EPSON®

EXCEED YOUR VISION

Administrator's Guide

Contents

Administrator's Guide

Welcome to the *Administrator's Guide*.

For a printable PDF copy of this guide, click here.

Note: Not all features mentioned in this *Administrator's Guide* are available with every product model.

You can use two software utilities to configure your product's advanced network settings: Web Config and EpsonNet Config. This guide covers Web Config in detail; for information on using EpsonNet Config, see the EpsonNet Config help utility.

The available network functions vary by product. (Unavailable functions are not displayed on the product's control panel or software settings screen.) Epson products support the following system administration functions:

- SSL/TLS communication: use Secure Sockets Layer/Transport Layer Security to encrypt traffic and avoid spoofing between the product and a computer
- IPsec/IP filtering: control access and secure communications between the product and a network gateway
- Individual protocol control: enable and disable single services
- Import and export settings: migrate settings from product to product

Using Web Config Network Configuration Software

Follow the instructions in these sections to configure your product's administrator network settings using the Web Config software.

Note: Before you can configure system administration settings, connect the product to a network. See the product's *User's Guide* for instructions.

About Web Config
Accessing Web Config
Changing the Administrator Password in Web Config
Using Your Product on a Secure Network

About Web Config

Web Config is a browser-based application you can use to configure a product's settings. Basic and advanced setting pages are available.

Note: Before you can configure system administration settings, connect the product to a network. See the product's *User's Guide* for instructions.

You can lock the settings you select by setting up an administrator password for your product. See the product's *User's Guide* for instructions.

Parent topic: Using Web Config Network Configuration Software

Accessing Web Config

You can access Web Config from your browser using HTTP or HTTPS.

By default, you access Web Config for the first time using HTTP. If you continue to use HTTP, Web Config will not display all available menus.

1. Determine the product IP address. See the product's *User's Guide* for instructions.

2. Start your web browser and make sure JavaScript is enabled.

3. Type the product IP address into the browser as follows, depending on the protocol you are using:

   • IPv4: http://*product IP address*

   • IPv6: http://[*product IP address*]/

The Basic Settings page appears:
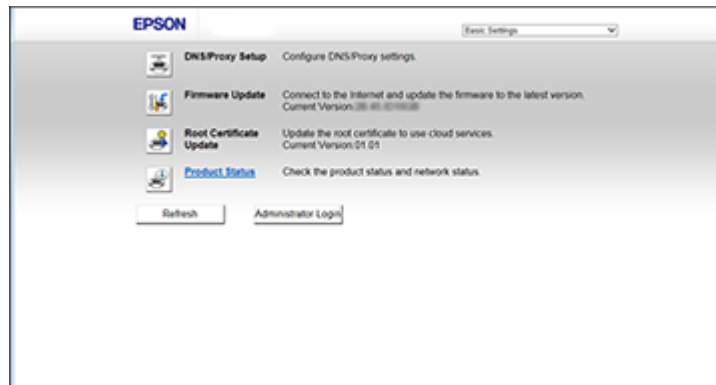
4. To use HTTPS, configure your browser to use HTTPS for the address.

    A message warning about the self-signed certificate appears.

To access Web Config after configuring HTTPS, enter https:// before the product IP address, shown in step 3.

Note: If the product name is registered with the DNS server, you can use the product name instead of the product IP address to access Web Config.

Parent topic: Using Web Config Network Configuration Software

Changing the Administrator Password in Web Config

You can set an administrator password using your product's control panel or using Web Config or EpsonNet Config. You use the same administrator password in all cases.

Note: See your product's *User's Guide* for instructions on setting an administrator password using the control panel. If you forget your administrator password, contact Epson for support, as described in the product's *User's Guide*.

1. Access Web Config, select **Administrator Settings**, and select **Change Administrator Authentication Information**.

You see a window like this:
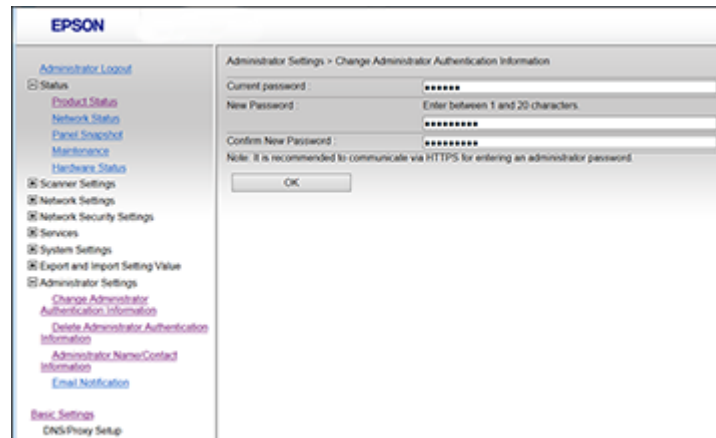
2. Do one of the following:

   - If you have set an administrator password before, enter the current password, then enter and confirm the new password in the fields provided.

   - If you have not set an administrator password before, enter a new password and confirm it in the fields provided

3. Click **OK**

Parent topic: Using Web Config Network Configuration Software

Using Your Product on a Secure Network

Follow the instructions in these sections to configure security features for your product on the network using the Web Config software.

Configuring SSL/TLS Settings
Configuring IPsec/IP Filtering
Configuring SNMPv3 Protocol Settings
Connecting the Product to an IEEE 802.1X Network
Using a Digital Certificate
Configuring Protocols and Services in Web Config
Using an Email Server

Parent topic: Using Web Config Network Configuration Software

Configuring SSL/TLS Settings

If your product supports HTTPS, you can configure SSL/TLS to encrypt communications with your product.

1. Access Web Config and select **Network Security Settings**.

2. Select **SSL/TLS** and select **Basic**.

3. Select one of the options for the **Encryption Strength** setting

4. Select **Enable** or **Disable** for the **Redirect HTTP to HTTPS** setting as necessary.

5. Click **Next**.

   You see a confirmation message.

