EPSON
EXCEED YOUR VISION

Manual do administrador

Conteúdo

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 de importação e exportação: 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, precisa conectar o produto a uma rede. Consulte o *Manual do usuário* do produto para mais instruções.

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, precisa conectar 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. Determine 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*]/

A página de configurações básicas irá aparecer:

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

Mudança da senha de administrador no Web Config

Você pode definir uma senha de administrador usando o painel de controle do produto ou usando o 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, selecione **Definições do administrador** e selecione **Alterar informações de autenticação do administrador**.

Você verá uma janela como esta:

2. 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.
3. Clique em **OK**.

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

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 ajustes SSL/TLS
Configuração de filtragem IPsec/IP
Configuração de protocolo SNMPv3
Conexão do produto a uma rede IEEE 802.1X
Uso de um certificado digital
Configuração de protocolos e serviços em Web Config
Uso de um servidor de e-mail
Importação e exportação de configurações de Web Config

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

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 **Definições de segurança de rede**.
2. Selecione **SSL/TLS** e selecione **Básico**.
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: Uso do seu produto em uma rede segura

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.

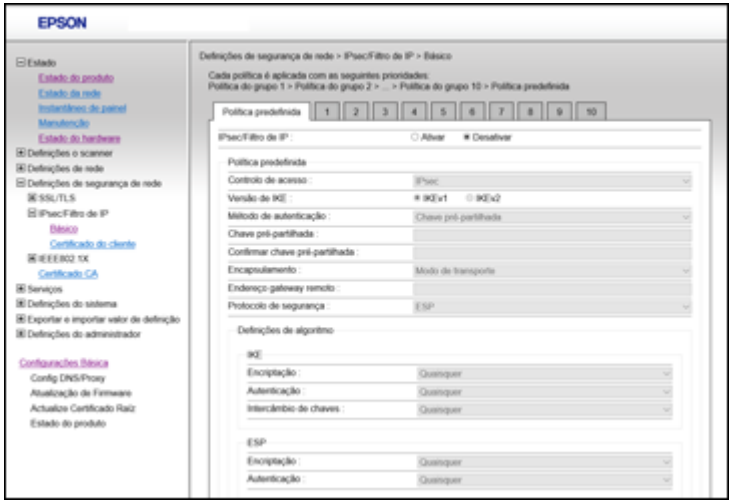
Tema principal: Configuração de filtragem IPsec/IP

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 **Definições de segurança de rede**.
2. Selecione **IPsec/Filtro de IP** e 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**.

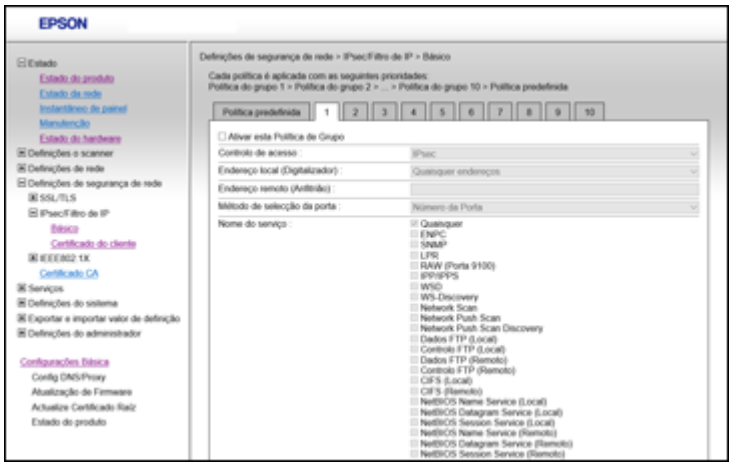
Tema principal: Configuração de filtragem IPsec/IP

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 **Definições de segurança de rede**.
2. Selecione **IPsec/Filtro de IP** e 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
Controlo de Acesso	Selecione **Permitir Acesso** para permitir que pacotes IP passem Selecione **Recusar Acesso** para evitar que pacotes IP passem Selecione **IPsec** para permitir que pacotes IPsec passem
Versão de IKE	Selecione uma versão do protocolo de Internet Key Exchange (IKE) que corresponda ao seu ambiente de rede.
Método de autenticação	Selecione um método de autenticação, ou selecione **Certificado** se você importou um certificado CA assinado
Chave pré-partilhada	Se necessário, digite uma chave pré-compartilhada entre 1 e 127 caracteres
Confirmar chave pré-partilhada	Confirme a chave pré-compartilhada que você digitou.
Encapsulamento	Se selecionou **IPsec** como opção de **Controlo de Acesso**, selecione um desses modos de encapsulamento: **Modo de transporte**: se estiver usando o produto na mesma rede LAN; pacotes de camada 4 ou posterior são codificados **Modo Túnel**: 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
Endereço gateway remoto(Modo Túnel)	Se selecionou **Modo Túnel** como opção de **Encapsulamento**, digite um endereço gateway entre 1 e 39 caracteres

