

# Manual do administrador



---

# Conteúdo

|  |          |
|--|----------|
| <b>Manual do administrador</b> .....   | <b>7</b> |
| <b>Uso do software de configuração de rede Web Config</b> .....              | <b>8</b> |
| Sobre Web Config .....   | 8        |
| Acesso ao Web Config .....   | 8        |
| Restrição de recursos disponíveis a usuários .....                           | 9        |
| Restrição a recurso de usuário .....   | 10       |
| Configuração de restrições de recurso de usuário .....                       | 10       |
| Mudança da senha de administrador no Web Config .....                        | 12       |
| Uso do seu produto em uma rede segura .....                                  | 13       |
| Configuração de comunicação SSL/TLS .....                                    | 14       |
| Configuração de ajustes SSL/TLS .....  | 14       |
| Configuração de um certificado de servidor para o produto.....               | 15       |
| Configuração de filtragem IPsec/IP .....                                     | 16       |
| Sobre IPsec/Filtro de IP .....   | 16       |
| Configuração de política de filtragem IPsec/IP padrão .....                  | 16       |
| Configuração de políticas de IPsec/Filtro de IP de grupo.....                | 17       |
| Configurações de política de filtragem IPsec/IP.....                         | 18       |
| Exemplos de configuração de filtragem IPsec/IP .....                         | 24       |
| Configuração de um certificado de filtragem IPsec/IP.....                    | 26       |
| Configuração de protocolo SNMPv3 .....                                       | 26       |
| Configurações SNMPv3.....  | 27       |
| Configuração de ajustes S/MIME .....   | 28       |
| Configuração de ajustes básicos S/MIME .....                                 | 28       |
| Configurações S/MIME .....   | 29       |
| Configuração de um certificado para S/MIME.....                              | 32       |
| Importação de um certificado de criptografia para um destino de e-mail ..... | 32       |
| Conexão do produto a uma rede IEEE 802.1X .....                              | 33       |
| Configuração de uma rede IEEE802.1X .....                                    | 34       |
| Configurações da rede IEEE 802.1X .....                                      | 35       |
| Configuração de um certificado para uma rede IEEE 802.1X.....                | 36       |

|  |           |
|--|-----------|
| Estado da rede IEEE 802.1X .....                                       | 37        |
| Uso de um certificado digital.....                                     | 38        |
| Sobre certificação digital.....  | 38        |
| Obtenção e importação de Certificado CA assinado.....                  | 38        |
| Ajustes de configuração CSR .....                                      | 40        |
| Configurações de importação CSR.....                                   | 41        |
| Exclusão de certificado CA assinado .....                              | 42        |
| Atualização de um certificado auto-assinado.....                       | 42        |
| Uso de um servidor LDAP .....  | 44        |
| Configuração do servidor LDAP e seleção de configurações de busca..... | 44        |
| Configuração do servidor LDAP.....                                     | 46        |
| Configurações de busca LDAP .....                                      | 48        |
| Verificação da conexão do servidor LDAP.....                           | 48        |
| Mensagens de relatório de conexão LDAP .....                           | 49        |
| Configuração de protocolos em Web Config .....                         | 49        |
| Configurações de protocolo .....                                       | 50        |
| Uso de um servidor de e-mail .....                                     | 54        |
| Configuração de um servidor de e-mail .....                            | 55        |
| Configuração do servidor de e-mail .....                               | 55        |
| Verificação da conexão do servidor de e-mail.....                      | 56        |
| Mensagens de relatório de conexão do servidor de e-mail.....           | 57        |
| Configuração de notificação por e-mail.....                            | 59        |
| <b>Uso do software de configuração de rede EpsonNet Config.....</b>    | <b>61</b> |
| Instalação do EpsonNet Config.....                                     | 61        |
| Configuração de um endereço IP do produto usando EpsonNet Config ..... | 61        |
| <b>Uso do software de configuração Epson Device Admin.....</b>         | <b>64</b> |
| <b>Criptografia de senhas.....</b>                                     | <b>65</b> |
| Configuração de uma senha de encriptação .....                         | 65        |
| Restauração da chave de encriptação de senha .....                     | 67        |
| <b>Gerenciamento de retenção de dados.....</b>                         | <b>68</b> |
| Deletar todos os dados do produto.....                                 | 68        |
| Modificação da configurações de deleção automática .....               | 70        |

|   |           |
|---|-----------|
| <b>Solução de problemas .....</b>   | <b>72</b> |
| Mensagens de erro de digitalização .....  | 72        |
| Resolução de problemas do uso de software de rede .....                           | 74        |
| Não é possível acessar o Web Config .....   | 75        |
| A mensagem "Vencido" aparece .....  | 75        |
| A mensagem "O nome do certificado de segurança não é igual" aparece .....         | 76        |
| Nome do modelo ou endereço IP não exibidos no EpsonNet Config .....               | 76        |
| Resolução de problemas de segurança de rede .....                                 | 76        |
| Chave pré-compartilhada foi esquecida .....                                       | 76        |
| Não é possível fazer a comunicação com o produto usando comunicação IPsec.....    | 77        |
| Comunicação estava funcionando, mas parou.....                                    | 77        |
| Não é possível criar a porta de impressão segura IPP .....                        | 78        |
| Não é possível fazer a conexão depois da configuração de filtragem IPsec/IP ..... | 78        |
| Não é possível acessar o produto depois de configurar IEEE 802.1X.....            | 78        |
| Resolução de problemas de certificado digital .....                               | 78        |
| Mensagens de aviso de certificado digital .....                                   | 78        |
| Não é possível importar um certificado digital .....                              | 80        |
| Não é possível atualizar um certificado nem criar um CSR .....                    | 80        |
| Certificado CA assinado excluído.....   | 81        |
| Onde obter ajuda.....   | 81        |
| <b>Avisos.....</b>  | <b>84</b> |
| Marcas comerciais .....   | 84        |
| Avisos sobre direitos autorais.....   | 84        |
| Atribuição de direitos autorais .....   | 85        |



---

# Manual do administrador

Seja bem-vindo ao *Manual do administrador*.

Para uma versão imprimível em PDF deste manual, clique [aqui](#).

**Observação:** Nem todos os recursos mencionados neste *Manual do administrador* estão disponíveis em todo modelo de produto.

Você pode usar dois softwares para fazer as configurações de rede avançadas do seu produto: Web Config e EpsonNet Config. Este manual trata do Web Config em detalhes; para informações sobre uso do EpsonNet Config, consulte o utilitário de ajuda do EpsonNet Config.

As funções de rede disponíveis podem variar de acordo com o produto. (Funções indisponíveis não são exibidas no painel de controle do produto nem na tela de configurações do software.) Os produtos Epson suportam as seguintes funções de administração de sistema:

- Comunicação SSL/TLS: use Secure Sockets Layer/Transport Layer Security para codificar tráfego e evitar spoofing entre o produto e um computador
- Filtragem IPsec/IP: controle acesso e comunicações seguras entre o produto e um gateway de rede
- Controle de protocolo individual: habilite e desabilite serviços únicos
- Configuração remota de destinos de scan e fax: use um servidor LDAP para procurar contatos de e-mail e fax
- Restrição a recurso de usuário: permita ou negue acesso a impressão, digitalização, fax e cópia com base em usuário
- Importação e exportação de configurações de impressora: transfira configurações de um produto a outro

---

# Uso do software de configuração de rede Web Config

Siga as instruções nessas seções para fazer as configurações de rede administradora usando o software Web Config.

**Observação:** Antes de poder fazer as configurações de administração do sistema, é preciso que conecte o produto a uma rede. Consulte o *Manual do usuário* do produto para mais instruções.

[Sobre Web Config](#)

[Acesso ao Web Config](#)

[Restrição de recursos disponíveis a usuários](#)

[Uso do seu produto em uma rede segura](#)

## Sobre Web Config

Web Config é um aplicativo a base de navegador que você pode usar para configurar o seu produto. Páginas de configurações básicas e avançadas estão disponíveis.

**Observação:** Antes de poder fazer as configurações de administração do sistema, é preciso que conecte o produto a uma rede. Consulte o *Manual do usuário* do produto para mais instruções.

Você pode bloquear as configurações que seleciona definindo uma senha de administrador para o produto. Consulte o *Manual do usuário* do produto para instruções.

**Tema principal:** [Uso do software de configuração de rede Web Config](#)

## Acesso ao Web Config

Você pode acessar o Web Config do seu navegador usando HTTP ou HTTPS.

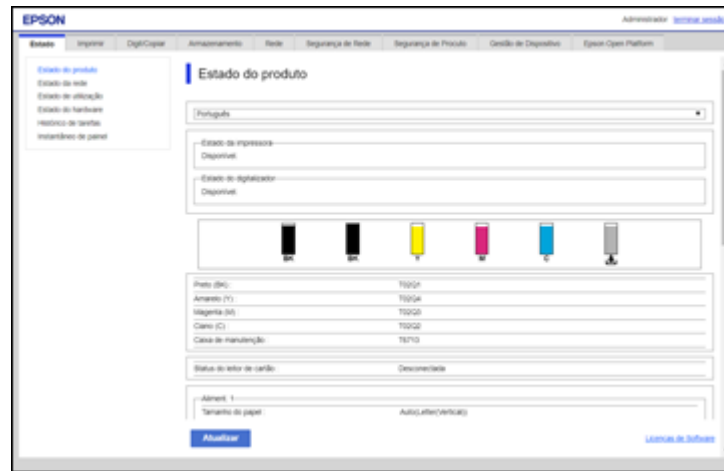
O padrão é acessar o Web Config pela primeira vez usando HTTP. Se continuar usando HTTP, Web Config não exibirá todos os menus disponíveis.

1. Imprima uma folha de estado de rede para o seu produto e identifique o endereço IP do produto. Consulte o *Manual do usuário* do produto para mais instruções.
2. Inicie seu navegador e verifique se JavaScript está habilitado.
3. Digite o endereço IP do produto no navegador assim, dependendo do protocolo que está usando
  - IPv4: `http://endereço IP do produto`



- IPv6: [http://\[endereço IP do produto\]/](http://[endereço IP do produto]/)

A página de estado aparece:



4. Para usar HTTPS, configure o seu navegador para usar HTTPS para o endereço.

Uma mensagem avisando sobre o certificado auto assinado irá aparecer.

Para acessar o Web Config depois de configurar HTTPS, digite <https://> antes do endereço IP do produto, mostrado no passo 3.

**Observação:** Se o nome do produto está registrado com o servidor DNS, você pode usar o nome do produto ao invés do endereço IP para acessar o Web Config.

**Tema principal:** [Uso do software de configuração de rede Web Config](#)

## Restrição de recursos disponíveis a usuários

Siga as instruções nessas seções para restringir usuários de usarem certos recursos do produto e crie uma senha de administrador para bloquear as restrições usando o software Web Config.

[Restrição a recurso de usuário](#)

[Configuração de restrições de recurso de usuário](#)

[Mudança da senha de administrador no Web Config](#)

**Tema principal:** [Uso do software de configuração de rede Web Config](#)

## Restrição a recurso de usuário

Você pode restringir recursos do produto disponíveis para até 10 usuários individuais, com diferentes recursos disponíveis a cada usuário. Isso requer que usuários entrem no painel de controle do produto usando seu nome de usuário e senha antes de usar recursos do painel de controle.

Com Windows, você também pode restringir impressão e digitalização do software do produto. Isso requer que usuários façam login no software de impressão ou digitalização e permite que o software autentique os usuários antes que impressão ou digitalização prossiga. Para instruções em configurar restrições de software, consulte o utilitário de ajuda no software de impressão ou digitalização.

**Tema principal:** [Restrição de recursos disponíveis a usuários](#)

## Configuração de restrições de recurso de usuário

Você pode criar até 10 contas de usuário e restringir acesso a recursos do painel de controle separadamente para cada um.

1. Acesse o Web Config e selecione a guia **Segurança do Produto**.

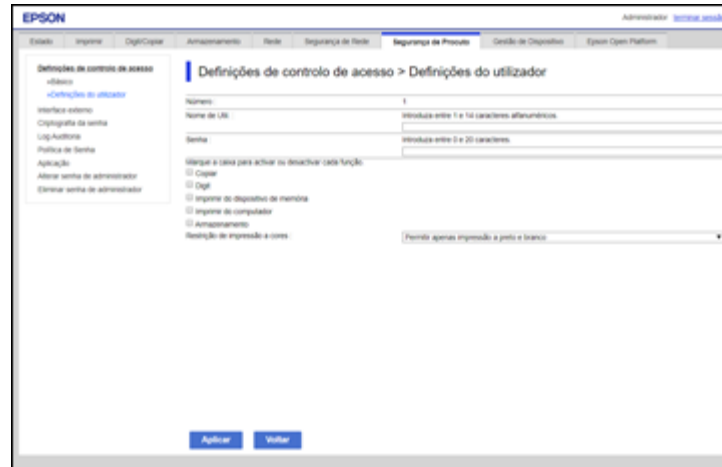
Você verá uma janela como esta:



2. Marque a caixa de diálogo **Activa o controlo de acesso**.

3. Se você configurou o produto para um servidor LDAP ou rede IEEE 802.1x, você pode desmarcar a caixa de diálogo **Permite a impressão e digitalização sem informações de autenticação de um computador** para evitar que o produto receba trabalhos enviados de outras fontes:
  - O driver de sistema operacional padrão
  - Um driver de impressora PCL ou PostScript
  - Serviços na internet tais como Epson Connect
  - Smartphones e outros dispositivos móveis
4. Clique em **OK**.
5. Selecione **Definições do utilizador**.
6. Clique em **Adicionar**.

Você verá uma janela como esta:



The screenshot shows the EPSON control panel interface. The top navigation bar includes 'Estado', 'Impressão', 'Digit/Cópia', 'Armazenamento', 'Rede', 'Segurança de Rede', 'Segurança de Produto', 'Gestão de Dispositivos', and 'Epson Open Platform'. The main content area is titled 'Definições de controle de acesso > Definições do utilizador'. On the left, there is a sidebar with options: 'Definições de controle de acesso', 'Definições do utilizador', 'Interface externo', 'Criptografia de senha', 'Log/Auditoria', 'Política de Senha', 'Ativação', 'Alterar senha de administrador', and 'Eliminar senha de administrador'. The main area contains the following fields and options:

- 'Nome de usuário' with a value of 8 and a character count of 8.
- 'Nome de Usuário' with a character count of 1 a 14 caracteres alfanuméricos.
- 'Senha' with a character count of 2 a 20 caracteres.
- 'Marque a lista para activar ou desactivar cada função':
  - Copiar
  - Digit
  - Impor de dispositivos de memória
  - Impor de computadores
  - Armazenamento
- 'Restrição de impressão a cores' with a dropdown menu set to 'Permitir apenas impressões a preto e branco'.

At the bottom, there are 'Aplicar' and 'Voltar' buttons.

7. Digite um nome para o usuário no campo Nome de usuário seguindo as diretrizes na tela. Use caracteres ASCII (0x20-0x7E).
8. Digite uma senha para o usuário no campo Senha seguindo as diretrizes na tela.

**Observação:** Se precisar resetar uma senha, deixe o campo Senha em branco.

9. Marque a caixa de diálogo para cada função que deseja que o usuário possa realizar e desmarque cada função a qual queira restringir o acesso.
10. Clique em **Aplicar**.

**Observação:** Quando você edita uma conta de usuário completa, você vê a opção **Excluir**. Clique aí para excluir um usuário, se necessário.

**Observação:** Você pode importar e exportar uma lista de recursos de usuário usando o EpsonNet Config. Consulte o utilitário de ajuda no software para instruções.