6. Click **OK**.

Parent topic: Using Your Product on a Secure Network

Configuring IPsec/IP Filtering

Follow the instructions in these sections to configure IPsec/IP traffic filtering using Web Config.

Parent topic: Using Your Product on a Secure Network

About IPsec/IP Filtering

You can filter traffic to the product over the network based on IP address, service, and port by configuring a default policy that applies to every user or group connecting to the product. For control of individual users or user groups, you can configure group policies.

Note: IPsec is supported only by computers running Windows Vista or later, or Windows Server 2008 or later.

Parent topic:

Configuring Default IPsec/IP Filtering Policy

You can configure the default policy for IPsec/IP traffic filtering using Web Config.

1. Access Web Config and select **Network Security Settings**.

2. Select **IPsec/IP Filtering** and select **Basic**.

   You see a window like this:
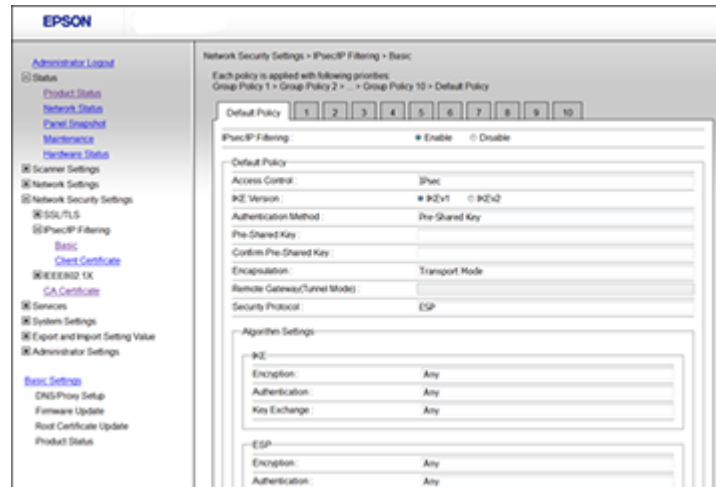
3. Select **Enable** to enable IPsec/IP filtering.

4. Select the filtering options you want to use for the default policy.

5. Click **Next**.

   You see a confirmation message.

6. Click **OK**.

Parent topic:

Configuring Group IPsec/IP Filtering Policies

You can configure group policies for IPsec/IP traffic filtering using Web Config.

1. Access Web Config and select **Network Security Settings**.

2. Select **IPsec/IP Filtering** and select **Basic**.

3. Click a tab number for the policy number you want to configure.

    You see a window like this:

4. Select the **Enable this Group Policy** checkbox.

5. Select the filtering options you want to use for this group policy.

6. Click **Next**.

    You see a confirmation message.

7. Click **OK**.

8. If you want to configure additional group policies, click the next tab number and repeat the configuration steps as necessary.

Parent topic: Configuring IPsec/IP Filtering

IPsec/IP Filtering Policy Settings

Default Policy Settings

Setting	Options/Description
Access Control	Select **Permit Access** to permit IP packets to pass through
	Select **Refuse Access** to prevent IP packets from passing through
	Select **IPsec** to permit IPsec packets to pass through
IKE Version	Select the version of the Internet Key Exchange (IKE) protocol that matches your network environment
Authentication Method	Select an authentication method, or select **Certificate** if you have imported a CA-signed certificate
Pre-Shared Key	If necessary, enter a pre-shared key between 1 and 127 characters long
Confirm Pre-Shared Key	Confirm the pre-shared key you entered
Encapsulation	If you selected **IPsec** as the **Access Control** option, select one of these encapsulation modes:
	Transport Mode: if you are using the product on the same LAN; IP packets of layer 4 or later are encrypted
	Tunnel Mode: if you are using the product on an Internet-capable network, such as IPsec-VPN; the header and data of IP packets are encrypted
Remote Gateway(Tunnel Mode)	If you selected **Tunnel Mode** as the **Encapsulation** option, enter a gateway address between 1 and 39 characters long
Security Protocol	If you selected **IPsec** as the **Access Control** option, select one of these security protocols:
	ESP: to ensure the integrity of authentication and data, and encrypt data
	AH: to ensure the integrity of authentication and data; if data encryption is prohibited, you can use IPsec

Setting	Options/Description
Algorithm Settings	Select the encryption algorithm settings for the security protocol you selected

Group Policy Settings

Setting	Options/Description
Access Control	Select **Permit Access** to permit IP packets to pass through Select **Refuse Access** to prevent IP packets from passing through Select **IPsec** to permit IPsec packets to pass through
Local Address(Scanner)	Select an IPv4 or IPv6 address that matches your network environment; if the IP address is assigned automatically, select **Use auto-obtained IPv4 address**
Remote Address(Host)	Enter the device's IP address (between 0 and 43 characters long) to control access, or leave blank to control all addresses; if the IP address is assigned automatically, such as by DHCP, the connection may be unavailable, so configure a static address instead
Method of Choosing Port	Select the method you want to used for specifiying ports
Service Name	If you selected **Service Name** as the **Method of Choosing Port** option, select a service name option here; see the next table for more information

Setting	Options/Description
Transport Protocol	If you selected **Port Number** as the **Method of Choosing Port** option, select one of these encapsulation modes: **Any Protocol** **TCP** **UDP** **ICMPv4** See the next table for more information
Local Port	If you selected **Port Number** as the **Method of Choosing Port** option, and **TCP** or **UDP** for the **Transport Protocol** option, enter the port numbers that control receiving packets (up to 10 ports), separated by commas, for example **25,80,143,5220**; leave this setting blank to control all ports; see the next table for more information
Remote Port	If you selected **Port Number** as the **Method of Choosing Port** option, and **TCP** or **UDP** for the **Transport Protocol** option, enter the port numbers that control sending packets (up to 10 ports), separated by commas, for example **25,80,143,5220**; leave this setting blank to control all ports; see the next table for more information
IKE Version	Select **IKEv1** or **IKEv2** depending on the device that the product is connected to
Authentication Method	If you selected **IPsec** as the **Access Control** option, select an authentication method here
Pre-Shared Key	If you selected **Pre-Shared Key** as the **Authentication Method** option, enter a pre-shared key between 1 and 127 characters long here and in the **Confirm Pre-Shared Key** field