Configuração	Opções/Descrição
Protocolo de segurança	Se selecionou **IPsec** como opção de **Controlo de Acesso**, selecione um desses protocolos de segurança: **ESP**: para garantir a integridade de autenticação e dados, e codificar dados **AH**: para garantir a integridade de autenticação e dados, se codificação de dados for proibida, você pode usar IPsec
Definições de algoritmo	Selecione as configurações do algoritmo de criptografia para o protocolo de segurança que você selecionou.

Configurações de política de grupo

Configuração	Opções/Descrição
Controlo de Acesso	Selecione **Permitir Acesso** para permitir que pacotes IP passem Selecione **Recusar Acesso** para evitar que pacotes IP passem Selecione **IPsec** para permitir que pacotes IPsec passem
Endereço local(Digitalizador)	Selecione um endereço IPv4 ou IPv6 que seja igual ao seu ambiente de rede; se o endereço IP é definido automaticamente, selecione **Usar endereço IPv4 obtido automaticamente**
Endereço remoto(Host)	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
Método de seleção da porta	Selecione o método que deseja usar para especificar portas

Configuração	Opções/Descrição
Nome do serviço	Se selecionou **Nome de Serviço** como opção de **Método de Escolha de Porta**, selecione uma opção de nome de serviço aqui, consulte a tabela a seguir para mais informações
Protocolo de Transporte	Se selecionou **Número da Porta** como opção de **Método de seleção da porta**, selecione um desses modos de encapsulamento: **Qualquer protocolo** **TCP** **UDP** **ICMPv4** Consulte a próxima tabela para mais informações
Porta Local	Se selecionou **Número da Porta** como opção de **Método de seleção da porta** e **TCP** ou **UDP** para opção de **Protocolo de transporte**, digite os números de porta que controlam o recebimento de pacotes (até 10 portas), separados por vírgulas, por exemplo **25,80,143,5220**; deixe esta configuração em branco para controlar todas as portas; consulte a próxima tabela para mais informações
Porta remota	Se selecionou **Número da Porta** como opção de **Método de seleção da porta** e **TCP** ou **UDP** para opção de **Protocolo de transporte**, digite os números de porta que controlam o envio de pacotes (até 10 portas), separados por vírgulas, por exemplo **25,80,143,5220**; deixe esta configuração em branco para controlar todas as portas; consulte a próxima tabela para mais informações
Versão de IKE	Selecione **IKEv1** ou **IKEv2** dependendo do dispositivo ao qual o produto esteja conectado.

Configuração	Opções/Descrição
Método de autenticação	Se selecionou **IPsec** como opção de **Controle de Acesso**, selecione um método de autenticação aqui
Chave pré-partilhada	Se selecionou **Chave pré-partilhada** como opção de **Método de autenticação**, digite uma chave pré-compartilhada entre 1 e 127 caracteres aqui e no campo **Confirmar chave pré-partilhada**
Encapsulamento	Se selecionou **IPsec** como opção de **Controlo de Acesso**, selecione um desses modos de encapsulamento: **Modo de transporte**: se estiver usando o produto na mesma rede LAN; pacotes de camada 4 ou posterior são codificados **Modo Túnel**: 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
Endereço gateway remoto(Modo Túnel)	Se selecionou **Modo Túnel** como opção de **Encapsulamento**, digite um endereço gateway entre 1 e 39 caracteres
Protocolo de segurança	Se selecionou **IPsec** como opção de **Controlo de Acesso**, selecione um desses protocolos de segurança: **ESP**: para garantir a integridade de autenticação e dados, e codificar dados **AH**: para garantir a integridade de autenticação e dados, se codificação de dados for proibida, você pode usar IPsec
Definições de algoritmo	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	Operations controlled
ENPC	UDP	3289/Qualquer porta	Buscando um produto a partir de aplicações tais como drivers de scanner ou EpsonNet Config
SNMP	UDP	161/Qualquer porta	Adquirindo e configurando MIB de aplicações tais como drivers de scanner ou EpsonNet Config
WSD	TCP	Qualquer porta/5357	Controle de WSD
WS-Discovery	UDP	3702/Qualquer porta	Buscando um produto de WSD
Network Scan	TCP	1865/Qualquer porta	Encaminhamento de dados de scan do Document Capture Pro
Network Push Scan	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
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 atualização de firmware e atualização de certificado de raiz em um cliente HTTP ou HTTPS
HTTPS (Remoto)	TCP	Qualquer porta/443	

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

Aceitar digitalização usando Epson Scan 2 e configurações do scanner

Use este exemplo para permitir comunicação de dados de digitalização e configurações de scanner de serviços especificados.