**Tema principal:** [Restrição de recursos disponíveis a usuários](#)

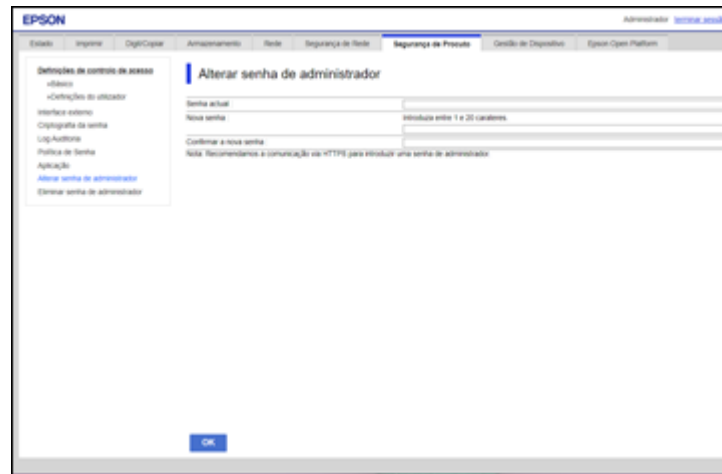
## **Mudança da senha de administrador no Web Config**

Você pode definir uma senha de administrador usando o painel de controle do produto, Web Config ou EpsonNet Config. Você usa a mesma senha de administrador em todos os casos.

**Observação:** Consulte o *Manual do usuário* do produto para instruções sobre como configurar uma senha de administrador usando o painel de controle. Se esquecer sua senha de administrador, entre em contato com a Epson para obter ajuda, conforme descrito no *Manual do usuário* do produto.

1. Acesse o Web Config e selecione a guia **Segurança do Produto**.
2. Selecione **Alterar senha de administrador**.

Você verá uma janela como esta:



3. Digite um nome de usuário, se necessário.
4. Execute um dos seguintes procedimentos:
  - Se definiu uma senha de administrador antes, digite a senha atual, depois digite e confirme a nova senha nos campos fornecidos.
  - Se não definiu uma senha de administrador antes, digite uma nova senha e a confirme nos campos fornecidos.
5. Clique em **OK**.

**Tema principal:** [Restrição de recursos disponíveis a usuários](#)

## Uso do seu produto em uma rede segura

Siga as instruções nessas seções para configurar recursos de segurança para o seu produto na rede usando o software Web Config.

[Configuração de comunicação SSL/TLS](#)

[Configuração de filtragem IPsec/IP](#)

[Configuração de protocolo SNMPv3](#)

[Configuração de ajustes S/MIME](#)

[Conexão do produto a uma rede IEEE 802.1X](#)

Uso de um certificado digital  
Uso de um servidor LDAP  
Configuração de protocolos em Web Config  
Uso de um servidor de e-mail

**Tema principal:** Uso do software de configuração de rede Web Config

## Configuração de comunicação SSL/TLS

Siga as instruções nessas seções para configurar comunicação SSL/TLS usando o Web Config.

Configuração de ajustes SSL/TLS  
Configuração de um certificado de servidor para o produto

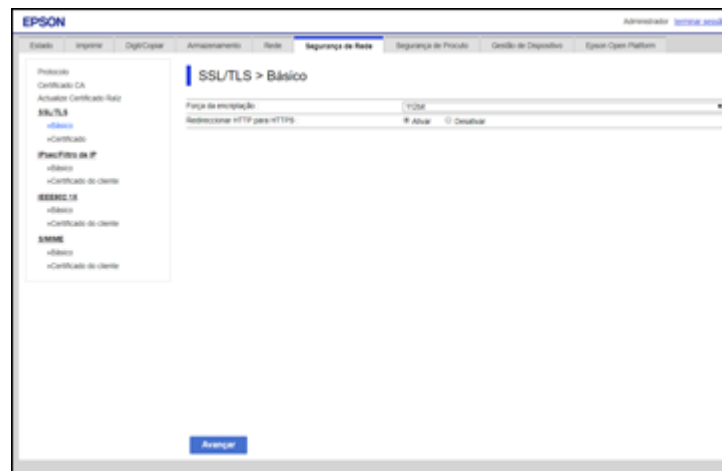
**Tema principal:** Uso do seu produto em uma rede segura

## Configuração de ajustes SSL/TLS

Se seu produto suporta HTTPS, você pode configurar SSL/TLS para codificar comunicações com seu produto.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob **SSL/TLS**, selecione **Básico**.

Você verá uma janela como esta:



3. Selecione uma das opções para a configuração **Força da encriptação**.

4. Selecione **Ativar** ou **Desativar** como configuração de **Redireccionar HTTP para HTTPS** conforme necessário.
5. Clique em **Avançar**.  
Você verá uma mensagem de confirmação.
6. Clique em **OK**.

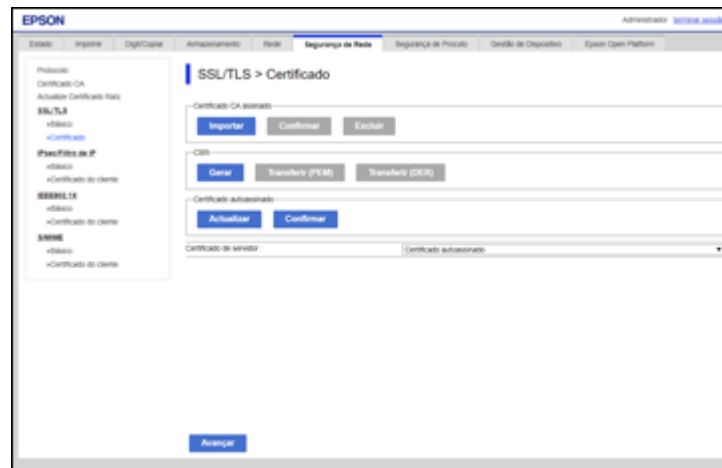
**Tema principal:** [Configuração de comunicação SSL/TLS](#)

### Configuração de um certificado de servidor para o produto

Você pode configurar um certificado de servidor para o produto.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob **SSL/TLS**, selecione **Certificado**.

Você verá uma janela como esta:



3. Selecione uma das seguintes opções:
  - **Certificado CA assinado:** selecione **Importar** se você obteve certificado CA assinado. Selecione o arquivo a ser importado e clique em **OK**.
  - **Certificado autoassinado:** selecione **Atualizar** se você não obteve um certificado CA (Certificate Authority) assinado e deseja que o produto gere um certificado autoassinado
4. Clique em **Avançar**.

Você verá uma mensagem de confirmação.

5. Clique em **OK**.

**Tema principal:** [Configuração de comunicação SSL/TLS](#)

## **Configuração de filtragem IPsec/IP**

Siga as instruções nessas seções para configurar a filtragem de tráfego IPsec/IP usando o Web Config.

[Sobre IPsec/Filtro de IP](#)

[Configuração de política de filtragem IPsec/IP padrão](#)

[Configuração de políticas de IPsec/Filtro de IP de grupo](#)

[Configurações de política de filtragem IPsec/IP](#)

[Exemplos de configuração de filtragem IPsec/IP](#)

[Configuração de um certificado de filtragem IPsec/IP](#)

**Tema principal:** [Uso do seu produto em uma rede segura](#)

### **Sobre IPsec/Filtro de IP**

Você pode filtrar tráfego para o produto pela rede com base em endereço IP, serviço e porta configurando uma política padrão que se aplica a todo usuário ou grupo se conectando ao produto. Para controle de usuários individuais ou grupos de usuários, você pode configurar políticas de grupo.

**Observação:** Apenas computadores rodando Windows Vista ou posterior, ou Windows Server 2008 ou posterior suportam IPsec.

**Tema principal:** [Configuração de filtragem IPsec/IP](#)

### **Configuração de política de filtragem IPsec/IP padrão**

Você pode configurar a política padrão para filtragem de tráfego IPsec/IP usando o Web Config.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob **IPsec/Filtro de IP**, selecione **Básico**.



Você verá uma janela como esta:



3. Selecione **Ativar** para habilitar filtragem IPsec/IP.
4. Selecione as opções de filtragem que deseja usar como política padrão.
5. Clique em **Avançar**.  
Você verá uma mensagem de confirmação.
6. Clique em **OK**.

**Tema principal:** [Configuração de filtragem IPsec/IP](#)

### **Configuração de políticas de IPsec/Filtro de IP de grupo**

Você pode configurar as políticas de grupo para filtragem de tráfego IPsec/IP usando o Web Config.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob **IPsec/Filtro de IP**, selecione **Básico**.
3. Clique em um número de guia para o número da política que deseja configurar.

Você verá uma janela como esta:



4. Marque a caixa de diálogo **Ativar esta Política de Grupo**.
5. Selecione as opções de filtragem que deseja para esta política de grupo.
6. Clique em **Avançar**.  
Você verá uma mensagem de confirmação.
7. Clique em **OK**.
8. Se desejar configurar políticas de grupo adicionais, clique no próximo número de guia e repita os passos de configuração conforme necessário.

**Tema principal:** [Configuração de filtragem IPsec/IP](#)

### Configurações de política de filtragem IPsec/IP

#### Configurações de política predefinida

| Configuração              | Opções/Descrição   |
|---------------------------|--|
| <b>Controlo de Acesso</b> | <b>Permitir Acesso</b> para permitir que pacotes IP passem<br><b>Recusar Acesso</b> para evitar que pacotes IP passem<br><b>IPsec</b> para permitir que pacotes IPsec passem |

| <b>Configuração</b>                   | <b>Opções/Descrição</b>   |
|---------------------------------------|---|
| <b>Versão de IKE</b>                  | Selecione uma versão do protocolo de Internet Key Exchange (IKE) que corresponda ao seu ambiente de rede.   |
| <b>Método de autenticação</b>         | Selecione um método de autenticação, ou selecione <b>Certificado</b> se você importou um certificado CA assinado  |
| <b>Chave pré-partilhada</b>           | Se necessário, digite uma chave pré-compartilhada entre 1 e 127 caracteres  |
| <b>Confirmar chave pré-partilhada</b> | Confirme a chave pré-compartilhada que você digitou.  |
| <b>Tipo de ID</b>                     | Se selecionou <b>IKEv2</b> como a configuração de <b>Versão de IKE</b> , selecione o tipo de ID na lista.   |
| <b>ID</b>                             | Se você selecionou <b>IKEv2</b> como a configuração de <b>Versão de IKE</b> , digite a informação de identificação necessária.  |
| <b>Encapsulamento</b>                 | Se selecionou <b>IPsec</b> como opção de <b>Controlo de Acesso</b> , selecione um desses modos de encapsulamento:<br><br><b>Modo de transporte:</b> se estiver usando o produto na mesma rede LAN; pacotes de camada 4 ou posterior são codificados<br><br><b>Modo Túnel:</b> se estiver usando o produto em uma rede com capacidade de internet, tal como IPsec-VPN; o cabeçalho e dados de pacotes IP são codificados |
| <b>Endereço gateway remoto</b>        | Se selecionou <b>Modo Túnel</b> como opção de <b>Encapsulamento</b> , digite um endereço gateway entre 1 e 39 caracteres  |
| <b>Protocolo de segurança</b>         | Se selecionou <b>IPsec</b> como opção de <b>Controlo de Acesso</b> , selecione um desses protocolos de segurança:<br><br><b>ESP:</b> para garantir a integridade de autenticação e dados, e codificar dados<br><br><b>AH:</b> para garantir a integridade de autenticação e dados, se codificação de dados for proibida, você pode usar IPsec   |

| Configuração                   | Opções/Descrição   |
|--------------------------------|--|
| <b>Definições de algoritmo</b> | Selecione as configurações do algoritmo de criptografia para o protocolo de segurança que você selecionou. |

#### Configurações de política de grupo

| Configuração                       | Opções/Descrição  |
|------------------------------------|---|
| <b>Controlo de Acesso</b>          | <b>Permitir Acesso</b> para permitir que pacotes IP passem<br><b>Recusar Acesso</b> para evitar que pacotes IP passem<br><b>IPsec</b> para permitir que pacotes IPsec passem  |
| <b>Endereço local (Impressora)</b> | Selecione um endereço IPv4 ou IPv6 que seja igual ao seu ambiente de rede; se o endereço IP é definido automaticamente, selecione <b>Usar endereço IPv4 obtido automaticamente</b>  |
| <b>Endereço remoto (Anfitrião)</b> | Digite o endereço IP do dispositivo (entre 0 e 43 caracteres) para controlar acesso, ou deixe em branco para controlar todos os endereços; se o endereço IP for definido automaticamente, tal como por DHCP, a conexão pode estar indisponível, então configure um endereço estático ao invés disso |
| <b>Método de seleção da porta</b>  | Selecione o método que deseja usar para especificar portas  |
| <b>Nome do serviço</b>             | Se selecionou <b>Nome de Serviço</b> como opção de <b>Método de Escolha de Porta</b> , selecione uma opção de nome de serviço aqui, consulte a tabela a seguir para mais informações  |

| <b>Configuração</b>            | <b>Opções/Descrição</b>  |
|--------------------------------|--|
| <b>Protocolo de Transporte</b> | <p>Se selecionou <b>Número da Porta</b> como opção de <b>Método de seleção da porta</b>, selecione um desses modos de encapsulamento:</p> <p><b>Qualquer protocolo</b><br/> <b>TCP</b><br/> <b>UDP</b><br/> <b>ICMPv4</b></p> <p>Consulte a tabela de Diretrizes de política de grupo para mais informações</p>  |
| <b>Porta Local</b>             | <p>Se selecionou <b>Número da Porta</b> como opção de <b>Método de seleção da porta</b> e <b>TCP</b> ou <b>UDP</b> para opção de <b>Protocolo de transporte</b>, digite os números de porta que controlam o recebimento de pacotes (até 10 portas), separados por vírgulas, por exemplo <b>25,80,143,5220</b>; deixe esta configuração em branco para controlar todas as portas; consulte a próxima tabela para mais informações</p> |
| <b>Porta remota</b>            | <p>Se selecionou <b>Número da Porta</b> como opção de <b>Método de seleção da porta</b> e <b>TCP</b> ou <b>UDP</b> para opção de <b>Protocolo de transporte</b>, digite os números de porta que controlam o envio de pacotes (até 10 portas), separados por vírgulas, por exemplo <b>25,80,143,5220</b>; deixe esta configuração em branco para controlar todas as portas; consulte a próxima tabela para mais informações</p>       |
| <b>Versão de IKE</b>           | <p>Selecione <b>IKEv1</b> ou <b>IKEv2</b> dependendo do dispositivo ao qual o produto esteja conectado.</p>  |
| <b>Método de autenticação</b>  | <p>Se selecionou <b>IPsec</b> como opção de <b>Controle de Acesso</b>, selecione um método de autenticação aqui</p>  |
| <b>Chave pré-partilhada</b>    | <p>Se selecionou <b>Chave pré-partilhada</b> como opção de <b>Método de autenticação</b>, digite uma chave pré-compartilhada entre 1 e 127 caracteres aqui e no campo <b>Confirmar chave pré-partilhada</b></p>  |
| <b>Tipo de ID</b>              | <p>Se selecionou <b>IKEv2</b> como a configuração de <b>Versão de IKE</b>, selecione o tipo de ID na lista.</p>  |

| Configuração                   | Opções/Descrição  |
|--------------------------------|---|
| <b>ID</b>                      | Se você selecionou <b>IKEv2</b> como a configuração de <b>Versão de IKE</b> , digite a informação de identificação necessária.  |
| <b>Encapsulamento</b>          | Se selecionou <b>IPsec</b> como opção de <b>Controlo de Acesso</b> , selecione um desses modos de encapsulamento:<br><br><b>Modo de transporte:</b> se estiver usando o produto na mesma rede LAN; pacotes de camada 4 ou posterior são codificados<br><br><b>Modo Túnel:</b> se estiver usando o produto em uma rede com capacidade de internet, tal como IPsec-VPN; o cabeçalho e dados de pacotes IP são codificados |
| <b>Endereço gateway remoto</b> | Se selecionou <b>Modo Túnel</b> como opção de <b>Encapsulamento</b> , digite um endereço gateway entre 1 e 39 caracteres  |
| <b>Protocolo de segurança</b>  | Se selecionou <b>IPsec</b> como opção de <b>Controlo de Acesso</b> , selecione um desses protocolos de segurança:<br><br><b>ESP:</b> para garantir a integridade de autenticação e dados, e codificar dados<br><br><b>AH:</b> para garantir a integridade de autenticação e dados, se codificação de dados for proibida, você pode usar IPsec   |
| <b>Definições de algoritmo</b> | Selecione as configurações do algoritmo de criptografia para o protocolo de segurança que você selecionou.  |