Setting	Options/Description
Encapsulation	If you selected **IPsec** as the **Access Control** option, select one of these encapsulation modes: **Transport Mode**: if you are using the product on the same LAN; IP packets of layer 4 or later are encrypted **Tunnel Mode**: if you are using the product on an Internet-capable network, such as IPsec-VPN; the header and data of IP packets are encrypted
Remote Gateway(Tunnel Mode)	If you selected **Tunnel Mode** as the **Encapsulation** option, enter a gateway address between 1 and 39 characters long
Security Protocol	If you selected **IPsec** as the **Access Control** option, select one of these security protocols: **ESP**: to ensure the integrity of authentication and data, and encrypt data **AH**: to ensure the integrity of authentication and data; if data encryption is prohibited, you can use IPsec
Algorithm Settings	Select the encryption algorithm settings for the security protocol you selected

Group Policy Guidelines

Service name	Protocol type	Local/Remote port number	Operations controlled
ENPC	UDP	3289/Any port	Searching for a product from applications such as scanner drivers or EpsonNet Config
SNMP	UDP	161/Any port	Acquiring and configuring MIB from applications such as scanner drivers or EpsonNet Config
WSD	TCP	Any port/5357	Controlling WSD
WS-Discovery	UDP	3702/Any port	Searching for a product from WSD

Service name	Protocol type	Local/Remote port number	Operations controlled
Network Scan	TCP	1865/Any port	Forwarding scan data from Document Capture Pro
Network Push Scan	TCP	Any port/2968	Acquiring job information on push scanning from Document Capture Pro
Network Push Scan Discovery	UDP	2968/Any port	Searching for a computer during push scanning from Document Capture Pro
HTTP (Local)	TCP	80/Any port	Forwarding Web Config and WSD data to a HTTP or HTTPS server
HTTPS (Local)	TCP	443/Any port	
HTTP (Remote)	TCP	Any port/80	Communicating with firmware update and root certificate update on a HTTP or HTTPS client
HTTPS (Remote)	TCP	Any port/443	

Parent topic:

IPsec/IP Filtering Configuration Examples

You can configure IPsec and IP filtering in a variety of ways, as shown in the examples here.

Receiving IPsec Packets Only

Use this example only for configuring a default policy.

- **IPsec/IP Filtering**: **Enable**
- **Access Control**: **IPsec**
- **Authentication Method**: **Pre-Shared Key**
- **Pre-Shared Key**: Enter a key up to 127 characters long

Accepting Scan Using Epson Scan 2 and Scanner Settings

Use this example to allow communication of scanning data and scanner settings from specified services.

Default policy:

- **IPsec/IP Filtering**: **Enable**
- **Access Control**: **Refuse Access**

Group policy:

- **Enable this Group Policy**: Select this box
- **Access Control**: **Permit Access**
- **Remote Address(Host)**: Client IP address
- **Method of Choosing Port**: **Service Name**
- **Service Name**: Select **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)**, and **HTTPS (Local)**

Receiving Access from a Specified IP Address Only

In these examples, the client will be able to access and configure the product in any policy configuration.

Default policy:

- **IPsec/IP Filtering**: **Enable**
- **Access Control**: **Refuse Access**

Group policy:

- **Enable this Group Policy**: Select this box
- **Access Control**: **Permit Access**
- **Remote Address (Host)**: Administrator's client IP address

Parent topic: Configuring IPsec/IP Filtering

Configuring an IPsec/IP Filtering Certificate

You can configure a certificate for IPsec/IP traffic filtering using Web Config.

1. Access Web Config and select **Network Security Settings**.
2. Select **IPsec/IP Filtering** and select **Client Certificate**.

You see a window like this:
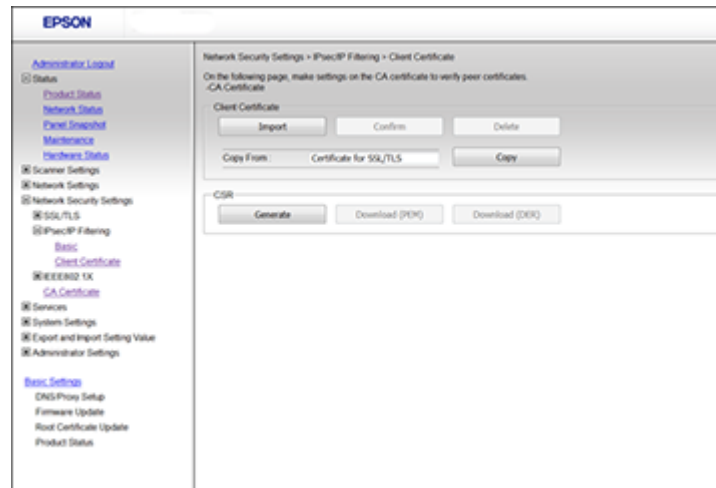
3. Do one of the following:

   • Click **Import** to add a new client certificate.

   • Select the certificate you want to use as the **Copy From** option and click **Copy**.

4. Click **OK**.

Parent topic: Configuring IPsec/IP Filtering

Related tasks

Obtaining and Importing a CA-signed Certificate

Configuring SNMPv3 Protocol Settings

If your product supports the SNMPv3 protocol, you can monitor and control access to your product using that protocol.