Política padrão:

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

Política de grupo:

- **Ativar esta Política de Grupo**: Selecione esta caixa
- **Controlo de Acesso**: **Permitir acesso**
- **Endereço Remoto(Host)**: Endereço IP de cliente
- **Método de seleção da porta**: **Nome do serviço**
- **Nome do serviço**: Selecione **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** e **HTTPS (Local)**

Recepção de acesso apenas de um endereço IP especificado

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:

- **Ativar esta Política de Grupo**: Selecione esta caixa
- **Controlo de Acesso**: **Permitir acesso**
- **Endereço remoto(Host)**: Endereço IP de cliente do administrador

Tema principal: Configuração de filtragem IPsec/IP

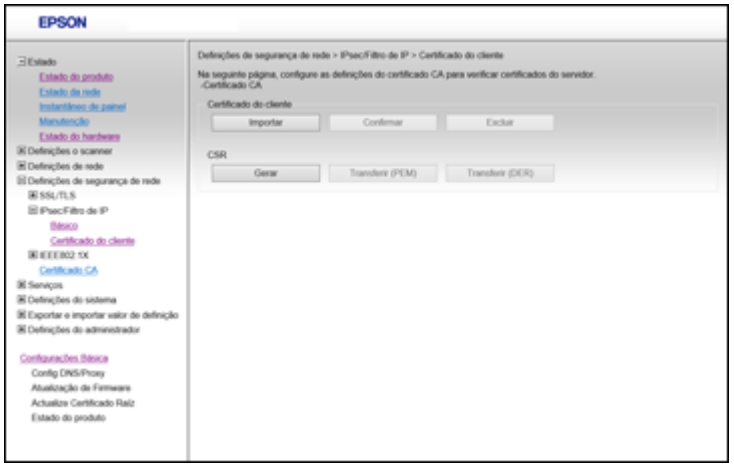
Configuração de um certificado de filtragem IPsec/IP

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

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

2. Selecione **IPsec/Filtro de IP** e selecione **Certificado de Cliente**.

   Você verá uma janela como esta:



3. Execute um dos seguintes procedimentos:
   - Clique em **Importar** para adicionar um novo certificado de cliente.
   - Selecione o certificado que deseja usar como a opção de **Copiar de** e clique em **Copiar**.
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 **Serviços**.
2. Selecione **Protocolo**.

Você verá uma janela como esta:

3. Marque a caixa de diálogo **Ativar SNMPv3** para habilitar configurações SNMPv3.
4. Selecione as configurações que deseja na seção Configurações SNMPv3.
5. Clique em **Avançar**.

   Você verá uma mensagem de confirmação.
6. 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
Nome de Util.	Digite um nome de usuário de 1 a 32 caracteres em ASCII
Definições de autenticação	
Algoritmo	Selecione o algoritmo para autenticação
Palavra-passe	Digite uma senha de 8 a 32 caracteres em ASCII
Confirmar palavra-passe	Digite a senha de autenticação novamente

Configuração	Opções/Descrição
Definições de encriptação	
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

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

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 **Definições de segurança de rede**.
2. Selecione **IEEE802.1X** e selecione **Básico**.

Você verá uma janela como esta:

3. Selecione **Ativar** como configuração de **IEEE802.1X (Rede com Fio)**.
4. Selecione as opções de configurações IEEE 802.1X que deseja usar.
5. Clique em **Avançar**.

   Você verá uma mensagem de confirmação.
6. Clique em **OK**.

Tema principal: Conexão do produto a uma rede IEEE 802.1X

Configurações da rede IEEE 802.1X

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

Configuração	Opções/Descrição
Tipo EAP	Selecione um desses métodos de autenticação para conexões entre o produto e um servidor RADIUS: **EAP-TLS** ou **PEAP-TLS**: Você deve obter e importar um certificado CA assinado **PEAP/MSCHAPv2**: Você deve configurar uma senha
ID do utilizador	Digite uma identificação entre 1 e 128 ASCII caracteres para autenticação em um servidor RADIUS

Configuração	Opções/Descrição
Senha	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.
Confirmar palavra-passe	Digite a senha de autenticação novamente
ID do servidor	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
Validação de certificado	Selecione um certificado válido independentemente do método de autenticação; importe o certificado usando a opção de **Certificados de CA**.
Nome Anônimo	Se selecionou **PEAP-TLS** ou **PEAP/MSCHAPv2** como a configuração de **Método de Autenticação**, 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: **Alta** para AES256/3DES **Média** para AES256/3DES/AES128/RC4