#### Diretrizes de Política de Grupo

| Nome de serviço | Tipo de protocolo | Número de porta local/remota | Controla essas operações   |
|-----------------|-------------------|------------------------------|--|
| Variável        | —                 | —                            | Todos os serviços  |
| ENPC            | UDP               | 3289/Qualquer porta          | Buscando um produto a partir de aplicações tais como drivers de impressora ou scanner ou EpsonNet Config |

| <b>Nome de serviço</b>          | <b>Tipo de protocolo</b> | <b>Número de porta local/remota</b> | <b>Controla essas operações</b>  |
|---------------------------------|--------------------------|-------------------------------------|--|
| SNMP                            | UDP                      | 161/Qualquer porta                  | Adquirindo e configurando MIB de aplicações tais como drivers de impressora ou scanner ou EpsonNet Config                    |
| LPR                             | TCP                      | 515/Qualquer porta                  | Encaminhamento de dados LPR  |
| RAW (Porta9100)                 | TCP                      | 9100/Qualquer porta                 | Encaminhamento de dados RAW  |
| IPP/IPPS                        | TCP                      | 631/Qualquer porta                  | Encaminhamento de dados AirPrint (impressão IPP/IPPS)  |
| WSD                             | TCP                      | Qualquer porta/5357                 | Controle de WSD  |
| WS-Discovery                    | UDP                      | 3702/Qualquer porta                 | Buscando um produto de WSD   |
| Pesquisa de rede                | TCP                      | 1865/Qualquer porta                 | Encaminhamento de dados de scan do Document Capture Pro  |
| Digitalização em rede por botão | TCP                      | Qualquer porta/2968                 | Adquirindo informação de trabalho sobre push scanning do Document Capture Pro  |
| Network Push Scan Discovery     | UDP                      | 2968/Qualquer porta                 | Buscando um computador durante push scanning do Document Capture Pro   |
| Dados FTP (Local)               | TCP                      | 20/Qualquer porta                   | Encaminhando dados de impressão FTP para servidor FTP  |
| Controlo FTP (Local)            | TCP                      | 21/Qualquer porta                   | Controlando impressão FTP para servidor FTP  |
| Dados FTP (Remoto)              | TCP                      | Qualquer porta/20                   | Encaminhando dados de scan e dados de fax recebido para cliente FTP; controla apenas um servidor FTP que usa porta remota 20 |
| Controlo FTP (Remoto)           | TCP                      | Qualquer porta/21                   | Encaminhando dados de scan e dados de fax recebido para cliente FTP  |
| CIFS (Local)*                   | TCP                      | 445/Qualquer porta                  | Compartilhando uma pasta de rede em servidor CIFS  |

| Nome de serviço                  | Tipo de protocolo | Número de porta local/remota | Controla essas operações  |
|----------------------------------|-------------------|------------------------------|---|
| CIFS (Remoto)*                   | TCP               | Qualquer porta/445           | Encaminhando dados de scan e dados de fax recebido para uma pasta em servidor CIFS                                      |
| NetBIOS Name Service (Local)     | UDP               | 137/Qualquer porta           | Compartilhando uma pasta de rede em servidor CIFS   |
| NetBIOS Datagram Service (Local) | UDP               | 138/Qualquer porta           |   |
| NetBIOS Session Service (Local)  | TCP               | 139/Qualquer porta           |   |
| NetBIOS Name Service (Remoto)    | UDP               | Qualquer porta/137           | Encaminhando dados de scan e dados de fax recebido para uma pasta em servidor CIFS                                      |
| NetBIOS Datagram (Remoto)        | UDP               | Qualquer porta/138           |   |
| NetBIOS Session Service (Remoto) | TCP               | Qualquer porta/139           |   |
| HTTP (Local)                     | TCP               | 80/Qualquer porta            | Encaminhando dados de Web Config e WSD para um servidor HTTP ou HTTPS   |
| HTTPS (Local)                    | TCP               | 443/Qualquer porta           |   |
| HTTP (Remoto)                    | TCP               | Qualquer porta/80            | Comunicando com Epson Connect, atualização de firmware e atualização de certificado de raiz em um cliente HTTP ou HTTPS |
| HTTPS (Remoto)                   | TCP               | Qualquer porta/443           |   |

\* Para controlar encaminhamento de dados de scan e de fax recebido, compartilhe uma pasta da rede ou dados de fax recebido de um PC-Fax, selecione **Número da Porta** como opção de **Método de seleção da porta** e especifique os números de porta para CIFS e NetBIOS.

**Tema principal:** [Configuração de filtragem IPsec/IP](#)

#### **Exemplos de configuração de filtragem IPsec/IP**

Você pode configurar filtragem IPsec e IP de diversas formas, conforme mostrado nos exemplos aqui.



### **Recepção apenas de pacotes IPsec**

Use este exemplo apenas para configurar uma política padrão.

- **IPsec/Filtro de IP: Ativar**
- **Controlo de Acesso: IPsec**
- **Método de autenticação: Chave pré-partilhada**
- **Chave pré-partilhada:** Digite uma chave de até 127 caracteres

### **Recepção de dados de impressão e configurações de impressora**

Use este exemplo para permitir comunicação de dados de impressão e configurações de impressora de serviços especificados.

Política padrão:

- **IPsec/Filtro de IP: Ativar**
- **Controlo de Acesso: Recusar acesso**

Política de grupo:

- **Controlo de Acesso: Permitir acesso**
- **Endereço remoto (Anfitrião):** Endereço IP de cliente
- **Método de seleção da porta: Nome do serviço**
- **Nome do serviço:** Selecione **ENPC**, **SNMP**, **HTTP (Local)**, **HTTPS (Local)** e **RAW (Porta9100)**

### **Recepção de acesso apenas de um endereço especificado para acesso ao produto**

Nesses exemplos, o cliente será capaz de acessar e configurar o produto em qualquer configuração de política.

Política padrão:

- **IPsec/Filtro de IP: Ativar**
- **Controlo de Acesso: Recusar acesso**

Política de grupo:

- **Controlo de Acesso: Permitir acesso**
- **Endereço remoto (Anfitrião):** Endereço IP de cliente do administrador

**Tema principal:** [Configuração de filtragem IPsec/IP](#)

## Configuração de um certificado de filtragem IPsec/IP

Você pode configurar um certificado para filtragem de tráfego IPsec/IP usando o Web Config.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob **IPsec/Filtro de IP**, selecione **Certificado do cliente**.

Você verá uma janela como esta:



3. Clique em **Importar** para adicionar um novo certificado de cliente e fazer qualquer configuração necessária.
4. Clique em **OK**.

**Tema principal:** [Configuração de filtragem IPsec/IP](#)

**Tarefas relacionadas**

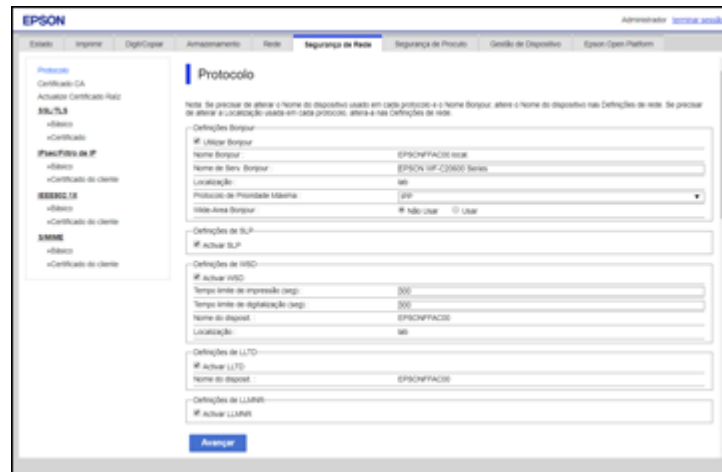
[Obtenção e importação de Certificado CA assinado](#)

## Configuração de protocolo SNMPv3

Se seu produto suporta o protocolo SNMPv3, você pode monitorar e controlar acesso ao seu produto usando esse protocolo.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.

Você verá uma janela como esta:



2. Navegue para baixo e selecione a caixa de diálogo **Ativar SNMPv3** para habilitar configurações SNMPv3.
3. Selecione as configurações que deseja na seção Configurações SNMPv3.
4. Clique em **Avançar**.  
Você verá uma mensagem de confirmação.
5. Clique em **OK**.

### Configurações SNMPv3

**Tema principal:** [Uso do seu produto em uma rede segura](#)

### Configurações SNMPv3

Você pode configurar esses ajustes de SNMPv3 no Web Config.

| Configuração                      | Opções/Descrição  |
|-----------------------------------|---|
| <b>Nome de Util.</b>              | Digite um nome de usuário de 1 a 32 caracteres em ASCII |
| <b>Definições de autenticação</b> |   |
| <b>Algoritmo</b>                  | Selecione o algoritmo para autenticação                 |

| Configuração                     | Opções/Descrição   |
|----------------------------------|--|
| Palavra-passe                    | Digite uma senha de 8 a 32 caracteres em ASCII           |
| Confirmar palavra-passe          | Digite a senha de autenticação novamente                 |
| <b>Definições de encriptação</b> |  |
| Algoritmo                        | Selecione o algoritmo para criptografia                  |
| Palavra-passe                    | Digite uma senha de 8 a 32 caracteres em ASCII           |
| Confirmar palavra-passe          | Digite a senha de codificação novamente                  |
| Nome de contexto                 | Digite um nome de contexto de 1 a 32 caracteres em ASCII |

Tema principal: [Configuração de protocolo SNMPv3](#)

## Configuração de ajustes S/MIME

Siga as instruções nessas seções para fazer configurações S/MIME usando o Web Config.

[Configuração de ajustes básicos S/MIME](#)

[Configurações S/MIME](#)

[Configuração de um certificado para S/MIME](#)

[Importação de um certificado de criptografia para um destino de e-mail](#)

Tema principal: [Uso do seu produto em uma rede segura](#)

### Configuração de ajustes básicos S/MIME

Você pode configurar a criptografia e o anexo de assinatura digital para e-mail conforme necessário .

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob **S/MIME**, selecione **Básico**.

Você verá uma janela como esta:



3. Selecione uma configuração para cada opção.
4. Clique em **Avançar**.  
Você verá uma mensagem de confirmação.
5. Clique em **OK**.

**Tema principal:** [Configuração de ajustes S/MIME](#)

## Configurações S/MIME

### Criptografia do e-mail

Você precisa importar um certificado de criptografia para cada destino registrado na lista de contatos. E-mails não criptografados são enviados para destinatários que não tenham um certificado de encriptação importado.

| <b>Configuração</b>            | <b>Opções/Descrição</b>   |
|--------------------------------|---|
| <b>Digitalizar para e-mail</b> | <p>Selecione configurações para digitalizar para e-mail</p> <p><b>Encriptação:</b> para configurar encriptação de e-mail</p> <p><b>Não encriptar:</b> digitaliza para um destinatário de e-mail sem criptografia</p> <p><b>Selecionar durante a execução:</b> decide se o e-mail deve ou não ser criptografado antes de ser enviado</p> <p><b>Predefinição durante a execução:</b> seleciona a ação padrão quando <b>Selecionar durante a execução</b> está selecionado</p>               |
| <b>Caixa para e-mail</b>       | <p>Selecione configurações para carregar arquivos para e-mail</p> <p><b>Encriptação:</b> para configurar encriptação de e-mail</p> <p><b>Não encriptar:</b> carrega um arquivo para um destinatário de e-mail sem criptografia</p> <p><b>Selecionar durante a execução:</b> decide se o e-mail deve ou não ser criptografado antes de ser enviado</p> <p><b>Predefinição durante a execução:</b> seleciona a ação padrão quando <b>Selecionar durante a execução</b> está selecionado</p> |
| <b>Fax para e-mail</b>         | Configure a encriptação de e-mail quando enviar um fax para e-mail  |
| <b>Algoritmo</b>               | Selecione o algoritmo para encriptação de e-mail  |

### **Assinatura digital**

Você precisa configurar o certificado de cliente para incluir uma assinatura digital.

| Configuração                   | Opções/Descrição   |
|--------------------------------|--|
| <b>Digitalizar para e-mail</b> | <p>Selecione configurações para digitalizar para e-mail</p> <p><b>Adicionar assinatura:</b> adiciona uma assinatura digital a e-mails</p> <p><b>Não adicionar assinatura:</b> digitaliza para um destinatário de e-mail sem uma assinatura digital</p> <p><b>Selecionar durante a execução:</b> decide se uma assinatura digital deve ou não ser adicionada ao e-mail antes de ser enviado</p> <p><b>Predefinição durante a execução:</b> seleciona a ação padrão quando <b>Selecionar durante a execução</b> está selecionado</p>               |
| <b>Caixa para e-mail</b>       | <p>Selecione configurações para carregar arquivos para e-mail</p> <p><b>Adicionar assinatura:</b> adiciona uma assinatura digital a e-mails</p> <p><b>Não adicionar assinatura:</b> carrega um arquivo para um destinatário de e-mail sem uma assinatura digital</p> <p><b>Selecionar durante a execução:</b> decide se uma assinatura digital deve ou não ser adicionada ao e-mail antes de ser enviado</p> <p><b>Predefinição durante a execução:</b> seleciona a ação padrão quando <b>Selecionar durante a execução</b> está selecionado</p> |
| <b>Fax para e-mail</b>         | Configure a assinatura digital quando enviar um fax para e-mail  |
| <b>Algoritmo</b>               | Selecione o algoritmo para a assinatura digital  |

**Tema principal:** [Configuração de ajustes S/MIME](#)

**Tarefas relacionadas**

[Importação de um certificado de criptografia para um destino de e-mail](#)

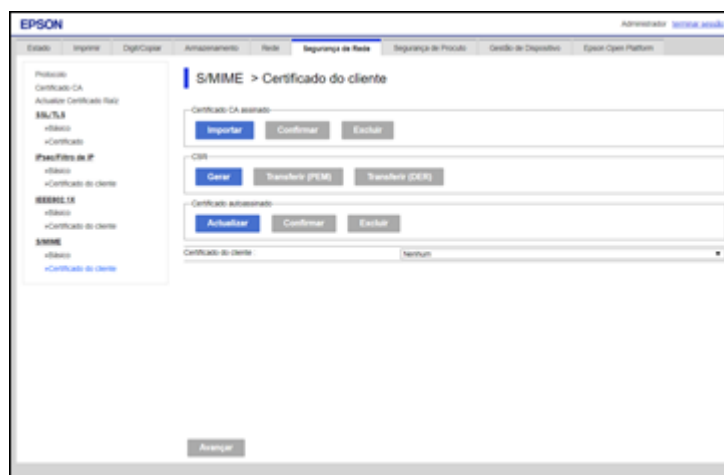
[Configuração de um certificado para S/MIME](#)

## Configuração de um certificado para S/MIME

Você pode configurar um certificado de cliente para usar a função de assinatura S/MIME.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob **S/MIME**, selecione **Certificado do cliente**.