1. Access Web Config and select **Services**.

2. Select **Protocol**.

You see a window like this:
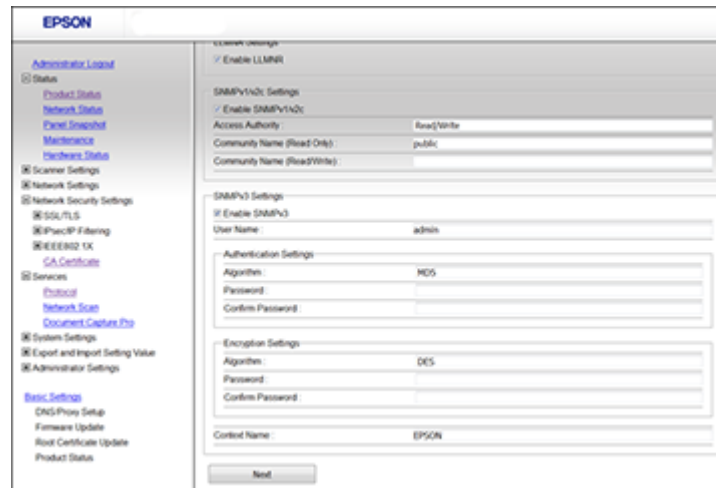
3. Select the **Enable SNMPv3** checkbox to enable SNMPv3 settings.

4. Select the settings you want in SNMPv3 Settings section.

5. Click **Next**.

    You see a confirmation message.

6. Click **OK**.

SNMPv3 Settings

Parent topic: Using Your Product on a Secure Network

SNMPv3 Settings

You can configure these SNMPv3 settings in Web Config.

Setting	Options/Description
User Name	Enter a user name from 1 to 32 characters long in ASCII
Authentication Settings	
Algorithm	Select the algorithm for authentication

Setting	Options/Description
Password	Enter a password from 8 to 32 characters long in ASCII
Confirm Password	Enter the authentication password again
Encryption Settings	
Algorithm	Select the algorithm for encryption
Password	Enter a password from 8 to 32 characters long in ASCII
Confirm Password	Enter the encryption password again
Context Name	Enter a context name from 1 to 32 characters long in ASCII

Parent topic: Configuring SNMPv3 Protocol Settings

Connecting the Product to an IEEE 802.1X Network

Follow the instructions in these sections to connect the product to an IEEE 802.1X network using Web Config.

Configuring an IEEE 802.1X Network

IEEE 802.1X Network Settings

Configuring a Certificate for an IEEE 802.1X Network

Parent topic: Using Your Product on a Secure Network

Configuring an IEEE 802.1X Network

If your product supports IEEE 802.1X, you can use it on a network with authentication provided by a RADIUS server with a hub as an authenticator using Web Config.

1. Access Web Config and select **Network Security Settings**.

2. Select **IEEE802.1X** and select **Basic**.

You see a window like this:
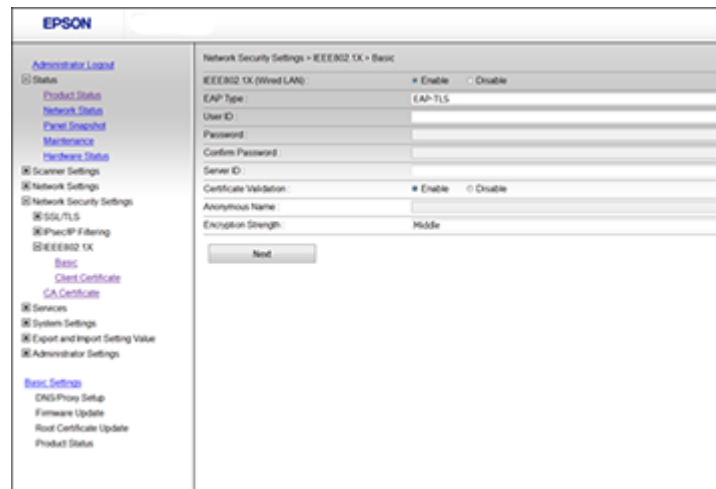
3. Select **Enable** as the **IEEE802.1X (Wired LAN)** setting.

4. Select the IEEE 802.1X setting options you want to use.

5. Click **Next**.

   You see a confirmation message.

6. Click **OK**.

Parent topic:

IEEE 802.1X Network Settings

You can configure these IEEE 802.1X network settings in Web Config.

Setting	Options/Description
EAP Type	Select one of these authentication methods for connections between the product and a RADIUS server:
	EAP-TLS or **PEAP-TLS**: You must obtain and import a CA-signed certificate
	PEAP/MSCHAPv2: You must configure a password

Setting	Options/Description
User ID	Enter an ID between 1 and 128 ASCII characters for authentication on a RADIUS server
Password	Enter a password between 1 and 128 ASCII characters for authentication of the product. If you are using Windows as a RADIUS server, enter up to 127 ASCII characters.
Confirm Password	Enter the authentication password again
Server ID	Enter a server ID between 1 and 128 ASCII characters for authentication on a specified RADIUS server; server ID is verified in the subject/subjectAltName field of a server certificate sent from the RADIUS server
Certificate Validation	Select a valid certificate regardless of the authentication method; import the certificate using the **CA Certificates** option
Anonymous Name	If you selected **PEAP-TLS** or **PEAP/MSCHAPv2** as the **Authentication Method** setting, you can configure an anonymous name between 1 and 128 ASCII characters instead of a user ID for phase 1 of a PEAP authentication
Encryption Strength	Select one of the following encryption strengths: **High** for AES256/3DES **Middle** for AES256/3DES/AES128/RC4

Parent topic: Connecting the Product to an IEEE 802.1X Network

Configuring a Certificate for an IEEE 802.1X Network

If your product supports IEEE 802.1X, you can configure a certificate for the network using Web Config.