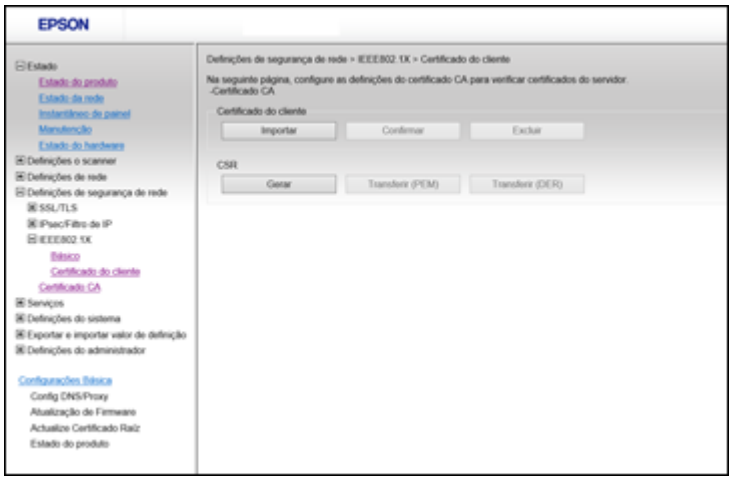
Tema principal: Conexão do produto a uma rede IEEE 802.1X

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 **Definições de segurança de rede**.
2. Selecione **IEEE802.1X** e selecione **Certificado de Cliente**.

Você verá uma janela como esta:



3. Execute um dos seguintes procedimentos:
   - Clique em **Importar** para adicionar um novo certificado de cliente.
   - Selecione o certificado que deseja usar como a opção de **Copiar de** e clique em **Copiar**.
4. Clique em **OK**.

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 autoassinado
Importação de um certificado CA
Exclusão de um certificado CA

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 CA
Um certificado CA indica que a identidade de um servidor foi verificada por terceiros. Você precisa obter um certificado CA para autenticação de servidor de um CA que os emita.

Certificado auto-assinado
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.

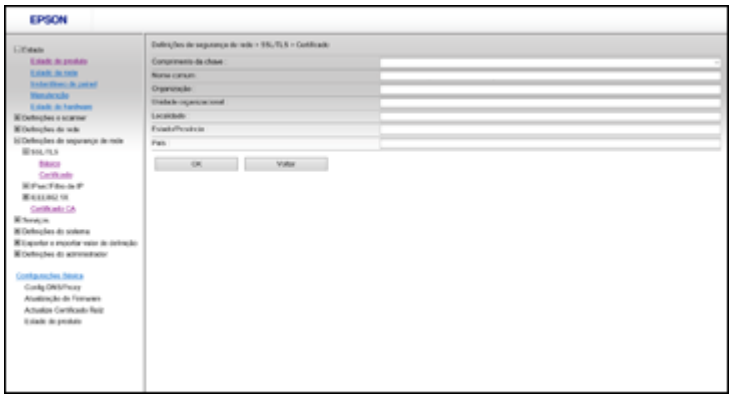
Tema principal: Uso de um certificado digital

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 **Definições de segurança de rede**.
2. Selecione uma das seguintes opções de segurança de rede e certificados correspondentes:
   - **SSL/TLS** e selecione **Certificado**
   - **IPsec/Filtro IP** e selecione **Certificado de Cliente**
   - **IEEE802.1X** e selecione **Certificado de Cliente**
3. Na seção CSR, selecione **Gerar**.

Você verá uma janela como esta:



4. Selecione as opções de configuração de CSR que deseja usar.
5. Clique em **OK**.

   Você verá uma mensagem de conclusão.
6. Selecione **Definições de segurança de rede** e selecione uma das seguintes opções de segurança de rede e certificados correspondentes:
   - **SSL/TLS** e selecione **Certificado**
   - **Filtragem IPsec/IP** e selecione **Certificado de Cliente**.
   - **IEEE802.1X** e selecione **Certificado de Cliente**.
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 **Definições de segurança de rede** e selecione uma das seguintes opções de segurança de rede e certificados correspondentes:
    - **SSL/TLS** e selecione **Certificado**
    - **Filtragem IPsec/IP** e selecione **Certificado de Cliente**.
    - **IEEE802.1X** e selecione **Certificado de Cliente**.
11. Na seção Certificado CA, 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

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
Comprimento de chave	Selecione um tamanho da chave para o CSR
Nome Comum	Digite um nome ou endereço de IP estático de 1 a 128 caracteres; por exemplo, **Impressora da recepção** ou **https://10.152.12.225**
Organização, **Unidade organizacional**, **Localidade**, **Estado/Província**	Digite informações em cada campo conforme necessário, de 0 a 64 caracteres em ASCII; separe múltiplos nomes com vírgulas
País	Digite um código de país de dois dígitos conforme especificado pelo padrão ISO-316