Você verá uma janela como esta:



3. Selecione uma das seguintes opções:
  - **Certificado CA assinado**: selecione **Importar** se você obteve certificado CA assinado. Selecione o arquivo a ser importado e clique em **OK**.
  - **Certificado autoassinado**: selecione **Atualizar** se você não obteve um certificado CA (Certificate Authority) assinado e deseja que o produto gere um certificado autoassinado
4. Clique em **Avançar**.  
Você verá uma mensagem de confirmação.
5. Clique em **OK**.

**Tema principal:** [Configuração de ajustes S/MIME](#)

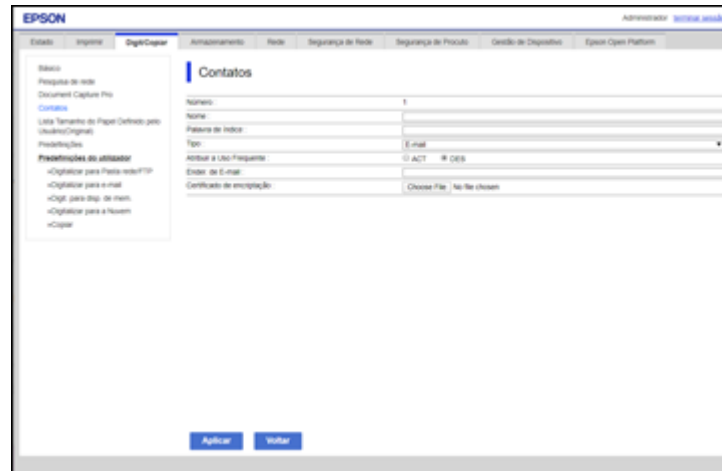
### Importação de um certificado de criptografia para um destino de e-mail

Você precisa importar um certificado de criptografia para cada destino de e-mail registrado na lista de contatos.



1. Acesse o Web Config e selecione a guia **Digit/Copiar** ou **Fax**.
2. Selecione **Contac**.
3. Selecione o número de destino para o qual deseja importar o certificado de criptografia e clique em **Editar**.

Você verá uma janela como esta:



4. Selecione **Email** como a configuração de **Tipo**.
5. Clique **Procurar** para selecionar o certificado de criptografia que deseja usar.
6. Selecione quaisquer outras configurações conforme necessário.
7. Clique em **Aplicar** quando terminar.

Um ícone de chave é exibido ao lado do destino na lista de contatos.

**Tema principal:** [Configuração de ajustes S/MIME](#)

**Referências relacionadas**

[Configurações S/MIME](#)

## Conexão do produto a uma rede IEEE 802.1X

Siga as instruções nessas seções para conectar o produto a uma rede IEEE 802.1X usando o Web Config.

Configuração de uma rede IEEE802.1X

Configurações da rede IEEE 802.1X

Configuração de um certificado para uma rede IEEE 802.1X

Estado da rede IEEE 802.1X

**Tema principal:** Uso do seu produto em uma rede segura

### Configuração de uma rede IEEE802.1X

Se seu produto suporta IEEE 802.1X, você pode usá-lo em uma rede com autenticação fornecida por um servidor RADIUS com um hub como autenticador usando o Web Config.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob **IEEE802.1X**, selecione **Básico**.

Você verá uma janela como esta:



3. Selecione **Ativar** como configuração de **IEEE802.1X (Rede com Fio)**.
4. Para usar o produto em uma rede Wi-Fi, habilite as configurações de Wi-Fi do seu produto. Consulte o *Manual do usuário* do seu produto para mais instruções.

O estado da conexão é exibido como a configuração **IEEE802.1X (Wi-Fi)**.

**Observação:** Você pode compartilhar as configurações de rede para Ethernet e Wi-Fi.

5. Selecione as opções de configurações IEEE 802.1X que deseja usar.
6. Clique em **Avançar**.  
Você verá uma mensagem de confirmação.
7. Clique em **OK**.

**Tema principal:** [Conexão do produto a uma rede IEEE 802.1X](#)

**Referências relacionadas**

[Configurações da rede IEEE 802.1X](#)

**Configurações da rede IEEE 802.1X**

Você pode configurar esses ajustes da rede IEEE 802.1X no Web Config.

| <b>Configuração</b>             | <b>Opções/Descrição</b>   |
|---------------------------------|---|
| <b>Método de Ligação</b>        | Exibe o método de conexão de rede atual.  |
| <b>Tipo EAP</b>                 | Selecione um desses métodos de autenticação para conexões entre o produto e um servidor RADIUS:<br><br><b>EAP-TLS</b> ou <b>PEAP-TLS</b> : Você deve obter e importar um certificado CA assinado.<br><br><b>PEAP/MSCHAPv2</b> ou <b>EAP-TTLS</b> : Você precisa configurar uma senha. |
| <b>ID do utilizador</b>         | Digite uma identificação entre 1 e 128 ASCII caracteres para autenticação em um servidor RADIUS.  |
| <b>Senha</b>                    | Digite uma senha entre 1 e 128 ASCII caracteres para autenticação do produto. Se estiver usando Windows como um servidor RADIUS, digite até 127 caracteres ASCII.   |
| <b>Confirmar palavra-passe</b>  | Digite a senha de autenticação novamente.   |
| <b>ID do servidor</b>           | Digite uma identificação do servidor entre 1 e 128 caracteres ASCII para autenticação em um servidor RADIUS especificado; a identificação do servidor é verificada no campo subject/subjectAltName de um certificado de servidor enviado de um servidor RADIUS.                       |
| <b>Validação de certificado</b> | Selecione um certificado válido independentemente do método de autenticação; importe o certificado usando a opção de <b>Certificado de CA</b> .   |

| Configuração         | Opções/Descrição  |
|----------------------|---|
| Nome Anônimo         | Se selecionou <b>EAP-TTLS</b> , <b>PEAP-TLS</b> ou <b>PEAP/MSCHAPv2</b> como a configuração de <b>Método de Autenticação</b> , você pode configurar um nome anônimo entre 1 e 128 caracteres ASCII ao invés de uma identificação de usuário para fase 1 de uma autenticação PEAP. |
| Força da encriptação | Selecione uma das seguintes forças de encriptação:<br><b>Alta</b> para AES256/3DES<br><b>Média</b> para AES256/3DES/AES128/RC4  |

Tema principal: [Conexão do produto a uma rede IEEE 802.1X](#)

### Configuração de um certificado para uma rede IEEE 802.1X

Se seu produto suporta IEEE 802.1X, você pode configurar um certificado para a rede usando o Web Config.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob **IEEE802.1X**, selecione **Certificado do cliente**.

Você verá uma janela como esta:



3. Clique em **Importar** para adicionar um novo certificado de cliente.

4. Clique em **OK**.

**Tema principal:** [Conexão do produto a uma rede IEEE 802.1X](#)

### Estado da rede IEEE 802.1X

Você pode verificar o estado das configurações da rede IEEE 802.1X imprimindo uma folha de estado do seu produto. Consulte o *Manual do usuário* do produto para instruções sobre impressão de uma folha de estado de rede.

A folha de estado de rede exibe as informações nesta tabela para redes IEEE 802.1X.

| Identificação do estado                                    | Descrição do estado   |
|--|---|
| Disable (Desativar)  | IEEE 802.1X está desativado   |
| EAP Success (EAP bem-sucedido)                             | Autenticação IEEE 802.1X está confirmada e a conexão de rede está disponível  |
| Authenticating (Autenticando)                              | Autenticação IEEE 802.1X em andamento   |
| Config Error (Erro de configuração)                        | Autenticação falhou porque a identificação de usuário não foi definida  |
| Client Certificate Error (Erro de certificado do cliente)  | Autenticação falhou porque o certificado de cliente está fora da validade   |
| Timeout Error (Erro de tempo esgotado)                     | Autenticação falhou porque não há resposta do servidor RADIUS e/ou do autenticador  |
| User ID Error (Erro de identificação de usuário)           | Autenticação falhou porque a identificação de usuário do produto e/ou o protocolo de certificado está incorreto   |
| Server ID Error (Erro de identificação de servidor)        | Autenticação falhou porque a identificação de servidor no certificado do servidor e a identificação do servidor não batem   |
| Server Certificate Error (Erro de certificado de servidor) | Autenticação falhou porque o certificado de servidor está fora da validade ou a cadeia do certificado de servidor está incorreta  |
| CA Certificate Error (Erro de certificado de CA)           | Autenticação falhou porque o certificado CA está incorreto, não importado ou fora da validade   |
| EAP Failure (Falha de EAP)                                 | Autenticação falhou porque o certificado de cliente está incorreto (EAP-TLS ou PEAP-TLS), ou a identificação de usuário ou senha estão incorretas (PEAP/MSCHAPv2 ou EAP-TTLS) |

**Tema principal:** [Conexão do produto a uma rede IEEE 802.1X](#)

## Uso de um certificado digital

Siga as instruções nessas seções para configurar e usar certificados digitais usando o Web Config.

[Sobre certificação digital](#)

[Obtenção e importação de Certificado CA assinado](#)

[Ajustes de configuração CSR](#)

[Configurações de importação CSR](#)

[Exclusão de certificado CA assinado](#)

[Atualização de um certificado auto-assinado](#)

**Tema principal:** [Uso do seu produto em uma rede segura](#)

### Sobre certificação digital

Você pode configurar os seguintes certificados digitais para sua rede usando Web Config:

#### **Certificado CA assinado**

Você pode garantir comunicações seguras usando um certificado CA assinado para cada recurso de segurança. Os certificados devem ser assinados por e obtidos de uma CA (autoridade de certificado).

#### **Certificado autoassinado**

Um certificado autoassinado é emitido e assinado pelo próprio produto. Você pode usar o certificado apenas para comunicação SSL/TLS, porém a segurança não é confiável e você pode ver um alerta de segurança no navegador durante o uso.

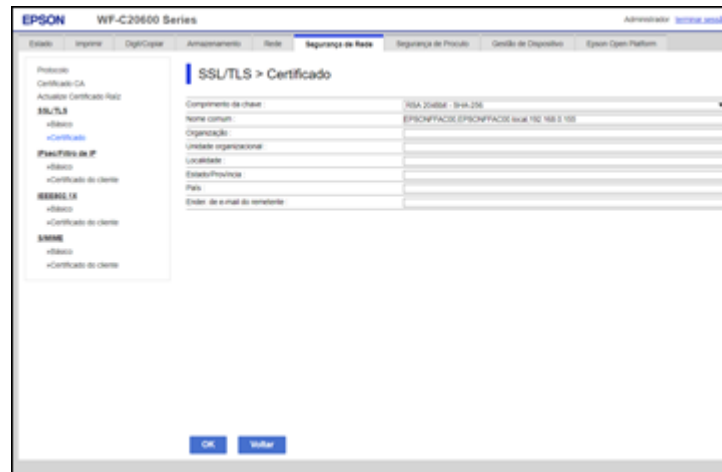
**Tema principal:** [Uso de um certificado digital](#)

### Obtenção e importação de Certificado CA assinado

Você pode obter um certificado CA assinado criando um CSR (Certificate Signing Request ou pedido de assinatura de certificado) usando Web Config e enviando a uma autoridade de certificado (CA). O CSR criado no Web Config é no formato PEM/DER. Você pode importar um CSR criado no Web Config de cada vez.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob uma das opções de segurança de rede a seguir, selecione o certificado correspondente:
  - **SSL/TLS e Certificado**
  - **IPsec/Filtro IP e Certificado de Cliente**
  - **IEEE802.1X e Certificado de Cliente**

3. Na seção CSR, selecione **Gerar**.  
Você verá uma janela como esta:



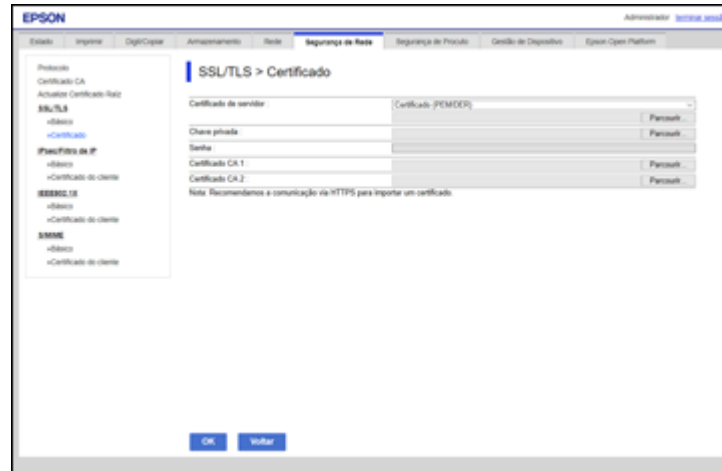
The screenshot shows the EPSON WF-C2060 Series web interface. The top navigation bar includes 'Estado', 'Impressão', 'Digitalização', 'Armazenamento', 'Rede', 'Segurança de Rede', 'Segurança de Produto', 'Configuração de Dispositivo', and 'Epson Open Platform'. The 'Segurança de Rede' tab is selected, and the 'SSL/TLS > Certificado' sub-tab is active. The left sidebar contains a tree view with categories: 'Protocolo' (Certificado CA, Atualizar Certificado Raiz), 'SSL/TLS' (Gerar, Importar), 'Protocolo de IP' (Gerar, Importar), 'SMB' (Gerar, Importar), and 'SMB' (Gerar, Importar). The main content area is titled 'SSL/TLS > Certificado' and contains a form with the following fields: 'Componente de chave' (set to RSA 2048 - SHA-256), 'Nome comum' (EPSONFACSE.EPSONFACSE local 192.168.1.100), 'Organização', 'Unidade organizacional', 'Localidade', 'Estado/província', 'País', and 'Endereço de e-mail do remetente'. At the bottom of the form are 'OK' and 'Cancelar' buttons.

4. Selecione as opções de configuração de CSR que deseja usar.
5. Clique em **OK**.  
Você verá uma mensagem de conclusão.
6. Selecione a guia **Segurança de Rede** novamente e selecione a opção de segurança da rede e o certificado correspondente.
7. Na seção CSR, clique na opção **Transferir** que seja igual ao formato especificado pela sua autoridade de certificado para baixar o CSR.

**Cuidado:** Não gere outro CSR senão você poderá não ser capaz de importar um certificado CA assinado.

8. Envie o CSR à autoridade de certificado seguindo as diretrizes de formato fornecidas pela autoridade.
9. Salve o certificado CA assinado emitido em um computador conectado ao produto.  
Antes de prosseguir, as configurações de data e hora do produto devem estar corretas. Consulte o *Manual do usuário* do produto para mais instruções.

10. Selecione a guia **Segurança de Rede** novamente e selecione a opção de segurança da rede e o certificado correspondente.
11. Na seção Certificado CA assinado, clique em **Importar**.  
Você verá uma janela como esta:



12. Selecione o formato do certificado como configuração de **Certificado de Servidor**.
13. Selecione as configurações de importação de certificado conforme necessário para o formato e a fonte para a qual você o obteve.
14. Clique em **OK**.  
Você verá uma mensagem de confirmação.
15. Clique em **Confirmar** para verificar a informação do certificado.

**Tema principal:** [Uso de um certificado digital](#)

#### **Referências relacionadas**

[Ajustes de configuração CSR](#)

[Configurações de importação CSR](#)

#### **Ajustes de configuração CSR**

Você pode selecionar essas configurações ao configurar um CSR no Web Config.



