para um dispositivo que não tem as mesmas informações?

Verifique as informações do CSR e, em seguida, importe o certificado para um dispositivo que tenha as mesmas informações.

❏ Substituiu o CSR guardado no scanner após enviar o CSR para uma autoridade de certificação?

Volte a obter o certificado CA assinado com o CSR.

### O certificado CA assinado tem mais de 5 KB?

Não pode importar um certificado CA assinado com mais de 5 KB.

### A palavra-passe para importar o certificado está correcta?

Se não se lembrar da palavra-passe, não pode importar o certificado.

### Informações relacionadas

➡ "Importar um certificado CA assinado" na página 66

## Não é possível actualizar um certificado auto-assinado

### Introduziu o Nome comum?

É necessário introduzir o **Nome comum**.

### Foram introduzidos caracteres não suportados no Nome comum? Por exemplo, o japonês não é suportado.

Introduza entre 1 e 128 caracteres no formato IPv4, IPv6, nome de anfitrião ou FQDN em ASCII (0x20-0x7E).

### Incluiu uma vírgula ou um espaço no Nome comum?

Se introduziu uma vírgula, o **Nome comum** está dividido nesse ponto. Se introduziu apenas um espaço antes ou depois da vírgula, ocorre um erro.

### Informações relacionadas

➡ "Atualizar um certificado assinado automaticamente" na página 68

## Não consegue criar um CSR

### Introduziu o Nome comum?

É necessário introduzir o **Nome comum**.

### Foram introduzidos caracteres não suportados em Nome comum, Organização, Unidade organizacional, Localidade, Estado/Província? Por exemplo, o japonês não é suportado.

Introduza caracteres no formato IPv4, IPv6, nome de anfitrião ou FQDN em ASCII (0x20-0x7E).

### Incluiu uma vírgula ou um espaço no Nome comum?

Se introduziu uma vírgula, o **Nome comum** está dividido nesse ponto. Se introduziu apenas um espaço antes ou depois da vírgula, ocorre um erro.

### Informações relacionadas

➡ "Obter um certificado CA assinado" na página 64

## Aparece um aviso relacionado com um certificado digital

| Mensagens | Causa/O que fazer |
|---|---|
| Introduza um certificado de servidor. | **Causa:**<br>Não selecionou um ficheiro a importar.<br>**O que fazer:**<br>Selecione um ficheiro e clique em **Importar**. |

## Configurações de segurança avançada para empresas

| Mensagens | Causa/O que fazer |
|---|---|
| Certificado CA 1 não introduzido. | **Causa:**<br>O certificado CA 1 não está introduzido, apenas está introduzido o certificado CA 2.<br>**O que fazer:**<br>Importe o certificado CA 1 primeiro. |
| Valor inválido abaixo. | **Causa:**<br>Estão contidos caracteres não suportados no caminho do ficheiro e/ou na palavra-passe.<br>**O que fazer:**<br>Certifique-se de que os caracteres são introduzidos corretamente para o item. |
| Data e hora inválidos. | **Causa:**<br>A data e a hora do scanner não foram definidas.<br>**O que fazer:**<br>Defina a data e a hora utilizando o Web Config ou o EpsonNet Config. |
| Senha inválida. | **Causa:**<br>A palavra-passe definida para o certificado CA e a palavra-passe introduzida não correspondem.<br>**O que fazer:**<br>Introduza a palavra-passe correta. |
| Ficheiro inválido. | **Causa:**<br>Não está a importar um ficheiro de certificado no formato X509.<br>**O que fazer:**<br>Certifique-se de que está a selecionar o certificado correto enviado por uma autoridade de certificação fidedigna. |
| | **Causa:**<br>O ficheiro que importou é demasiado grande. O tamanho máximo do ficheiro é 5 KB.<br>**O que fazer:**<br>Se selecionar o ficheiro correto, o certificado pode estar corrompido ou ser falsificado. |
| | **Causa:**<br>A cadeia contida no certificado é inválida.<br>**O que fazer:**<br>Para mais informações sobre o certificado, consulte o sítio web da autoridade de certificação. |
| Não é possível utilizar os Certificados de Servidor que incluem mais do que três certificados CA. | **Causa:**<br>O ficheiro do certificado no formato PKCS#12 contém mais de 3 certificados CA.<br>**O que fazer:**<br>Importe cada certificado convertendo-o do formato PKCS#12 para o formato PEM ou importe o ficheiro do certificado no formato PKCS#12 que contém até 2 certificados CA. |

| Mensagens | Causa/O que fazer |
|---|---|
| O certificado expirou. Verifique se o certificado é válido ou verifique a data e hora no produto. | **Causa:**<br>O certificado está fora de prazo.<br>**O que fazer:**<br>❏ Se o certificado estiver fora de prazo, obtenha e importe o novo certificado.<br>❏ Se o certificado não estiver fora de prazo, certifique-se de que a data e a hora do scanner estão definidas corretamente. |
| É necessária uma chave privada. | **Causa:**<br>Não existe nenhuma chave privada associada ao certificado.<br>**O que fazer:**<br>❏ Se o certificado estiver no formato PEM/DER e tiver sido obtido a partir de um CSR utilizando um computador, especifique o ficheiro de chave privada.<br>❏ Se o certificado estiver no formato PKCS#12 e tiver sido obtido a partir de um CSR utilizando um computador, crie um ficheiro que contenha a chave privada. |
| | **Causa:**<br>Voltou a importar o certificado PEM/DER obtido a partir de um CSR utilizando o Web Config.<br>**O que fazer:**<br>Se o certificado estiver no formato PEM/DER e tiver sido obtido a partir de um CSR utilizando o Web Config, apenas o pode importar uma vez. |
| Configuração falhada. | **Causa:**<br>Não é possível terminar a configuração porque a comunicação entre o scanner e o computador falhou ou o ficheiro não pode ser lido devido a alguns erros.<br>**O que fazer:**<br>Depois de verificar o ficheiro especificado e a comunicação, volte a importar o ficheiro. |

### Informações relacionadas

➡ "Informações sobre certificação digital" na página 63

## Apagar um certificado CA assinado por engano

### Existe um ficheiro de cópia de segurança para o certificado?

Se tiver o ficheiro de cópia de segurança, volte a importar o certificado.

Se obtiver um certificado utilizando um CSR criado através do Web Config, não pode importar novamente um certificado apagado. Crie um CSR e obtenha um novo certificado.

### Informações relacionadas

➡ "Apagar um certificado CA assinado" na página 67

➡ "Importar um certificado CA assinado" na página 66