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	**Chave privada**: Não configure porque o produto contem uma chave particular **Senha**: Não configure **Certificado CA 1/Certificado CA 2**: Opcional
Formato PEM/DER obtido de um computador	**Chave privada**: Configure uma chave particular **Senha**: Não configure **Certificado CA 1/Certificado CA 2**: Opcional
Formato PKCS#12 obtido de um computador	**Chave Particular**: Não configure **Senha**: Opcional **Certificado CA 1/Certificado CA 2**: Não configure

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 **Definições de segurança de rede**.
2. Selecione uma das opções de segurança de rede a seguir e certificado correspondente:
   - **SSL/TLS** e selecione **Certificado**
   - **Filtragem IPsec/IP** e selecione **Certificado de Cliente**.
   - **IEEE802.1X** e selecione **Certificado de Cliente**.
3. Clique em **Excluir**.

   Você verá uma mensagem de conclusão.
4. Clique em **OK**.

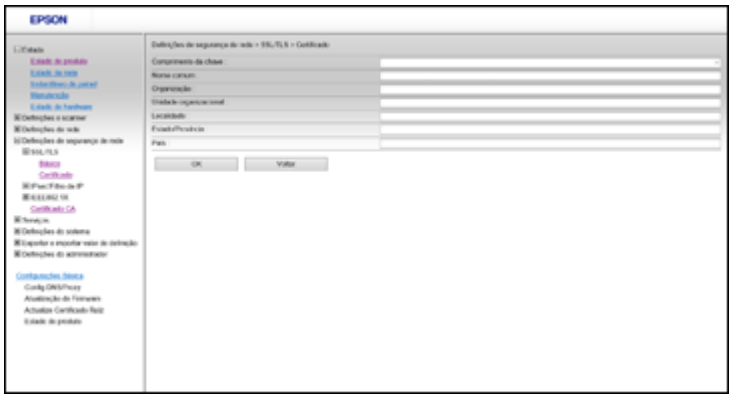
Tema principal: Uso de um certificado digital

Atualização de um certificado autoassinado

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 **Definições de segurança de rede**, selecione **SSL/TLS** e selecione **Certificado**.
2. Clique em **Actualizar**.

Você verá uma janela como esta:



3. Digite um identificador para o seu produto de 1 a 128 caracteres no campo **Nome Comum**.
4. Selecione um período de validade para o certificado como configuração de **Validade do Certificado (ano)**.
5. Clique em **Avançar**.

   Você verá uma mensagem de conclusão.
6. Clique em **OK**.
7. Clique em **Confirmar** para verificar a informação do certificado.

Tema principal: Uso de um certificado digital

Importação de um certificado CA

Você pode importar um certificado CA usando Web Config.

1. Acesse o Web Config e selecione **Definições de segurança de rede**.
2. Selecione **Certificado CA**.
3. Selecione **Importar**.

4. Selecione o certificado CA que deseja importar.

5. Clique em **OK**.

Quando vir a página da **Certificado CA** e o certificado importado for exibido, a importação terminou.

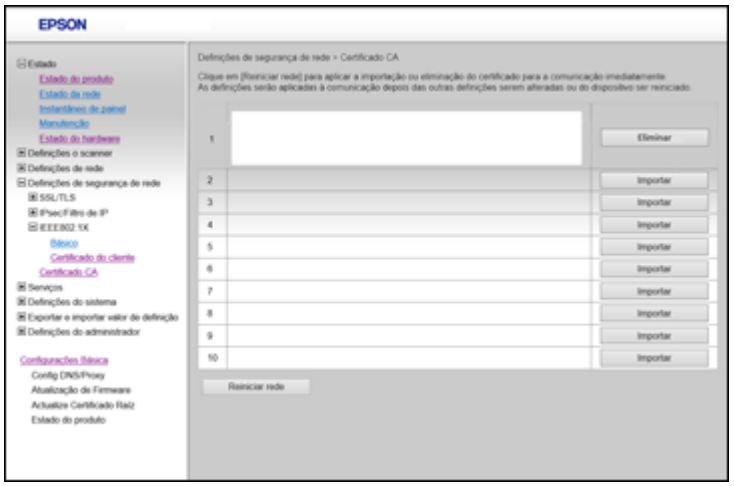
Tema principal: Uso de um certificado digital

Exclusão de um certificado CA

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

1. Acesse o Web Config e selecione **Definições de segurança de rede**.

2. Selecione **Certificado CA**.



3. Encontre o certificado que deseja remover e clique no botão **Eliminar** ao lado dele.
4. Clique em **OK** para confirmar a deleção.