**Observação:** O tamanho da chave e abreviações disponíveis variam de acordo com a autoridade de certificado (CA), então siga as regras daquela autoridade ao digitar informações no CSR.

| Configuração   | Opções/Descrição  |
|--|---|
| <b>Comprimento de chave</b>  | Selecione um tamanho da chave para o CSR  |
| <b>Nome Comum</b>  | Digite um nome ou endereço de IP estático de 1 a 128 caracteres; por exemplo, <b>Impressora da recepção</b> ou <b>https://10.152.12.225</b> |
| <b>Organização, Unidade organizacional, Localidade, Estado/Província</b> | Digite informações em cada campo conforme necessário, de 0 a 64 caracteres em ASCII; separe múltiplos nomes com vírgulas                    |
| <b>País</b>  | Digite um código de país de dois dígitos conforme especificado pelo padrão ISO-316  |
| <b>Endereço de e-mail do remetente</b>                                   | Digite o endereço de e-mail do remetente para a configuração de servidor de e-mail.   |

**Tema principal:** [Uso de um certificado digital](#)

### Configurações de importação CSR

Você pode configurar esses ajustes ao importar um CSR no Web Config.

**Observação:** Os requisitos de configuração de importação variam de acordo com o formato do certificado e como você obteve o certificado.

| Formato de certificado                  | Descrições de configuração  |
|---|---|
| Formato PEM/DER obtido do Web Config    | <b>Chave privada:</b> Não configure porque o produto contém uma chave particular<br><b>Senha:</b> Não configure<br><b>Certificado CA 1/Certificado CA 2:</b> Opcional |
| Formato PEM/DER obtido de um computador | <b>Chave privada:</b> Configure uma chave particular<br><b>Senha:</b> Não configure<br><b>Certificado CA 1/Certificado CA 2:</b> Opcional                             |

| Formato de certificado                  | Descrições de configuração   |
|---|--|
| Formato PKCS#12 obtido de um computador | <p><b>Chave Particular:</b> Não configure</p> <p><b>Senha:</b> Opcional</p> <p><b>Certificado CA 1/Certificado CA 2:</b> Não configure</p> |

**Tema principal:** [Uso de um certificado digital](#)

### Exclusão de certificado CA assinado

Você pode excluir um certificado CA assinado com Web Config quando o certificado vence ou se não tem mais necessidade de uma conexão codificada.

**Observação:** Se você obteve um certificado CA assinado do Web Config, você não pode importar um certificado excluído; você deve obter e importar um novo certificado.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob uma das opções de segurança de rede a seguir, selecione o certificado correspondente:
  - **SSL/TLS e Certificado**
  - **IPsec/Filtro IP e Certificado de Cliente**
  - **IEEE802.1X e Certificado de Cliente**
  - **S/MIME e Certificado de Cliente**
3. Clique em **Excluir**.  
Você verá uma mensagem de conclusão.
4. Clique em **OK**.

**Tema principal:** [Uso de um certificado digital](#)

### Atualização de um certificado auto-assinado

Se seu produto suporta o recurso de servidor HTTPS, você pode atualizar o certificado autoassinado usando o Web Config.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Sob uma das opções de segurança de rede a seguir, selecione o certificado correspondente:
  - **SSL/TLS e Certificado**
  - **S/MIME e Certificado de Cliente (WF-C879R)**

**Observação:** Quando atualizar um certificado autoassinado para S/MIME, você não pode modificar o endereço de e-mail do remetente na guia **Rede > Servidor de e-mail > Básico**. É necessário que modifique todas as configurações de assinatura para **Não adicionar assinatura** na guia **Segurança de Rede > S/MIME > Básico** e depois apague o certificado autoassinado para S/MIME.

3. Sob **Certificado autoassinado**, clique em **Atualizar**.

Você verá uma janela como esta:

The screenshot displays the EPSON administration web interface. The top navigation bar includes 'Estado', 'Impressão', 'Digital Copier', 'Armazenamento', 'Rede', 'Segurança de Rede', 'Segurança de Protocolo', 'Configuração de Dispositivos', and 'Epson Open Platform'. The 'Segurança de Rede' tab is active, showing 'SSL/TLS > Certificado'. The left sidebar lists various security settings: 'Proteção', 'Certificado CA', 'Atualizar Certificado Root', 'SSL/TLS', 'Filtro de IP', 'S/MIME', and 'S/MIME'. The main content area contains the following fields:

- Complemento da chave: RSA 2048 - 1024 bits
- Nome comum: EPSONFACE.EPSONFACE.ACUL192.168.1.192
- Organização: SEPO EPSON CORP
- Data válida (UTC): 2020-04-03 21:59:43 UTC
- Validade do certificado (ano): 10
- Endereço de e-mail do remetente: (empty)

At the bottom of the form are two buttons: 'Avançar' and 'Voltar'.

4. Digite um identificador para o seu produto de 1 a 128 caracteres no campo **Nome Comum**.

**Observação:** Você pode adicionar até 5 endereços IPv4, endereços IPv6, nomes de anfitrião ou FQDNs; separados por vírgulas. O primeiro valor é designado ao campo Nome Comum e o resto é adicionado ao campo Alias do assunto do certificado. Você não pode adicionar um espaço antes ou depois de uma vírgula.

5. Selecione um período de validade para o certificado como configuração de **Validade do Certificado (ano)**.
6. Clique em **Avançar**.  
Você verá uma mensagem de conclusão.
7. Clique em **OK**.

8. Clique em **Confirmar** para verificar a informação do certificado.

**Tema principal:** [Uso de um certificado digital](#)

## Uso de um servidor LDAP

Siga as instruções nessas seções para usar um servidor LDAP para fornecer informações de destino de e-mail e fax usando o Web Config.

[Configuração do servidor LDAP e seleção de configurações de busca](#)

[Configuração do servidor LDAP](#)

[Configurações de busca LDAP](#)

[Verificação da conexão do servidor LDAP](#)

[Mensagens de relatório de conexão LDAP](#)

**Tema principal:** [Uso do seu produto em uma rede segura](#)

## Configuração do servidor LDAP e seleção de configurações de busca

Você pode configurar o servidor LDAP e selecionar configurações de busca para ele usando o Web Config.

1. Acesse o Web Config e selecione a guia **Rede**.
2. Sob **Servidor LDAP**, selecione **Básico**.

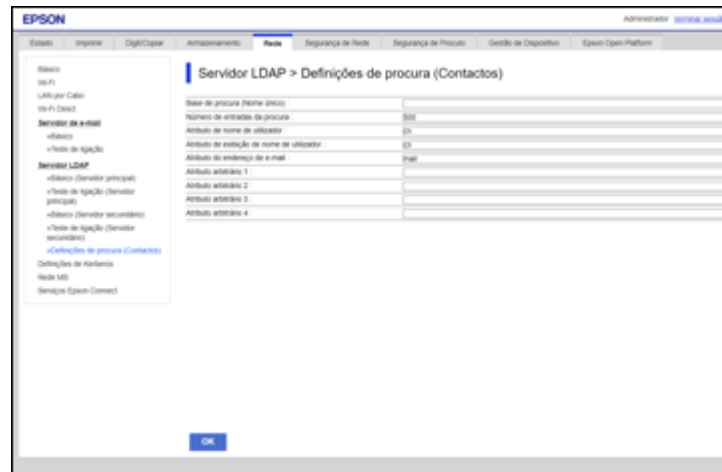
**Observação:** Você pode selecionar o servidor primário ou secundário, conforme necessário.

Você verá uma janela como esta:



3. Selecione **Usar** como configuração de **Usar Servidor LDAP**.
4. Selecione as configurações do servidor LDAP.
5. Clique em **OK**.
6. Selecione a guia **Rede**, se necessário.
7. Sob **Servidor LDAP**, selecione **Definições de procura(Contatos)**.

Você verá uma janela como esta:



8. Selecione as configurações de procura LDAP que deseja usar.
9. Clique em **OK**.

**Tema principal:** [Uso de um servidor LDAP](#)

**Referências relacionadas**

[Configuração do servidor LDAP](#)

[Configurações de busca LDAP](#)

### Configuração do servidor LDAP

Você pode configurar esses ajustes do servidor LDAP no Web Config.

| Configuração                            | Opções/Descrição   |
|---|--|
| <b>Endereço dos Servidores LDAP</b>     | <p>Digite o endereço do servidor LDAP conforme necessário, dependendo do formato do servidor:</p> <ul style="list-style-type: none"> <li>• Formato IPv4 ou IPv6: Digite de 1 a 255 caracteres</li> <li>• Formato FQDN: Digite de 1 a 255 caracteres alfanuméricos em ASCII; você pode usar "-", exceto no início ou no fim de um endereço</li> </ul> |
| <b>Número de Porta do Servidor LDAP</b> | <p>Digite o número de porta do servidor LDAP entre 1 e 65535</p>   |

| Configuração                        | Opções/Descrição  |
|-------------------------------------|---|
| Ligação segura                      | Selecione o método de criptografia para conexão ao servidor LDAP.   |
| Validação de certificado            | Selecione <b>Ativar</b> para validar o certificado quando fizer a conexão ao servidor LDAP.   |
| Tempo limite de procura (seg.)      | Digite um intervalo de tempo de busca antes de o tempo esgotar entre 5 e 300 segundos   |
| Método de autenticação              | Selecione um dos métodos de autenticação disponíveis listados   |
| Domínio Kerberos a utilizar         | Se selecionou <b>Autenticação Kerberos</b> como a opção de <b>Método de autenticação</b> , selecione o domínio de autenticação Kerberos correto dos domínios definidos sob o item de menu <b>Definições de Kerberos</b> .   |
| Administrador DN/Nome de utilizador | Deixe este espaço em branco ou digite um nome de usuário para o servidor LDAP de 0 a 128 caracteres em Unicode (UTF-8); não use caracteres de controle tais como 0x00-0x1F ou OX7F (não disponível quando selecionou <b>Autenticação anônima</b> como opção de <b>Método de autenticação</b> )      |
| Palavra-passe                       | Deixe este espaço em branco ou digite uma senha de 1 a 128 caracteres em Unicode (UTF-8) para autenticação do servidor LDAP; não use caracteres de controle tais como 0x00-0x1F ou OX7F (não disponível quando selecionou <b>Autenticação anônima</b> como opção de <b>Método de autenticação</b> ) |
| <b>Definições de Kerberos</b>       |   |
| Domínio                             | Se selecionou <b>Autenticação Kerberos</b> como o <b>Método de autenticação</b> , digite o escopo de autenticação Kerberos de 0 a 255 caracteres em ASCII; você pode definir até 10 domínios com endereços e números de porta associados.   |
| Endereço KDC                        | Deixe este espaço em branco ou, se selecionou <b>Autenticação Kerberos</b> como o <b>Método de autenticação</b> , digite o endereço de servidor de autenticação Kerberos de 0 a 255 caracteres em formato IPv4, IPv6 ou FQDN  |
| Número da porta (Kerberos)          | Deixe este espaço em branco ou, se selecionou <b>Autenticação Kerberos</b> como o <b>Método de autenticação</b> , digite o número de porta do servidor Kerberos entre 1 e 65535   |

Tema principal: [Uso de um servidor LDAP](#)

### Configurações de busca LDAP

Você pode configurar esses ajustes de busca LDAP no Web Config.

| Configuração   | Opções/Descrição   |
|--|--|
| <b>Base de procura (Nome Distinto)</b>               | Deixe em branco ou busque por um nome de domínio arbitrário no servidor LDAP usando de 1 a 128 caracteres Unicode (UTF-8)  |
| <b>Número de entradas de procura</b>                 | Especifique o número máximo de entradas de busca antes que uma mensagem de erro apareça, de 1 a 500  |
| <b>Atributo de nome de utilizador</b>                | Digite o nome do atributo para exibir ao buscar nomes de usuários de 1 a 255 caracteres em Unicode (UTF-8); o primeiro caractere deve ser a-z, ou A-Z                          |
| <b>Atributo de exibição de nome de usuário</b>       | Deixe em branco ou digite o nome do atributo para exibir como o nome de usuário de 1 a 255 caracteres em Unicode (UTF-8); o primeiro caractere deve ser a-z, ou A-Z            |
| <b>Atributo de número de fax</b>                     | Digite o nome do atributo para exibir ao buscar números de fax de 1 a 255 caracteres usando A-Z, a-z, 0-9, e "-" em Unicode (UTF-8); o primeiro caractere deve ser a-z, ou A-Z |
| <b>Atributo de endereço de e-mail</b>                | Deixe em branco ou digite o nome do atributo para exibir ao buscar por endereços de e-mail de 1 a 255 caracteres em Unicode (UTF-8); o primeiro caractere deve ser a-z, ou A-Z |
| <b>Atributo Arbitrário 1 a Atributo Arbitrário 4</b> | Deixe em branco ou especifique outros atributos para buscar de 1 a 255 caracteres em Unicode (UTF-8); o primeiro caractere deve ser a-z, ou A-Z                                |

Tema principal: [Uso de um servidor LDAP](#)

### Verificação da conexão do servidor LDAP

Você pode testar a conexão do servidor LDAP e visualizar um relatório de conexão usando Web Config.

1. Acesse o Web Config e selecione a guia **Rede**.
2. Sob **Servidor LDAP**, selecione **Testar Conexão**.

**Observação:** Você pode selecionar o servidor primário ou secundário, conforme necessário.



3. Clique em **Iniciar**.

O Web Config testa a conexão e exibe o relatório de conexão quando termina.

**Tema principal:** [Uso de um servidor LDAP](#)

### Mensagens de relatório de conexão LDAP

Você pode revisar as mensagens de relatório de conexão para diagnosticar problemas com a conexão LDAP no Web Config.

| Mensagem   | Descrição   |
|--|---|
| <b>O teste de ligação foi concluído com sucesso</b>  | A conexão com o servidor foi bem-sucedida.  |
| <b>O teste de ligação falhou. Verifique as definições.</b>                                 | Uma das seguintes condições ocorreu: <ul style="list-style-type: none"><li>• O endereço do servidor LDAP ou número da porta está incorreto</li><li>• O tempo se esgotou.</li><li>• Você selecionou <b>Não Usar</b> como configuração de <b>Usar Servidor LDAP</b></li><li>• Se selecionou <b>Autenticação Kerberos</b> como configuração de <b>Método de Autenticação</b>, as configurações do servidor Kerberos estão incorretas</li></ul> |
| <b>O teste de ligação falhou. Verifique a data e a hora na sua impressora ou servidor.</b> | A conexão falhou porque as configurações de hora para o produto e servidor LDAP não batem.  |
| <b>A autenticação falhou. Verifique as definições.</b>                                     | Autenticação falhou porque as configurações de Nome de usuário e Senha estão incorretas ou se selecionou <b>Autenticação Kerberos</b> como configuração de <b>Método de autenticação</b> , a data e a hora não estão configuradas corretamente.   |
| <b>Não pode acessar a impressora até o processamento estar concluído</b>                   | O produto está ocupado  |

**Tema principal:** [Uso de um servidor LDAP](#)

### Configuração de protocolos em Web Config

Você pode ativar ou desativar protocolos usando o Web Config.

1. Acesse o Web Config e selecione a guia **Segurança de Rede**.
2. Selecione ou desmarque a caixa ao lado do nome do serviço para ativar ou desativar um protocolo.
3. Defina quaisquer outras configurações de protocolo.
4. Clique em **Avançar**.
5. Clique em **OK**.

Depois dos protocolos reiniciarem, as modificações são aplicadas.