1. Access Web Config and select **Network Security Settings**.

2. Select **IEEE802.1X** and select **Client Certificate**.

You see a window like this:
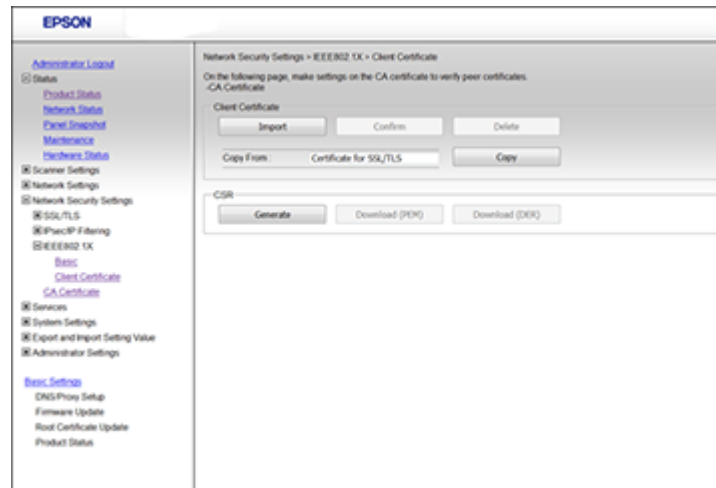
3. Do one of the following:

   - Click **Import** to add a new client certificate.
   - Select the certificate you want to use as the **Copy From** option and click **Copy**.

4. Click **OK**.

Parent topic: Connecting the Product to an IEEE 802.1X Network

Using a Digital Certificate

Follow the instructions in these sections to configure and use digital certificates using Web Config.

About Digital Certification
Obtaining and Importing a CA-signed Certificate
CSR Setup Settings
CSR Import Settings
Deleting a CA-signed Certificate
Updating a Self-signed Certificate
Importing a CA Certificate
Deleting a CA Certificate

Parent topic:

About Digital Certification

You can configure the following digital certificates for your network using Web Config:

CA-signed Certificate
You can ensure secure communications using a CA-signed certificate for each security feature. The certificates must be signed by and obtained from a CA (Certificate Authority).

CA Certificate
A CA certificate indicates that a third party has verified the identity of a server. You need to obtain a CA certificate for server authentication from a CA that issues it.

Self-signed Certificate
A self-signed certificate is issued and signed by the product itself. You can use the certificate for only SSL/TLS communication, however security is unreliable and you may see a security alert in the browser during use.

Parent topic:

Obtaining and Importing a CA-signed Certificate

You can obtain a CA-signed certificate by creating a CSR (Certificate Signing Request) using Web Config and submitting it to a certificate authority. The CSR created in Web Config is in PEM/DER format. You can import one CSR created from Web Config at a time.

1. Access Web Config and select **Network Security Settings**.

2. Select one of the following network security options and corresponding certificates:

   • **SSL/TLS** and select **Certificate**

   • **IPsec/IP Filtering** and select **Client Certificate**

   • **IEEE802.1X** and select **Client Certificate**

3. In the CSR section, select **Generate**.

You see a window like this:
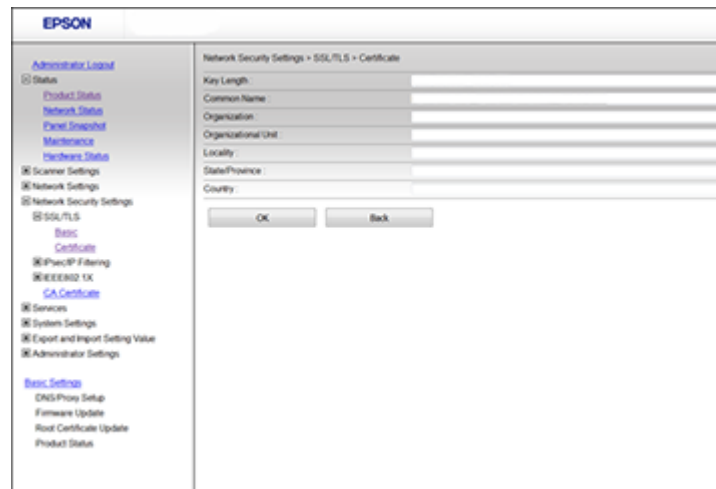
4. Select the CSR setting options you want to use.

5. Click **OK**.

    You see a completion message.

6. Select **Network Security Settings** and select one of the following network security options and corresponding certificates:

    *   **SSL/TLS** and select **Certificate**

    *   **IPsec/IP Filtering** and select **Client Certificate**

    *   **IEEE802.1X** and select **Client Certificate**

7. In the CSR section, click the **Download** option that matches the format specified by your certificate authority to download the CSR.

    Caution: Do not generate another CSR or you may not be able to import a CA-signed certificate.

8. Submit the CSR to the certificate authority following the format guidelines provided by that authority.

9. Save the issued CA-signed certificate to a computer connected to the product.

    Before proceeding, make sure the time and date settings are correct on your product. See the product's *User's Guide* for instructions.

10. Select **Network Security Settings** and select one of the following network security options and corresponding certificates:

- **SSL/TLS** and select **Certificate**
- **IPsec/IP Filtering** and select **Client Certificate**
- **IEEE802.1X** and select **Client Certificate**

11. In the CA Certificate section, click **Import**.

You see a window like this:
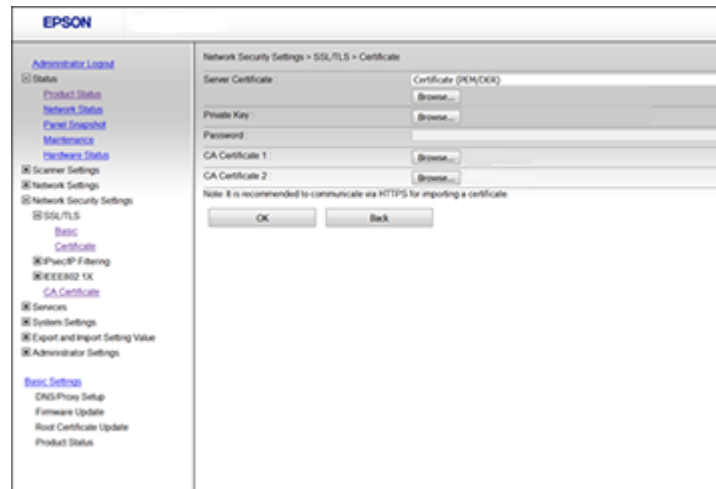
12. Select the format of the certificate as the **Server Certificate** setting.