Tema principal: Uso de um certificado digital

Configuração de protocolos e serviços em Web Config

Você pode ativar ou desativar protocolos usando o Web Config.

1. Acesse o Web Config, selecione **Serviços** e selecione **Protocolo**.
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**.
6. Selecione e configure serviços e protocolos conforme necessário.

Depois dos protocolos reiniciarem, as modificações são aplicadas.

Configurações de protocolo

Tema principal: Uso do seu produto em uma rede segura

Configurações de protocolo

Você pode configurar esses ajustes de protocolo no Web Config.

Protocolos

Nome	Descrição
Bonjour	Use o Bonjour para procurar por dispositivos e AirPrint
SLP	Use o SLP para push-scanning e busca em rede no EpsonNet Config.
WSD	Adicione dispositivos WSD ou imprima e digitalize da porta WSD.
LLTD	Exibe o produto no mapa da rede do Windows.
LLMNR	Use resolução de nome sem NetBIOS, mesmo que não possa usar DNS.
SNMPv1/v2c	Configure e monitore o seu produto remotamente.
SNMPv3	Configure e monitore o seu produto remotamente usando o protocolo SNMPv3.

Configurações Bonjour

Configuração	Opções/Descrição
Usar Bonjour	Procure e use dispositivos através do Bonjour (você não pode usar AirPrint se estiver desativado)
Nome de 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.

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 digitalização (seg)	Digite um valor para interrupção da comunicação para digitalização WSD entre 3 e 3.600 segundos.
Nome de disposit.	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 de disposit.	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 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 **Apenas leitura ou Escrita/leitura**
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
Activar SNMPv3	Ative SNMPv3 para produtos que suportem SNMPv3.
Nome de Util.	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 de contexto	Digite entre 1 e 32 caracteres

Tema principal: Configuração de protocolos e serviços 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 **Definições de rede**.
2. Selecione **Servidor de E-mail** e 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

Configuração do servidor de e-mail

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

Configuração	Opções/Descrição
Método de autenticação	Selecione o método de autenticação que seja igual o seu servidor de e-mail
Conta autenticada	Digite o nome da conta autenticada de 1 a 255 caracteres em ASCII
Palavra-passe autenticada	Digite a senha autenticada de 1 a 20 caracteres em ASCII usando A-Z, a-z, 0-9 e esses caracteres: ! # $ % ' * + - . / = ? ^ _ { ! } ~ @
Endereço de e-mail do remetente	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: ( ) < > [ ] ;

Configuração	Opções/Descrição
Endereço do servidor SMTP	Digite o endereço do servidor SMTP de 1 a 255 caracteres usando A-Z, a-z, 0-9 e "-" no formato IPv4 ou FQDN
Número da porta do servidor SMTP	Digite o número de porta do servidor SMTP entre 1 e 65535
Ligação segura	Selecione o método de segurança para o servidor de email; opções disponíveis dependem da configuração de **Método de autenticação**.
Validação de certificado	Ative a verificação de certificados válidos; a opção recomendada é **Ativar**
Endereço do servidor POP3	Digite o endereço do servidor POP de 1 a 255 caracteres usando A-Z, a-z, 0-9 e "-" no formato IPv4 ou FQDN
Número da porta do servidor POP3	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 **Definições de rede**.
2. Selecione **Servidor de E-mail** e selecione **Testar Conexão**.
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
O teste de ligação foi concluído com sucesso	A conexão com o servidor foi bem-sucedida

Mensagem	Descrição
Erro de comunicação com o servidor SMTP Verifique o seguinte - Configurações de Rede	Uma das seguintes condições ocorreu: • O produto não está conectado a uma rede • O servidor SMTP está fora do ar • A conexão com a rede foi interrompida durante a comunicação • Dados incompletos foram recebidos
Erro de comunicação com o servidor POP3 Verifique o seguinte - Configurações de Rede	Uma das seguintes condições ocorreu: • O produto não está conectado a uma rede • O servidor POP3 está fora do ar • A conexão com a rede foi interrompida durante a comunicação • Dados incompletos foram recebidos
Ocorreu um erro ao se conectar ao servidor SMTP. Verifique o seguinte - Endereço do servidor SMTP - Servidor DNS	Uma das seguintes condições ocorreu: • A resolução DNS falhou • A resolução de nome para um servidor SMTP falhou
Ocorreu um erro ao se conectar ao servidor POP3. Verifique o seguinte - Endereço do servidor POP3 - Servidor DNS	Uma das seguintes condições ocorreu: • A resolução DNS falhou • A resolução de nome para um servidor SMTP falhou
Erro de autenticação com o servidor SMTP. Verifique o seguinte - Método de autenticação - Conta autenticada - Senha autenticada	A autenticação do servidor SMTP falhou.
Erro de autenticação com o servidor POP3. Verifique o seguinte - Método de autenticação - Conta autenticada - Senha autenticada	A autenticação do servidor POP3 falhou.