[Configurações de protocolo](#)

**Tema principal:** [Uso do seu produto em uma rede segura](#)

## Configurações de protocolo

### Protocolos

| Nome                            | Descrição   |
|---------------------------------|---|
| <b>Bonjour</b>                  | Bonjour é usado para procurar por dispositivos e AirPrint.                |
| <b>SLP</b>                      | SLP é usado para push-scanning e busca em rede no EpsonNet Config.        |
| <b>WSD</b>                      | Adicione dispositivos WSD ou imprima e digitalize da porta WSD.           |
| <b>LLTD</b>                     | Exibe o produto no mapa da rede do Windows.                               |
| <b>LLMNR</b>                    | Use resolução de nome sem NetBIOS, mesmo que não possa usar DNS.          |
| <b>LPR</b>                      | Imprima a partir da porta LPR.  |
| <b>RAW(Porta9100)</b>           | Imprima a partir da porta RAW (Porta 9100).                               |
| <b>RAW(Porta personalizada)</b> | Imprima a partir da porta RAW (Porta personalizada).                      |
| <b>IPP</b>                      | Imprima pela internet, incluindo AirPrint.                                |
| <b>FTP</b>                      | Imprima por FTP.  |
| <b>SNMPv1/v2c</b>               | Configure e monitore o seu produto remotamente.                           |
| <b>SNMPv3</b>                   | Configure e monitore o seu produto remotamente usando o protocolo SNMPv3. |

### Configurações Bonjour

| Configuração                   | Opções/Descrição  |
|--------------------------------|---|
| Utilizar Bonjour               | Procure e use dispositivos através do Bonjour   |
| Nome Bonjour                   | Exibe o nome do Bonjour.  |
| Nome de Serv. Bonjour          | Exibe o nome de serviço do Bonjour.   |
| Localização                    | Exibe o nome da localização do Bonjour.   |
| Protocolo de Prioridade Máxima | Selecione o protocolo que é de mais alta prioridade para impressão com Bonjour.                                   |
| Wide-Area Bonjour              | Ativa o protocolo Wide-Area Bonjour; registre todos os produtos no servidor DNS para localizá-los em um segmento. |

### Configurações SLP

| Configuração | Opções/Descrição  |
|--------------|---|
| Activar SLP  | Ative a função SLP para usar a função Push Scan e busca em rede no EpsonNet Config. |

### Configurações WSD

| Configuração                        | Opções/Descrição   |
|-------------------------------------|--|
| Activar WSD                         | Ative a adição de dispositivos usando WSD, e a impressão e digitalização a partir da porta WSD.  |
| Tempo limite de impressão (seg)     | Digite um valor para interrupção da comunicação para impressão WSD entre 3 e 3.600 segundos.     |
| Tempo limite de digitalização (seg) | Digite um valor para interrupção da comunicação para digitalização WSD entre 3 e 3.600 segundos. |
| Nome do dispositivo                 | Exibe o nome do dispositivo WSD.   |
| Localização                         | Exibe o nome da localização do WSD.  |

### Configurações LLTD

| Configuração        | Opções/Descrição   |
|---------------------|--|
| Activar LLTD        | Ative LLTD para exibir o produto no mapa da rede do Windows. |
| Nome do dispositivo | Exibe o nome do dispositivo LLTD.                            |

### Configurações LLMNR

| Configuração  | Opções/Descrição   |
|---------------|--|
| Activar LLMNR | Ative LLMNR para usar a resolução de nome sem NetBIOS, mesmo que não possa usar DNS. |

### Configurações LPR

| Configuração                    | Opções/Descrição   |
|---------------------------------|--|
| Permitir impressão da porta LPR | Permita a impressão a partir da porta LPR.                       |
| Tempo limite de impressão (seg) | Digite um valor para impressão LPR que entre 0 e 3.600 segundos. |

### Configurações RAW (Porta9100)

| Configuração                       | Opções/Descrição   |
|------------------------------------|--|
| Permitir impressão RAW (Porta9100) | Permita impressão a partir da porta RAW (Porta 9100).  |
| Tempo limite de impressão (seg)    | Digite um valor de limite de tempo para a impressão usando a porta RAW (Porta 9100), entre 0 e 3.600 segundos. |

### Configurações RAW (porta personalizada)

| Configuração                                 | Opções/Descrição  |
|--|---|
| Permitir impressão RAW (Porta personalizada) | Permita a impressão a partir da porta RAW (porta personalizada).                          |
| Número da porta                              | Digite o número da porta para impressão RAW entre 1024 e 65535 (exceto 9100, 1865 e 2968) |

| <b>Configuração</b>                    | <b>Opções/Descrição</b>   |
|--|---|
| <b>Tempo limite de impressão (seg)</b> | Digite um valor de limite de tempo para a impressão usando a porta RAW (porta personalizada), entre 0 e 3.600 segundos. |

### Configurações IPP

| <b>Configuração</b>                      | <b>Opções/Descrição</b>   |
|--|---|
| <b>Activar IPP</b>                       | Ative a comunicação IPP para produtos que suportem IPP sejam exibidos (você não pode usar AirPrint se estiver desativado).  |
| <b>Permitir comunicação não segura</b>   | Permite que a impressora se comunique sem qualquer medida de segurança (IPP).   |
| <b>Tempo limite de comunicação (seg)</b> | Digite um valor para impressão IPP entre 0 e 3.600 segundos.  |
| <b>URL(Rede)</b>                         | Exibe os URLs de IPP (http e https) quando o produto está conectado usando LAN com fios ou Wi-Fi (o URL é o valor combinado do endereço IP do produto, número da porta e nome IPP da impressora). |
| <b>URL(Wi-Fi Direct)</b>                 | Exibe os URLs de IPP (http e https) quando o produto está conectado usando Wi-Fi Direct (o URL é o valor combinado do endereço IP do produto, número da porta e nome IPP da impressora).          |
| <b>Nome da impressora</b>                | Exibe o nome IPP da impressora.   |
| <b>Localização</b>                       | Exibe a localização do IPP.   |

### Configurações FTP

| <b>Configuração</b>                      | <b>Opções/Descrição</b>   |
|--|---|
| <b>Activar Servidor FTP</b>              | Ative a impressão FTP para produtos que suportem impressão FTP.               |
| <b>Tempo limite de comunicação (seg)</b> | Digite um valor para interrupção da comunicação FTP entre 3 e 3.600 segundos. |

### Configurações SNMPv1/v2c

| Configuração                         | Opções/Descrição  |
|--------------------------------------|---|
| Activar SNMPv1/v2c                   | Ative SNMPv1/v2c para produtos que suportem SNMPv3.   |
| Autoridade de acesso                 | Defina a autoridade de acesso quando SNMPv1/v2c estiver ativado para <b>Apenas leitura ou Escrita/leitura</b> . |
| Nome da comunidade (Apenas leitura)  | Digite entre 0 e 32 caracteres ASCII.   |
| Nome da comunidade (Escrita/leitura) | Digite entre 0 e 32 caracteres ASCII.   |

### Configurações SNMPv3

| Configuração               | Opções/Descrição  |
|----------------------------|---|
| Ative SNMPv3               | Ative SNMPv3 para produtos que suportem SNMPv3.                 |
| Nome de utilizador         | Digite entre 1 e 32 caracteres.                                 |
| Definições de autenticação | Selecione um algoritmo e determine uma senha para autenticação. |
| Definições de encriptação  | Selecione um algoritmo e determine uma senha para encriptação.  |
| Nome do contexto           | Digite entre 1 e 32 caracteres.                                 |

Tema principal: [Configuração de protocolos em Web Config](#)

Referências relacionadas

[Configurações SNMPv3](#)

## Uso de um servidor de e-mail

Siga as instruções nessas seções para usar um servidor de e-mail para enviar dados de scan e fax por e-mail, ou usar notificação por e-mail usando o Web Config.

[Configuração de um servidor de e-mail](#)

[Configuração do servidor de e-mail](#)

[Verificação da conexão do servidor de e-mail](#)

[Mensagens de relatório de conexão do servidor de e-mail](#)

## Configuração de notificação por e-mail

**Tema principal:** [Uso do seu produto em uma rede segura](#)

### Configuração de um servidor de e-mail

Você pode configurar um servidor de e-mail usando o Web Config.

1. Acesse o Web Config e selecione a guia **Rede**.
2. Sob **Servidor de e-mail**, selecione **Básico**.

Você verá uma janela como esta:



3. Selecione as configurações do servidor de e-mail.
4. Clique em **OK**.

**Tema principal:** [Uso de um servidor de e-mail](#)

### Referências relacionadas

[Configuração do servidor de e-mail](#)

### Configuração do servidor de e-mail

Você pode configurar esses ajustes de servidor de e-mail no Web Config.

| Configuração                            | Opções/Descrição   |
|---|--|
| <b>Método de autenticação</b>           | Selecione o método de autenticação que seja igual o seu servidor de e-mail   |
| <b>Conta autenticada</b>                | Digite o nome da conta autenticada de 1 a 255 caracteres em ASCII  |
| <b>Palavra-passe autenticada</b>        | Digite a senha autenticada de 1 a 20 caracteres em ASCII usando A-Z, a-z, 0-9 e esses caracteres:<br>! # \$ % ' * + - . / = ? ^ _ { ! } ~ @                  |
| <b>Endereço de e-mail do remetente</b>  | Digite o endereço de e-mail do remetente de 1 a 255 caracteres em ASCII; não use ponto (.) como o primeiro caractere nem use esses caracteres: ( ) < > [ ] ; |
| <b>Endereço do servidor SMTP</b>        | Digite o endereço do servidor SMTP de 1 a 255 caracteres usando A-Z, a-z, 0-9 e "-" no formato IPv4 ou FQDN  |
| <b>Número da porta do servidor SMTP</b> | Digite o número de porta do servidor SMTP entre 1 e 65535  |
| <b>Ligação segura</b>                   | Selecione o método de segurança para o servidor de e-mail; opções disponíveis dependem da configuração de <b>Método de autenticação</b>                      |
| <b>Validação de certificado</b>         | Ative a verificação de certificados válidos; a opção recomendada é <b>Ativar</b>   |
| <b>Endereço do servidor POP3</b>        | Digite o endereço do servidor POP de 1 a 255 caracteres usando A-Z, a-z, 0-9 e "-" no formato IPv4 ou FQDN   |
| <b>Número da porta do servidor POP3</b> | Digite o número de porta do servidor POP entre 1 e 65535   |

**Tema principal:** [Uso de um servidor de e-mail](#)

#### Verificação da conexão do servidor de e-mail

Você pode testar a conexão do servidor de e-mail e visualizar um relatório de conexão usando Web Config.

1. Acesse o Web Config e selecione a guia **Rede**.
2. Sob **Servidor de e-mail**, selecione **Teste de ligação**.
3. Clique em **Iniciar**.

Web Config testa a conexão e exibe o relatório de conexão quando termina.

**Tema principal:** [Uso de um servidor de e-mail](#)



## Mensagens de relatório de conexão do servidor de e-mail

Você pode revisar as mensagens de relatório de conexão para diagnosticar problemas com a conexão do servidor de e-mail no Web Config.

| Mensagem   | Descrição  |
|--|--|
| <b>O teste de ligação foi concluído com sucesso</b>  | A conexão com o servidor foi bem-sucedida  |
| <b>Erro de comunicação com o servidor SMTP Verifique o seguinte - Configurações de Rede</b>  | Uma das seguintes condições ocorreu: <ul style="list-style-type: none"><li>• O produto não está conectado a uma rede</li><li>• O servidor SMTP está fora do ar</li><li>• A conexão com a rede foi interrompida durante a comunicação</li><li>• Dados incompletos foram recebidos</li></ul> |
| <b>Erro de comunicação com o servidor POP3 Verifique o seguinte - Configurações de Rede</b>  | Uma das seguintes condições ocorreu: <ul style="list-style-type: none"><li>• O produto não está conectado a uma rede</li><li>• O servidor POP3 está fora do ar</li><li>• A conexão com a rede foi interrompida durante a comunicação</li><li>• Dados incompletos foram recebidos</li></ul> |
| <b>Ocorreu um erro ao se conectar ao servidor SMTP. Verifique o seguinte - Endereço do servidor SMTP - Servidor DNS</b>                | Uma das seguintes condições ocorreu: <ul style="list-style-type: none"><li>• A resolução DNS falhou</li><li>• A resolução de nome para um servidor SMTP falhou</li></ul>   |
| <b>Ocorreu um erro ao se conectar ao servidor POP3. Verifique o seguinte - Endereço do servidor POP3 - Servidor DNS</b>                | Uma das seguintes condições ocorreu: <ul style="list-style-type: none"><li>• A resolução DNS falhou</li><li>• A resolução de nome para um servidor POP3 falhou</li></ul>   |
| <b>Erro de autenticação com o servidor SMTP. Verifique o seguinte - Método de autenticação - Conta autenticada - Senha autenticada</b> | A autenticação do servidor SMTP falhou   |

| <b>Mensagem</b>  | <b>Descrição</b>   |
|--|--|
| <b>Erro de autenticação com o servidor POP3. Verifique o seguinte - Método de autenticação - Conta autenticada - Senha autenticada</b> | A autenticação do servidor POP3 falhou   |
| <b>Método de comunicação não suportado. Verifique o seguinte - Endereço do servidor SMTP - Número da porta do servidor SMTP</b>        | O protocolo de comunicação não é suportado   |
| <b>Conexão ao servidor SMTP falhou. Mude conexão segura para Nenhum.</b>   | Existe uma desigualdade de SMTP entre um servidor e um cliente, ou quando o servidor não suporta uma conexão segura SMTP     |
| <b>Conexão ao servidor SMTP falhou. Mude conexão segura para SSL/TLS.</b>  | Existe uma desigualdade de SMTP entre um servidor e um cliente, ou o servidor solicita uma conexão SSL/TLS para SMTP         |
| <b>Conexão ao servidor SMTP falhou. Mude conexão segura para STARTTLS.</b>   | Existe uma desigualdade de SMTP entre um servidor e um cliente, ou quando o servidor solicita uma conexão STARTTLS para SMTP |
| <b>A conexão não é de confiança. Verifique o seguinte - Data e hora</b>  | A configuração de data e hora do produto está incorreta ou o certificado venceu  |
| <b>A conexão não é de confiança. Verifique o seguinte - Certificado de CA</b>  | O produto possui uma desigualdade de certificado de raiz ou um certificado CA não foi importado                              |
| <b>A conexão não é segura.</b>   | O certificado está danificado  |
| <b>A autenticação do servidor SMTP falhou. Mude o método de autenticação para SMTP-AUTH.</b>   | Desigualdade de método de autenticação entre um servidor e um cliente. O servidor não suporta SMTP AUTH.                     |
| <b>A autenticação do servidor SMTP falhou. Mude o método de autenticação para POP antes de SMTP.</b>                                   | Desigualdade de método de autenticação entre um servidor e um cliente. O servidor não suporta SMTP AUTH.                     |
| <b>Endereço de e-mail do remetente está incorreto. Mude para o endereço de e-mail do seu serviço de e-mail.</b>                        | O endereço de e-mail do remetente especificado está errado   |

| Mensagem  | Descrição              |
|---|------------------------|
| Não pode acessar a impressora até o processamento estar concluído | O produto está ocupado |

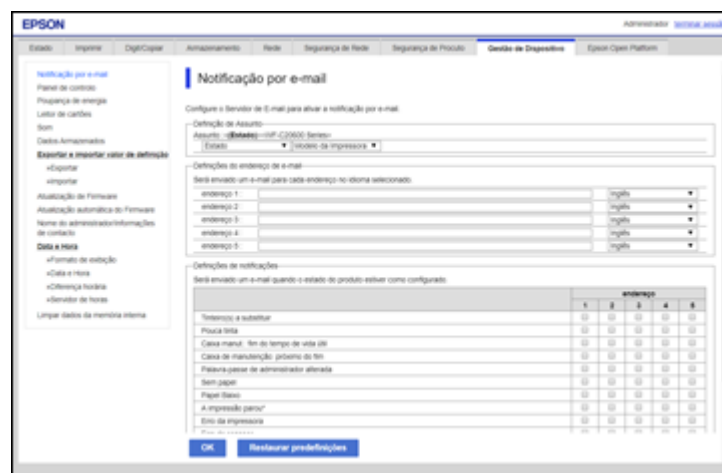
Tema principal: [Uso de um servidor de e-mail](#)

### Configuração de notificação por e-mail

Você pode configurar notificações por e-mail usando o Web Config para você poder receber alertas por e-mail quando certos eventos ocorrerem no produto, tais como ficando sem papel. Você pode registrar até 5 endereços de e-mail e selecionar os eventos para os quais você deseja ser notificado.