13. Select the certificate import settings as necessary for the format and the source from which you obtained it.

14. Click **OK**.

You see a confirmation message.

15. Click **Confirm** to verify the certificate information.

Parent topic: Using a Digital Certificate

CSR Setup Settings

You can select these settings when setting up a CSR in Web Config.

Note: The available key length and abbreviations vary by certificate authority, so follow the rules of that authority when entering information in the CSR.

Setting	Options/Description
Key Length	Select a key length for the CSR
Common Name	Enter a name or static IP address from 1 to 128 characters long; for example, **Reception printer** or **https://10.152.12.225**
Organization, **Organizational Unit**, **Locality**, **State/Province**	Enter information in each field as necessary, from 0 to 64 characters long in ASCII; separate any multiple names with commas
Country	Enter a two-digit country code number as specified by the ISO-3166 standard

Parent topic:

CSR Import Settings

You can configure these settings when importing a CSR in Web Config.

Note: The import setting requirements vary by certificate format and how you obtained the certificate.

Certificate format	Setting descriptions
PEM/DER format obtained from Web Config	**Private Key**: Do not configure because the product contains a private key **Password**: Do not configure **CA Certificate 1/CA Certificate 2**: Optional
PEM/DER format obtained from a computer	**Private Key**: Configure a private key **Password**: Do not configure **CA Certificate 1/CA Certificate 2**: Optional
PKCS#12 format obtained from a computer	**Private Key**: Do not configure **Password**: Optional **CA Certificate 1/CA Certificate 2**: Do not configure

Parent topic:

Deleting a CA-signed Certificate

You can delete an imported CA-signed certificate with Web Config when the certificate expires or if you have no more need for an encrypted connection.

Note: If you obtained a CA-signed certificate from Web Config, you cannot import a deleted certificate; you must obtain and import a new certificate.

1. Access Web Config and select **Network Security Settings**.
2. Select one of the following network security options and corresponding certificate:
   - **SSL/TLS** and select **Certificate**
   - **IPsec/IP Filtering** and select **Client Certificate**
   - **IEEE802.1X** and select **Client Certificate**
3. Click **Delete**.

   You see a completion message.
4. Click **OK**.

Parent topic:

Updating a Self-signed Certificate

If your product supports the HTTPS server feature, you can update a self-signed certificate using Web Config.

1. Access Web Config and select **Network Security Settings**, select **SSL/TLS**, and select **Certificate**.
2. Click **Update**.

You see a window like this:

3. Enter an identifier for your product from 1 to 128 characters long in the **Common Name** field.
4. Select a validity period for the certificate as the **Certificate Validity (year)** setting.
5. Click **Next**.

   You see a completion message.
6. Click **OK**.
7. Click **Confirm** to verify the certificate information.

   Parent topic: Using a Digital Certificate

Importing a CA Certificate

You can import a CA certificate using Web Config.

1. Access Web Config and select **Network Security Settings**.
2. Select **CA Certificate**.
3. Select **Import**.

4. Select the CA certificate you want to import.
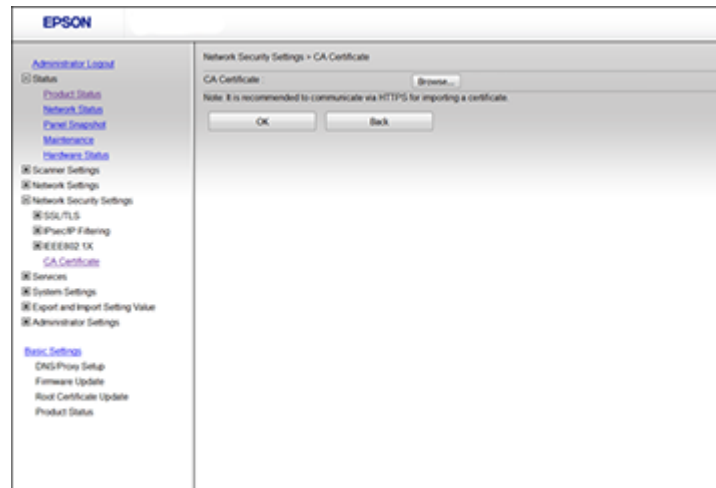
5. Click **OK**.

When you see the **CA Certificate** page and the imported certificate is displayed, the import is finished.

Parent topic: Using a Digital Certificate

Deleting a CA Certificate

You can delete an imported CA certificate with Web Config when the certificate expires or if you have no more need for an encrypted connection.

1. Access Web Config and select **Network Security Settings**.

2. Select **CA Certificate**.
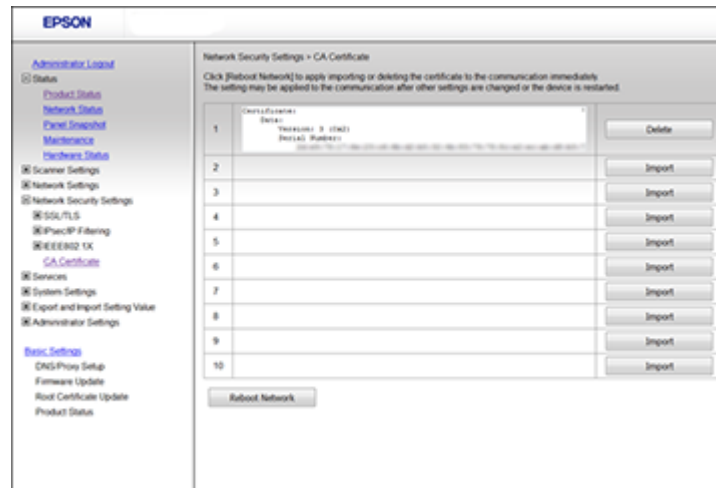
3. Locate the certificate you want to remove and click the **Delete** button next to it.