Mensagem	Descrição
Método de comunicação não suportado. Verifique o seguinte - Endereço do servidor SMTP - Conexão segura de número de porta do servidor SMTP (SSL) não é suportada.	O protocolo de comunicação não é suportado
Conexão ao servidor SMTP falhou. Mude conexão segura para Nenhum.	Existe uma desigualdade de SMTP entre um servidor e um cliente, ou quando o servidor não suporta uma conexão segura SMTP
Conexão ao servidor SMTP falhou. Mude conexão segura para SSL/TLS.	Existe uma desigualdade de SMTP entre um servidor e um cliente, ou o servidor solicita uma conexão SSL/TLS para SMTP
Conexão ao servidor SMTP falhou. Mude conexão segura para STARTTLS.	Existe uma desigualdade de SMTP entre um servidor e um cliente, ou quando o servidor solicita uma conexão STARTTLS para SMTP
A conexão não é de confiança. Verifique o seguinte - Data e hora	A configuração de data e hora do produto está incorreta ou o certificado venceu
A conexão não é de confiança. Verifique o seguinte - Certificado de CA	O produto possui uma desigualdade de certificado de raiz ou um certificado CA não foi importado
A conexão não é segura.	O certificado está danificado
A autenticação do servidor SMTP falhou. Mude o método de autenticação para SMTP-AUTH.	Desigualdade de método de autenticação entre um servidor e um cliente. O servidor não suporta SMTP AUTH.
A autenticação do servidor SMTP falhou. Mude o método de autenticação para POP antes de SMTP.	Desigualdade de método de autenticação entre um servidor e um cliente. O servidor não suporta SMTP AUTH.
Endereço de e-mail do remetente está incorreto. Mude para o endereço de e-mail do seu serviço de e-mail.	O endereço de e-mail do remetente especificado está errado
Não pode acessar o produto até o processamento estar concluído	O produto está ocupado

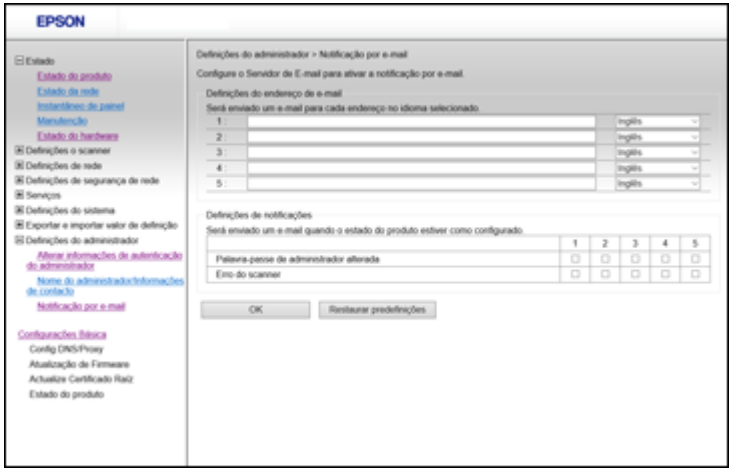
Tema principal: Uso de um servidor de e-mail

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. 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 **Definições do administrador**.
2. Selecione **Notificação por E-mail**.

   Você verá uma janela como esta:



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

Tema principal: Uso de um servidor de e-mail

Importação e exportação de configurações de Web Config

Siga as instruções nestas seções para importar e exportar as configurações do produto usando o software Web Config.

Exportação de configurações usando o Web Config
Importação de configurações usando o Web Config

Tema principal: Uso do seu produto em uma rede segura

Exportação de configurações usando o Web Config

Você pode exportar as configurações do produto e, como opção, criptografar as configurações no arquivo usando uma senha.

1. Acesse Web Config e selecione **Exportar e importar valor de definição**.
2. Selecione **Exportar**.
3. Selecione as configurações que deseja exportar.

   Observação: Se selecionar uma categoria superior, as sub-categorias também são selecionadas. Como padrão, os itens que são únicos à rede, como o endereço IP, não podem ser selecionados. Se desejar exportar estes itens, selecione **Ative para selecionar as definições individuais do dispositivo**. Recomenda-se que você exporte apenas itens únicos quando substituir um produto na rede ou pode encontrar conflitos na rede.

4. Digite uma senha de criptografia, se desejado.
5. Clique em **Exportar** e salve o arquivo.

Tema principal: Importação e exportação de configurações de Web Config

Importação de configurações usando o Web Config

Você pode importar configurações para o seu produto que tenham sido exportadas anteriormente Se usou criptografia quando as configurações foram exportadas, obtenha a senha necessário antes de importar.