1. Acesse o Web Config e selecione a guia **Gestão de Dispositivo**.

Você verá uma janela como esta:



2. Digite um endereço de e-mail no campo **Endereço 1**.
3. Selecione o idioma no qual você deseja receber as notificações por e-mail a partir do menu para o primeiro endereço de e-mail.
4. Digite endereços de e-mail adicionais em cada campo, conforme necessário, e selecione o idioma para cada um.
5. Selecione as caixas de diálogo para indicar os eventos dos quais você deseja receber notificações por e-mail.

6. Clique em **OK**.

**Tema principal:** [Uso de um servidor de e-mail](#)

---

# Uso do software de configuração de rede EpsonNet Config

Siga as instruções nessas seções para fazer as configurações de rede administradora usando o software EpsonNet Config.

No Windows, você pode fazer as configurações de rede em uma operação em lote. Consulte o utilitário de ajuda do EpsonNet Config para instruções.

**Observação:** Antes de poder fazer as configurações de administração do sistema, precisa conectar o produto a uma rede. Consulte o *Manual do usuário* do produto para mais instruções.

[Instalação do EpsonNet Config](#)

[Configuração de um endereço IP do produto usando EpsonNet Config](#)



## Instalação do EpsonNet Config

Para instalar o EpsonNet Config, baixe o software da página de suporte do produto no endereço [epson.com.br/suporte](http://epson.com.br/suporte) e siga as instruções na tela.

**Tema principal:** [Uso do software de configuração de rede EpsonNet Config](#)

## Configuração de um endereço IP do produto usando EpsonNet Config

Você pode configurar o endereço IP do produto usando o EpsonNet Config.

1. Ligue o produto.
2. Conecte o produto a uma rede usando um cabo de Ethernet.
3. Siga um destes passos para iniciar o EpsonNet Config:
  - **Windows 10:** Clique em  > **Todos os aplicativos > EpsonNet > EpsonNet Config.**
  - **Windows 8.x:** Navegue até a tela **Aplicativos** e selecione **EpsonNet > EpsonNet Config.**
  - **Windows (outras versões):** Clique em  ou em **Iniciar** e selecione **Todos os programas ou Programas.** Selecione **EpsonNet > EpsonNet Config.**
  - **Mac:** Abra a pasta **Aplicativos**, abra a pasta **Epson Software** e selecione **EpsonNet > EpsonNet Config > EpsonNet Config.**

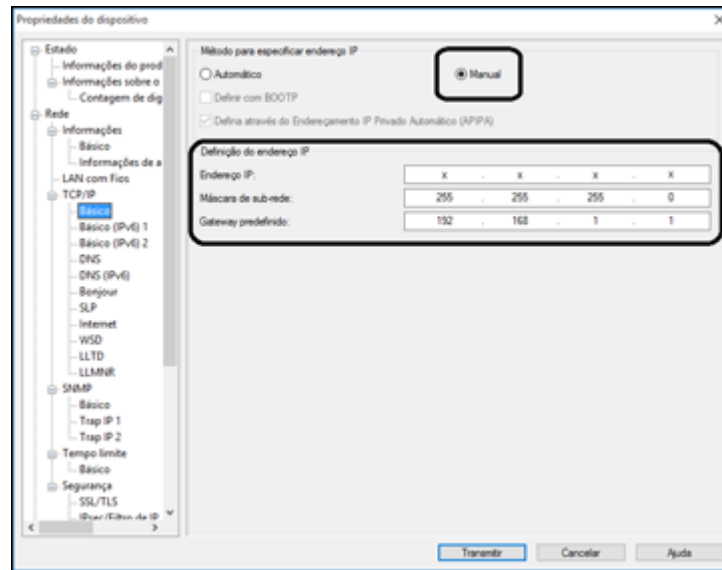
Depois de alguns momentos, o programa exibe os produtos conectados.

4. Clique duas vezes no produto que está configurando.

**Observação:** Se diversos produtos do mesmo modelo estiverem conectados, você pode identificá-los pelo endereço MAC.

5. Digite a senha atual de administrador, se necessário, e clique em **OK**.
6. Do menu à esquerda, sob **TCP/IP**, selecione **Básico**.

Você verá uma janela como esta:



7. Selecione **Manual**.
8. Digite as configurações de **Endereço IP**, **Máscara de Sub-rede** e **Gateway predefinido** do produto nos campos fornecidos.

**Observação:** Para conectar o produto a uma rede segura, digite um endereço de IP estático. Você também pode configurar o DNS selecionando **DNS** e digitar configurações de proxy selecionando **Internet** do menu **TCP/IP**.

9. Selecione **Transmitir**.

**Tema principal:** [Uso do software de configuração de rede EpsonNet Config](#)

---

## Uso do software de configuração Epson Device Admin

No Windows, você pode descobrir e monitorar dispositivos remotos, e fazer as configurações de rede em uma operação em lote. Consulte a ajuda do Epson Device Admin para instruções.

Para instalar o Epson Device Admin, baixe o software da página de suporte no endereço [epson.com.br/suporte](http://epson.com.br/suporte) e siga as instruções na tela.



---

## Criptografia de senhas

Siga as instruções nestas seções para criptografar informação confidencial armazenada no produto, como senhas e chaves particulares para os seus certificados.

[Configuração de uma senha de encriptação](#)


[Restauração da chave de encriptação de senha](#)

### Configuração de uma senha de encriptação

Você pode configurar a encriptação da senha para proteger informação confidencial armazenada no produto. Você também pode salvar uma cópia da chave de encriptação armazenada no chip Trusted Platform Module (TPM) do seu produto em um flash drive USB.

**Observação:** Certifique-se de tenha um flash drive USB com pelo menos 1MB de espaço livre para salvar uma cópia da chave de encriptação.

**Cuidado:** Se o chip TPM falhar, você não pode trocá-lo ou acessar qualquer informação confidencial armazenada no seu produto. As funções da impressora ainda estarão disponíveis, mas a função de encriptação de senha não pode ser usada. Entre em contato com a Epson para obter suporte técnico.

1. Aperte o botão  início, se necessário.
2. Selecione **Definições > Definições gerais > Administração do sistema > Definições de segurança**.

Você verá uma tela como esta:



3. Selecione **Criptografia da senha**.
4. Selecione **Lig.**.  
Uma mensagem sobre a reinicialização do produto aparece. Selecione **OK**.
5. Selecione **Continuar com o Backup**.  
Você vê a tela de backup da chave de encriptação.
6. Insira um flash drive USB na porta USB externa, localizada na frente do produto.
7. Selecione **Iniciar Backup**.  
O produto começa a fazer o backup da chave de encriptação no flash drive USB. Qualquer chave de encriptação armazenada anteriormente no flash drive será substituída.
8. Quando a mensagem de finalização aparecer, selecione **Fechar**.
9. Desligue o produto e volte a ligá-lo para aplicar a configuração de encriptação de senha.

**Observação:** O produto pode demorar mais do que o normal para ligar. Isso é normal.

**Tema principal:** [Criptografia de senhas](#)

**Referências relacionadas**

[Onde obter ajuda](#)

**Tarefas relacionadas**

[Restauração da chave de encriptação de senha](#)

## Restauração da chave de encriptação de senha

Se o chip TPM falhar, você pode restaurar a chave de encriptação a partir da cópia armazenada no seu flash drive USB.

1. Caso veja uma mensagem no painel de controle indicando que a TPM foi substituída quando ligar o produto, selecione **Restaurar a partir do backup**. Digite a senha de administrador, se necessário.
2. Insira o flash drive USB contendo a cópia da chave de encriptação na porta USB externa, localizada na frente do produto.
3. Selecione **Restaurar a partir do backup**.  
A chave de encriptação é restaurada no chip TPM.
4. Quando a mensagem de finalização aparecer, selecione **OK**.  
O produto reinicia.

**Tema principal:** [Criptografia de senhas](#)

---

## Gerenciamento de retenção de dados

Siga as instruções nestas seções para fazer as configurações de retenção de dados do produto ou para deletar qualquer dado armazenado no produto.

[Deletar todos os dados do produto](#)

[Modificação da configurações de deleção automática](#)

### Deletar todos os dados do produto

Se for dar o seu produto para alguém ou jogá-lo fora, recomendamos que delete todos os dados do produto.

1. Aperte o botão  início, se necessário.
2. Selecione **Definições** > **Definições gerais** > **Administração do sistema** > **Reset** (Reiniciar).


Você verá uma tela como esta:



3. Selecione **Erase All Data and Settings** (Apagar todos os dados e configurações).

4. Execute um dos seguintes procedimentos:
  - Selecione **Alta Velocidade** para fazer uma formatação rápida do disco rígido criptografado. A recuperação de dados ainda é possível se selecionar esta opção.
  - Selecione **Substituir** para fazer uma formação completa do disco rígido criptografado e rescrever todos os dados com zeros. Este processo leva aproximadamente 2 horas e meia e a recuperação de dados não é possível. Selecione esta opção para apagar completamente tudo que estiver armazenado, como dados sensíveis.
  - Selecione **Sobreposição Tripla** para apagar todos os dados usando um comando de eliminação dedicado. Este processo leva aproximadamente 2 horas e meia e a recuperação de dados não é possível. Selecione esta opção para executar um nível adicional de eliminação de dados.
5. Selecione **Sim**.

Quando todas as configurações tiverem sido restauradas, uma mensagem de reinicialização do produto aparece. Selecione **Fechar** e a tela **Administração do sistema** retorna.
6. Selecione **Limpar dados da memória interna > Excluir Todos os Trabalhos da Memória interna > Sim**.

Quando a memória estiver limpa, uma mensagem de finalização aparece.
7. Selecione a seta para trás.
8. Selecione **Definições de Pagor HDD > Apagar toda Memória**.
9. Execute um dos seguintes procedimentos:
  - Selecione **Alta Velocidade** para fazer uma formatação rápida do disco rígido criptografado. A recuperação de dados ainda é possível se selecionar esta opção.
  - Selecione **Substituir** para fazer uma formação completa do disco rígido criptografado e rescrever todos os dados com zeros. Este processo leva aproximadamente 2 horas e meia e a recuperação de dados não é possível. Selecione esta opção para apagar completamente tudo que estiver armazenado, como dados sensíveis.
  - Selecione **Sobreposição Tripla** para apagar todos os dados usando um comando de eliminação dedicado. Este processo leva aproximadamente 2 horas e meia e a recuperação de dados não é possível. Selecione esta opção para executar um nível adicional de eliminação de dados.
10. Selecione **Sim** para continuar.
11. Aperte o botão  início para retornar à tela inicial.
12. Desligue o produto e volte a ligá-lo para garantir que os dados tenham sido apagados.

**Tema principal:** [Gerenciamento de retenção de dados](#)

## Modificação da configurações de deleção automática

O seu produto pode deletar dados automaticamente depois de completar um trabalho de impressão ou cópia com a opção **Definição de Auto Apagar Memória**. Os seguintes dados são deletados depois de cada trabalho:


- Buffer de cópia
- Buffer de impressão
- Área de impressão autenticada pelo usuário

**Observação:** A ativação desta opção afeta o desempenho do seu produto.

1. Aperte o botão  início, se necessário.
2. Selecione **Definições > Definições gerais > Administração do sistema > Definições de Pagar HDD**.

Você verá uma tela como esta:



3. Selecione o campo **Definição de Auto Apagar Memória** para ativar a configuração.
4. Aperte o botão  início para retornar à tela inicial.

**Tema principal:** [Gerenciamento de retenção de dados](#)

---

## Solução de problemas

Consulte essas seções para resolver problemas que possa ter com o software de configuração de rede.

[Mensagens de erro de digitalização](#)

[Resolução de problemas do uso de software de rede](#)

[Resolução de problemas de segurança de rede](#)

[Resolução de problemas de certificado digital](#)

[Onde obter ajuda](#)

## Mensagens de erro de digitalização

Caso veja uma mensagem de erro quando digitalizar imagens e salvá-las em uma pasta compartilhada, procure por soluções nesta tabela.



| Mensagem  | Solução   |
|---|---|
| <p>Erro DNS. Verifique as definições de DNS.</p>  | <p>Tente o seguinte:</p> <ul style="list-style-type: none"> <li>• Certifique-se de que o endereço na lista de contatos na impressora e o endereço na pasta compartilhada seja o mesmo.</li> <li>• Se o endereço IP do computador for estático ou configurado manualmente, mude o nome do computador no caminho da rede do endereço IP. Por exemplo, mude de \\EPSON02\SCAN para \\192.168.xxx.xxx\SCAN.</li> <li>• Certifique-se de que o computador esteja ligado e não em modo de economia de energia, como em modo de repouso ou espera. Se o seu computador estiver em modo de repouso, você não pode salvar imagens digitalizadas na pasta compartilhada.</li> <li>• Desative temporariamente a firewall e software de segurança do seu computador. Se isso eliminar o erro, confira as configurações no software de segurança.</li> <li>• Você não pode salvar imagens digitalizadas em uma pasta compartilhada quando usar uma rede pública.</li> <li>• Se o endereço IP mudar quando reconectar usando DHCP em um laptop, obtenha o endereço IP novamente.</li> <li>• Verifique o DNS no seu produto e no servidor, computador ou roteador.</li> <li>• Certifique-se de que o nome e endereço IP do computador estejam corretos.</li> </ul> |
| <p>Erro de autenticação. Por favor, verifique as configurações de servidor de e-mail.</p> | <p>Se as restrições de usuário tiverem sido ativadas, certifique-se de que tenha digitado o nome e senha de usuário corretos. Além disso, certifique-se de que a senha não tenha vencido.</p>   |

| Mensagem   | Solução   |
|--|---|
| <p>Erro de comunicação. Verifique o Wi-Fi/ligação de rede.</p>   | <p>Tente o seguinte:</p> <ul style="list-style-type: none"> <li>• Certifique-se de que a Rede MS (MS Network) esteja ativada.</li> <li>• Certifique-se de que o endereço na lista de contatos na impressora e o endereço na pasta compartilhada seja o mesmo.</li> <li>• Direitos de acesso para o usuário na lista de contatos devem ser adicionados nas guias de Compartilhamento e Segurança nas propriedades da pasta compartilhada. Permissões de acesso também devem ser ativados para o usuário.</li> <li>• Imprima um relatório de conexão de rede para verificar se a impressora estiver conectada na rede.</li> </ul> |
| <p>O nome do ficheiro já está a ser utilizado. Mude o nome do ficheiro e digitalize novamente.</p>   | <p>Verifique se há um arquivo com o mesmo nome do arquivo que deseja salvar na pasta compartilhada. Apague o arquivo salvo ou selecione um nome diferente.</p>  |
| <p>Ficheiro(s) digitalizado(s) são muito grandes. Apenas XX página(s) foram enviados. Verifique se a pasta de destino tem espaço suficiente.</p> | <p>Tente o seguinte:</p> <ul style="list-style-type: none"> <li>• Aumente o espaço de armazenamento na pasta especificada.</li> <li>• Reduza o número de documentos.</li> <li>• Diminua a resolução de digitalização ou aumente a razão de compressão para reduzir o tamanho da imagem digitalizada.</li> </ul>   |

Tema principal: [Solução de problemas](#)

## Resolução de problemas do uso de software de rede

Consulte essas seções se tiver problemas usando o software de rede.