4. Click **OK** to confirm the deletion.

   Parent topic: Using a Digital Certificate

Configuring Protocols and Services in Web Config

You can enable or disable protocols using Web Config.

1. Access Web Config, select **Services**, and select **Protocol**.

2. Select or deselect the checkbox next to the service name to enable or disable a protocol.

3. Configure any other available protocol settings.

4. Click **Next**.

5. Click **OK**.

6. Select and configure services and protocol settings as necessary.

After the protocols restart, the changes are applied.

Protocol Settings

Parent topic: Using Your Product on a Secure Network

Protocol Settings

You can configure these protocol settings in Web Config.

Protocols

Name	Description
Bonjour	Use Bonjour to search for devices and AirPrint
SLP	Use SLP for push-scanning and network searching in EpsonNet Config
WSD	Add WSD devices, or print and scan from the WSD port
LLTD	Displays the product on the Windows network map
LLMNR	Use name resolution without NetBIOS even if you cannot use DNS
SNMPv1/v2c	Remotely set up and monitor your product
SNMPv3	Remotely set up and monitor your product with the SNMPv3 protocol

Bonjour Settings

Setting	Options/Description
Use Bonjour	Search for or use devices through Bonjour (you cannot use AirPrint if disabled)
Bonjour Name	Displays the Bonjour name
Bonjour Service Name	Displays the Bonjour service name
Location	Displays the Bonjour location name

SLP Settings

Setting	Options/Description
Enable SLP	Enable the SLP function to use the Push Scan function and network searching in EpsonNet Config

WSD Settings

Setting	Options/Description
Enable WSD	Enable adding devices using WSD, and printing and scanning from the WSD port
Scanning Timeout (sec)	Enter the communication timeout value for WSD scanning between 3 and 3600 seconds
Device Name	Displays the WSD device name
Location	Displays the WSD location name

LLTD Settings

Setting	Options/Description
Enable LLTD	Enable LLTD to display the product in the Windows network map
Device Name	Displays the LLTD device name

LLMNR Settings

Setting	Options/Description
Enable LLMNR	Enable LLMNR to use name resolution without NetBIOS, even if you cannot use DNS

SNMPv1/v2c Settings

Setting	Options/Description
Enable SNMPv1/v2c	Enable SNMPv1/v2c for products that support SNMPv3
Access Authority	Set the access authority when SNMPv1/v2c is enabled to **Read Only or Read/Write**
Community Name (Read Only)	Enter 0 to 32 ASCII characters
Community Name (Read/Write)	Enter 0 to 32 ASCII characters

SNMPv3 Settings

Setting	Options/Description
Enable SNMPv3	Enable SNMPv3 for products that support SNMPv3
User Name	Enter 1 to 32 characters
Authentication Settings	Select an algorithm and set a password for authentication
Encryption Settings	Select an algorithm and set a password for encryption
Context Name	Enter 1 to 32 characters

Parent topic: Configuring Protocols and Services in Web Config

Related references

SNMPv3 Settings

Using an Email Server

Follow the instructions in these sections to use an email server to send scan and fax data by email, or use email notification using Web Config.

Configuring an Email Server
Email Server Settings
Checking the Email Server Connection
Email Server Connection Report Messages
Configuring Email Notification

Parent topic: Using Your Product on a Secure Network

Configuring an Email Server

You can configure an email server using Web Config.

1. Access Web Config and select **Network Settings**.

2. Select **Email Server** and select **Basic**.

You see a window like this:
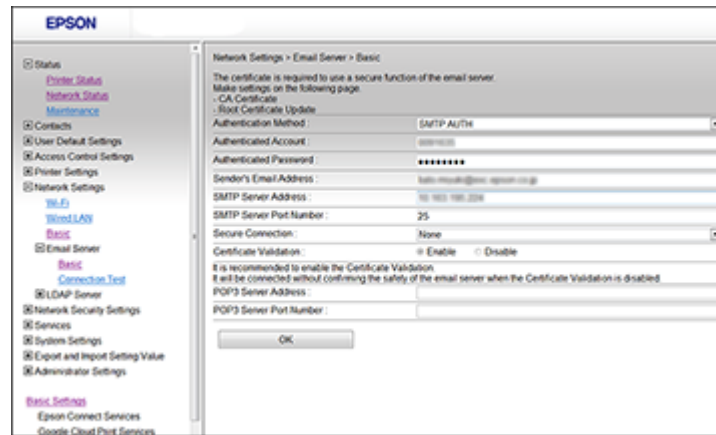
3. Select the email server settings.

4. Click **OK**.

Parent topic:

Email Server Settings

You can configure these email server settings in Web Config.