1. Acesse Web Config e selecione **Exportar e importar valor de definição**.
2. Selecione **Importar**.
3. Clique em **Procurar** e selecione o arquivo de configurações exportadas.
4. Se necessário, digite a senha de descriptografia.
5. Clique em **Avançar**.
6. Selecione as configurações para importar e clique em **Avançar**.

7. Clique em **OK**.

As configurações selecionadas são importadas para o produto.

Tema principal: Importação e exportação de configurações de Web Config

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 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 e selecione **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 parta **Epson Software** e selecione **EpsonNet** > **EpsonNet Config** > **EpsonNet Config**.

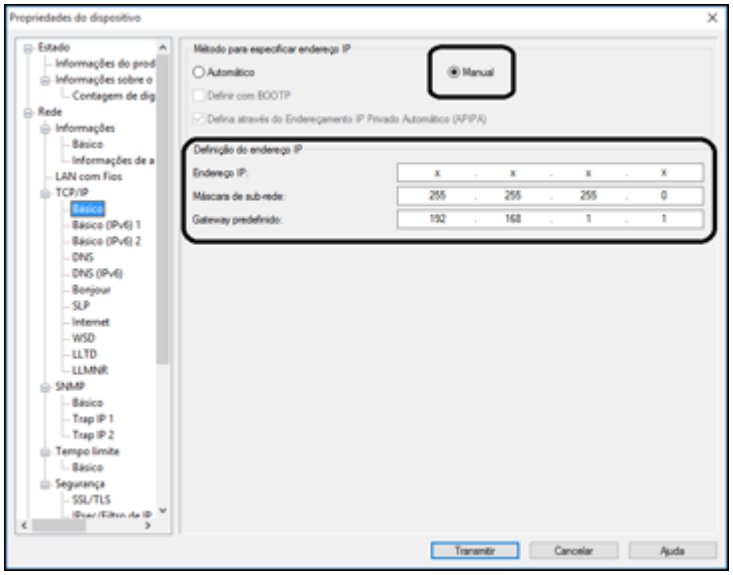
   Depois de alguns momentos, o programa exibe os produtos conectados.

4. Clique duas vezes no produto que está configurando.

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

5. Do menu à esquerda, selecione **TCP/IP**, e selecione **Básico**.

   Você verá uma janela como esta:



6. Selecione **Manual**.
7. 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**.

8. 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 e siga as instruções na tela.

Solução de problemas

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

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

Resolução de problemas do uso de software de rede

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

Não pode acessar 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 pode acessar 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. Consulte o *Manual do usuário* do seu produto para 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 um 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 e selecione **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 pode comunicar com o produto usando comunicação IPsec
Comunicação estava funcionando, mas parou
Não é possível fazer a conexão depois da configuração de filtragem IPsec/IP
Não pode 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 pode comunicar 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 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 pode 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 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 pode importar um certificado digital

Não pode 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.

Mensagem	Solução
Digite um certificado de servidor.	Selecione um arquivo de certificado e clique em **Importar**.
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: • Importe apenas os arquivos de certificado no formato X509 enviado por uma autoridade de certificado confiável. • O tamanho do arquivo deve ser de 5KB ou menos e não esteja corrompido nem fabricado. • A corrente no certificado deve ser válida; consulte o website da autoridade do certificado.
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.	Faça o seguinte para emparelhar uma chave particular com o certificado: • Para certificados do formato PEM/DER obtidos de um CSR usando um computador, especifique o arquivo de chave particular. • Para certificados do formato PKCS#12 obtidos de um CSR usando um computador, crie um arquivo contendo a chave particular. 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.
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 pode 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 pode 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 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 0800-288-37766

País	Telefone
Bolívia*	800-100-116
Brasil	Capitais e áreas metropolitanas: 3004-6627 Outras áreas: 0800-377-6627 / 0800-EPSONBR
Chile	(56 2) 2484-3400
Colômbia	Bogotá: (57 1) 523-5000 Outras cidades: 018000-915235
Costa Rica	800-377-6627
Equador*	1-800-000-044
El Salvador*	800-6570
Guatemala*	1-800-835-0358
Honduras**	800-0122 Código: 8320
México	Cidade do México: (52 55) 1323-2052 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 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.

** Disque os primeiros 7 dígitos, aguarde uma mensagem e, em seguida, digite o código.

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 ou entre em contato com o escritório Epson mais próximo.

Tema principal: Solução de problemas

Avisos

Consulte estas seções para conferir avisos importantes.

Marcas registradas

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

Mac é uma marca comercial 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

8/17

CPD-54165

Tema principal: Avisos sobre direitos autorais