[Não é possível acessar o Web Config](#)



[A mensagem "Vencido" aparece](#)

A mensagem "O nome do certificado de segurança não é igual" aparece  
Nome do modelo ou endereço IP não exibidos no EpsonNet Config

**Tema principal:** [Solução de problemas](#)

## Não é possível acessar o Web Config

Se você não consegue acessar o Web Config no seu produto, tente essas soluções:

- Certifique-se de que o produto está ligado e conectado à sua rede usando o endereço IP correto. Verifique a conexão usando o painel de controle do seu produto ou imprima uma folha de estado da rede. Consulte o *Manual do usuário* do seu produto para mais instruções.
- Se selecionou **Alta** como configuração de **Força da encriptação** no Web Config, seu navegador deve suportar codificação AES (256 bits) ou 3DES (168 bits). Verifique o suporte de codificação do seu navegador ou selecione uma opção diferente em **Força da encriptação**.
- Se estiver usando um servidor proxy com seu produto, configure as configurações de proxy do navegador assim:
  - **Windows 10:** Clique em  > **Configurações** > **Rede e Internet** > **Proxy**. Navegue para baixo e configure **Usar servidor proxy** como **ativado**. Selecione **Não usar proxy para endereços locais (Intranet)**.
  - **Windows 8.x:** Navegue até a tela **Aplicativos** e selecione **Configurações do computador** > **Rede** > **Proxy**. Navegue para baixo e configure **Usar servidor proxy** como **ativado**. Selecione **Não usar proxy para endereços locais (Intranet)**.
  - **Windows (outras versões):** Clique em  ou em **Iniciar** e selecione **Painel de controle** > **Rede e Internet** > **Opções da Internet** > **Conexões** > **Configurações da LAN** > **Servidor Proxy** > **Não usar proxy para endereços locais**.
  - **Mac:** Selecione **Preferências do Sistema** > **Rede** > **Avançado** > **Proxies**. Registre o endereço local sob **Ignorar configurações de proxy para estes Servidores & Domínios**. Por exemplo, 192.168.1.\*: Endereço local 192.168.1.XXX, máscara de sub-rede 255.255.255.0.

**Tema principal:** [Resolução de problemas do uso de software de rede](#)

## A mensagem "Vencido" aparece

Se a mensagem "vencido" aparece quando você acessa o Web Config usando comunicação SSL (HTTPS), o certificado está vencido. A data e a hora do produto devem estar configuradas corretamente e obtenha um novo certificado.

**Tema principal:** [Resolução de problemas do uso de software de rede](#)

## A mensagem "O nome do certificado de segurança não é igual" aparece

Se uma mensagem começando com "O nome do certificado de segurança não é igual" aparece quando você acessa o Web Config usando comunicação SSL (HTTPS), o endereço IP do produto no CSR ou certificado autoassinado não é igual ao que digitou no seu navegador. Mude o endereço IP que digitou na configuração **Nome Comum** e obtenha e importe um certificado novamente ou mude o nome do produto.

**Tema principal:** [Resolução de problemas do uso de software de rede](#)

## Nome do modelo ou endereço IP não exibidos no EpsonNet Config

Se o nome do modelo do produto e/ou endereço IP não é exibido no EpsonNet Config, tente essas soluções:

- Se selecionou a opção bloquear, cancelar ou desligar na segurança do Windows ou tela do firewall, o endereço IP e nome do modelo não podem ser exibidos no EpsonNet Config. Registre EpsonNet Config como uma exceção no seu firewall ou software de segurança, ou feche o software de segurança e tente rodar o EpsonNet Config novamente.
- O tempo de operação pode ter se esgotado. Selecione **Ferramentas**, selecione **Opções**, selecione **Tempo Limite** e aumente a opção de tempo para a configuração de **Erro de Comunicação**. Porém isso pode fazer com que o EpsonNet Config rode mais devagar.

**Tema principal:** [Resolução de problemas do uso de software de rede](#)

## Resolução de problemas de segurança de rede

Consulte essas seções se tiver problemas usando os recursos de segurança de rede.

[Chave pré-compartilhada foi esquecida](#)

[Não é possível fazer a comunicação com o produto usando comunicação IPsec](#)

[Comunicação estava funcionando, mas parou](#)

[Não é possível criar a porta de impressão segura IPP](#)

[Não é possível fazer a conexão depois da configuração de filtragem IPsec/IP](#)

[Não é possível acessar o produto depois de configurar IEEE 802.1X](#)

**Tema principal:** [Solução de problemas](#)

## Chave pré-compartilhada foi esquecida

Se você esqueceu uma chave pré-compartilhada, mude a chave usando o Web Config para o padrão ou política de grupo.

**Tema principal:** [Resolução de problemas de segurança de rede](#)

## Não é possível fazer a comunicação com o produto usando comunicação IPsec

Seu computador precisa estar usando um desses algoritmos suportados com o produto:

| Método de segurança             | Algoritmos suportados   |
|---------------------------------|---|
| Algoritmo de criptografia 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 | DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30* |
| Algoritmo de criptografia 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    |   |

\* Disponível somente para IKEv2

**Tema principal:** [Resolução de problemas de segurança de rede](#)

## Comunicação estava funcionando, mas parou

Se comunicação de rede estava funcionando, mas parou de repente, o endereço IP do produto e/ou do computador pode ter mudado ou é inválido. Tente estas soluções:

- Desative IPsec usando o painel de controle do produto.
- Se DHCP estiver vencido ou o endereço IPv6 estiver vencido ou não foi obtido, você pode não conseguir achar o endereço IP registrado no Web Config.
- Se isso não resolver o problema, digite um endereço de IP estático usando Web Config.

**Tema principal:** [Resolução de problemas de segurança de rede](#)

## **Não é possível criar a porta de impressão segura IPP**

Se você não consegue criar a porta de impressão segura IPP, tente essas soluções:

- Você precisa especificar o certificado de servidor correto para comunicação SSL/TLS usando o Web Config.
- Se estiver usando um certificado CA, você deve importá-lo para o computador que está acessando o produto.

**Tema principal:** [Resolução de problemas de segurança de rede](#)

## **Não é possível fazer a conexão depois da configuração de filtragem IPsec/IP**

O valor configurado pode estar incorreto. Desative a filtragem IPsec/IP a partir do painel de controle do produto. Conecte-se a partir do computador e configure as definições de filtragem IPsec/IP Filtering novamente.

**Tema principal:** [Resolução de problemas de segurança de rede](#)

## **Não é possível acessar o produto depois de configurar IEEE 802.1X**

Se você não puder acessar o produto depois de o configurar para IEEE 802.1X, desative IEEE 802.1X e Wi-Fi usando o painel de controle do produto. Depois conecte o produto a um computador e configure IEEE 802.1X usando o Web Config novamente.

**Tema principal:** [Resolução de problemas de segurança de rede](#)

## **Resolução de problemas de certificado digital**

Consulte essas seções se tiver problemas usando um certificado digital.

[Mensagens de aviso de certificado digital](#)

[Não é possível importar um certificado digital](#)

[Não é possível atualizar um certificado nem criar um CSR](#)

[Certificado CA assinado excluído](#)

**Tema principal:** [Solução de problemas](#)

## **Mensagens de aviso de certificado digital**

Se você vir uma mensagem de aviso ao usar um certificado digital, confira as soluções nesta tabela.

| <b>Mensagem</b>   | <b>Solução</b>  |
|---|---|
| Digite um certificado de servidor.  | Selecione um arquivo de certificado e clique em <b>Importar</b> .   |
| Certificado CA 1 não está digitado.   | Importe certificado CA 1 antes de importar outros certificados.   |
| Valor inválido abaixo.  | Remova quaisquer caracteres não suportados no caminho do arquivo e senha.   |
| Data e hora inválidas.  | Defina a data e a hora no produto usando Web Config, EpsonNet Config, ou o painel de controle do produto.   |
| Senha inválida.   | Digite a senha que seja igual à senha do certificado CA.  |
| Arquivo inválido.   | Tente o seguinte: <ul style="list-style-type: none"> <li>• Importe apenas os arquivos de certificado no formato X509 enviado por uma autoridade de certificado confiável.</li> <li>• O tamanho do arquivo deve ser de 5KB ou menos e não esteja corrompido nem fabricado.</li> <li>• A corrente no certificado deve ser válida; consulte o website da autoridade do certificado.</li> </ul> |
| Não pode usar os certificados de servidor que incluam mais de três certificados CA.                             | Importe arquivos de certificado no formato PKCS#12 que contenham um ou mais certificados CA, ou converta cada certificado para o formato PRM e importe-os novamente.  |
| O certificado está vencido. Verifique se o certificado é válido ou verifique a data e a hora na sua impressora. | A data e a hora do produto devem estar corretas, e se o certificado estiver vencido, obtenha e importe um novo certificado.   |

| Mensagem                       | Solução  |
|--------------------------------|--|
| Chave particular é necessária. | <p>Faça o seguinte para emparelhar uma chave particular com o certificado:</p> <ul style="list-style-type: none"> <li>• Para certificados do formato PEM/DER obtidos de um CSR usando um computador, especifique o arquivo de chave particular.</li> <li>• Para certificados do formato PKCS#12 obtidos de um CSR usando um computador, crie um arquivo contendo a chave particular.</li> </ul> <p>Se você importou novamente um certificado de formato PEM/DER obtido de um CSR usando Web Config, você só pode importá-lo uma vez. Você deve obter e importar um novo certificado.</p> |
| Configuração falhou.           | O produto e o computador devem estar conectados e o arquivo de certificado não deve estar corrompido, depois importe o certificado novamente.  |

**Tema principal:** [Resolução de problemas de certificado digital](#)

## Não é possível importar um certificado digital

Se você não consegue importar um certificado digital, tente essas soluções:

- O certificado CA assinado e o CSR precisam ter as mesmas informações. Se não forem iguais, importe o certificado para um dispositivo que tenha a mesma informação ou use o CSR para obter um certificado CA assinado novamente.
- O tamanho do arquivo do certificado CA assinado tem que ser menor do que 5KB.
- Você deve digitar a senha correta.

**Tema principal:** [Resolução de problemas de certificado digital](#)

## Não é possível atualizar um certificado nem criar um CSR

Se você não consegue atualizar um certificado autoassinado nem criar um CSR para um certificado CA assinado, tente essas soluções:

- Você deve digitar uma configuração de **Nome Comum** no Web Config.



- A configuração de **Nome Comum** não pode conter caracteres não suportados nem ser separado por vírgula. Corrija a configuração e atualize o certificado novamente.

**Tema principal:** [Resolução de problemas de certificado digital](#)

## Certificado CA assinado excluído

Se você excluiu acidentalmente um certificado CA assinado, tente essas soluções:

- Se você reteve um arquivo de backup, importe o certificado CA assinado novamente.
- Se você obteve o certificado usando um CSR criado no Web Config, você não pode importar um certificado excluído. Crie um novo CSR e obtenha um novo certificado.

**Tema principal:** [Resolução de problemas de certificado digital](#)

## Onde obter ajuda

Se você precisar de ajuda adicional com o seu produto Epson, entre em contato com a Epson.

A Epson oferece estes serviços de suporte técnico:

### Suporte pela Internet

Visite o site de suporte da Epson no endereço [epson.com.br/suporte](http://epson.com.br/suporte) para obter soluções para problemas comuns. É possível fazer o download de utilitários e documentação, consultar as perguntas frequentes e soluções de problemas ou enviar um e-mail para a Epson com suas perguntas.

### Converse com um representante de suporte

Antes de ligar para o suporte da Epson, tenha em mãos as seguintes informações:

- Nome do produto
- Número de série do produto (localizado na etiqueta do produto)
- Comprovante de compra (nota da loja) e data da compra
- Configuração do computador
- Descrição do problema

E ligue para:

| País      | Telefone                            |
|-----------|-------------------------------------|
| Argentina | (54 11) 5167-0300<br>0800-288-37766 |

| <b>País</b>           | <b>Telefone</b>   |
|-----------------------|---|
| Bolívia*              | 800-100-116   |
| Brasil                | Para obter o número de suporte para o seu produto, visite o site de suporte da Epson em <a href="http://epson.com.br/suporte">epson.com.br/suporte</a> , selecione o seu produto e clique na guia <b>Entre em contato conosco</b> . |
| Chile                 | (56 2) 2484-3400  |
| Colômbia              | Bogotá: (57 1) 592-2200<br>Outras cidades: 018000-915235  |
| Costa Rica            | 800-377-6627  |
| Equador*              | 1-800-000-044   |
| El Salvador*          | 800-6570  |
| Guatemala*            | 1-800-835-0358  |
| México                | Cidade do México: (52 55) 1323-2052<br>Outras cidades: 01-800-087-1080  |
| Nicarágua*            | 00-1-800-226-0368   |
| Panamá*               | 00-800-052-1376   |
| Paraguai              | 009-800-521-0019  |
| Peru                  | Lima: (51 1) 418-0210<br>Outras cidades: 0800-10126   |
| República Dominicana* | 1-888-760-0068  |
| Uruguai               | 00040-5210067   |
| Venezuela             | (58 212) 240-1111   |

\*Entre em contato com a companhia telefônica local para ligar para este número gratuito de um celular. Se o seu país não aparecer na lista, entre em contato com o escritório de vendas no país mais próximo. Tarifas de longa distância ou outras taxas podem ser cobradas.

**Compra de suprimentos e acessórios**

Você também pode comprar tinta e papel genuínos da Epson através de um revendedor autorizado. Para encontrar o revendedor de produtos mais próximo, visite o site [epson.com.br](http://epson.com.br) ou entre em contato com o escritório Epson mais próximo.

**Tema principal:** [Solução de problemas](#)

---

## Avisos

Consulte estas seções para conferir avisos importantes.

[Marcas comerciais](#)

[Avisos sobre direitos autorais](#)

### Marcas comerciais

EPSON® é uma marca registrada, EPSON Exceed Your Vision é uma logomarca registrada e Epson Connect™ é uma marca comercial da Seiko Epson Corporation.

Windows é uma marca comercial da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Mac e OS X são marcas comerciais da Apple Inc., registradas nos EUA e em outros países.

Aviso geral: Outros nomes de produtos são usados neste manual somente para fins de identificação e podem ser marcas comerciais de seus respectivos proprietários. A Epson renuncia a todo e qualquer direito sobre essas marcas.



Tema principal: [Avisos](#)

### Avisos sobre direitos autorais

Todos os direitos reservados. Nenhuma parte desta publicação pode ser reproduzida, armazenada em sistemas de recuperação ou transmitida de alguma forma ou meio eletrônico, mecânico, fotocópia, gravação ou qualquer outro sem a autorização prévia por escrito da Seiko Epson Corporation. As informações aqui contidas devem ser usadas apenas com este produto Epson. A Epson não se responsabiliza pela aplicação das informações aqui contidas a outros produtos.

Nem a Seiko Epson Corporation nem suas subsidiárias serão responsáveis perante o comprador do produto ou terceiros por danos, perdas, encargos ou despesas incorridos pelo comprador ou terceiros, em consequência de: acidentes, uso indevido ou abuso deste produto; consertos ou modificações e alterações não autorizadas ou (exceto nos EUA) o não-cumprimento das instruções de uso e manutenção da Seiko Epson Corporation.

A Seiko Epson Corporation isenta-se da responsabilidade por danos ou problemas decorrentes da utilização de qualquer produto opcional ou suprimentos que não possuam a designação "produtos originais" ou "produtos Epson aprovados" por parte da Seiko Epson Corporation.

A Seiko Epson Corporation não se responsabiliza por quaisquer danos decorrentes de interferência eletromagnética, que ocorre a partir da utilização de quaisquer cabos de interface não reconhecidos como Epson produtos aprovados pela Seiko Epson Corporation.

Estas informações estão sujeitas a alteração sem aviso prévio.

[Atribuição de direitos autorais](#)

**Tema principal:** [Avisos](#)

## **Atribuição de direitos autorais**

© 2020 Epson America, Inc.

10/20

CPD-58934

**Tema principal:** [Avisos sobre direitos autorais](#)