Setting	Options/Description
Authentication Method	Select the authentication method that matches your email server
Authenticated Account	Enter the authenticated account name from 1 to 255 characters long in ASCII
Authenticated Password	Enter the authenticated password from 1 to 20 characters long in ASCII using A-Z, a-z, 0-9, and these characters: ! # $ % ' * + - . / = ? ^ _ { ! } ~ @
Sender's Email Address	Enter the sender's email address from 1 to 255 characters long in ASCII; do not use a period (.) as the first character or use these characters: ( ) < > [ ] ;

Setting	Options/Description
SMTP Server Address	Enter the SMTP server address from 1 to 255 characters long using A-Z, a-z, 0-9, and "-" in IPv4 or FQDN format
SMTP Server Port Number	Enter the SMTP server port number between 1 and 65535
Secure Connection	Select the security method for the email server; available choices depend on the **Authentication Method** setting
Certificate Validation	Enable checking for a valid certificate; recommended value is **Enable**
POP3 Server Address	Enter the POP server address from 1 to 255 characters long using A-Z, a-z, 0-9, and "-" in IPv4 or FQDN format
POP3 Server Port Number	Enter the POP server port number between 1 and 65535

Parent topic: Using an Email Server

Checking the Email Server Connection

You can test the email server connection and view a connection report using Web Config.

1. Access Web Config and select **Network Settings**.

2. Select **Email Server** and select **Connection Test**.

3. Click **Start**.

   Web Config tests the connection and displays the connection report when it is finished.

Parent topic: Using an Email Server

Email Server Connection Report Messages

You can review the connection report messages to diagnose email server connection problems in Web Config.

Message	Description
Connection test was successful.	Connection to the server is successful

Message	Description
SMTP server communication error. Check the following - Network Settings	One of the following has occurred: • Product is not connected to a network • SMTP server is down • Network connection is disrupted while communicating • Received incomplete data
POP3 server communication error. Check the following - Network Settings	One of the following has occurred: • Product is not connected to a network • POP3 server is down • Network connection is disrupted while communicating • Received incomplete data
An error occurred while connecting to SMTP server. Check the following - SMTP Server Address - DNS Server	One of the following has occurred: • DNS resolution failed • Name resolution for an SMTP server failed
An error occurred while connecting to POP3 server. Check the following - POP3 Server Address - DNS Server	One of the following has occurred: • DNS resolution failed • Name resolution for an SMTP server failed
SMTP server authentication error. Check the following - Authentication Method - Authenticated Account - Authenticated Password	SMTP server authentication failed
POP3 server authentication error. Check the following - Authentication Method - Authenticated Account - Authenticated Password	POP3 server authentication failed
Unsupported communication method. Check the following - SMTP Server Address - SMTP Server Port Number Secure connection (SSL) is unsupported.	The communication protocol is unsupported

Message	Description
Connection to SMTP server failed. Change Secure Connection to None.	There is an SMTP mismatch between a server and a client, or when the server does not support an SMTP secure connection
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	There is an SMTP mismatch between a server and a client, or the server requests an SSL/TLS connection for SMTP
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	There is an SMTP mismatch between a server and a client, or when the server requests a STARTTLS connection for SMTP
The connection is untrusted. Check the following - Date and Time	The product's date and time setting is incorrect or the certificate has expired
The connection is untrusted. Check the following - CA Certificate	The product has a root certificate mismatch or a CA Certificate has not been imported
The connection is not secured.	The certificate is damaged
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Authentication method mismatch between a server and a client. The server does not support SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Authentication method mismatch between a server and a client. The server does not support SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	The specified sender's Email address is wrong
Cannot access the product until processing is complete.	The product is busy

**Parent topic:** Using an Email Server

Configuring Email Notification

You can configure email notifications using Web Config so you can receive alerts by email when certain events occur on the product. You can register up to 5 email addresses and select the events for which you want to be notified.

1. Access Web Config and select **Administrator Settings**.

2. Select **Email Notification**.

You see a window like this:
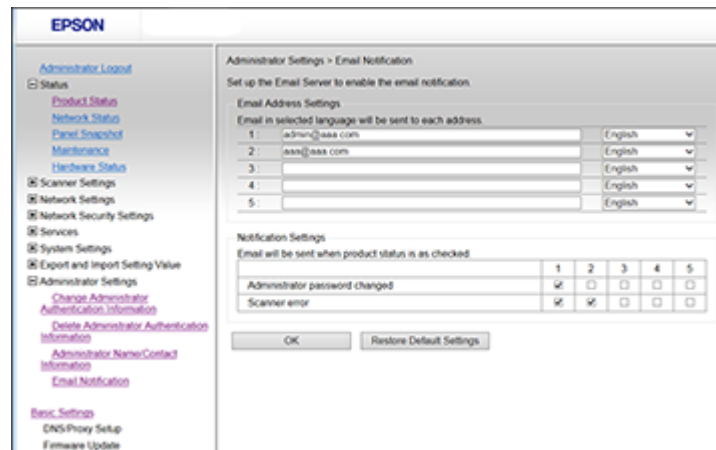
3. Enter an email address in the **1** field.

4. Select the language in which you want to receive the email notifications from the drop-down menu for the first email address.

5. Enter additional email addresses in fields **2** through **5** as necessary, and select a language for each.

6. Select the checkboxes to indicate the events for which you want to receive email notifications.

7. Click **OK**.

Parent topic: Using an Email Server

Importing and Exporting Web Config Settings

Follow the instructions in these sections to import and export your product's settings using the Web Config software.

Exporting Settings Using Web Config

Importing Settings Using Web Config

Parent topic: Using Your Product on a Secure Network

Exporting Settings Using Web Config

You can export your product's settings and optionally encrypt the settings file with a password.

1. Access Web Config and select **Export and Import Setting Value**.

2. Select **Export**.

3. Select the settings you want to export.

   Note: If you select a parent category, the child categories are also selected. By default, items that are unique on the network, such as IP address, cannot be selected. If you want to export these items, select **Enable to select the individual settings of device**. It is recommended that you export only unique items when replacing a product on the network, otherwise you may encounter conflicts on the network.

4. Enter an encryption password, if desired.

5. Click **Export** and save the file.

Parent topic: Importing and Exporting Web Config Settings

Importing Settings Using Web Config

You can import settings to your product that you have exported previously. If encryption was used when the settings were exported, obtain the necessary password before you import.

1. Access Web Config and select **Export and Import Setting Value**.

2. Select **Import**.

3. Click **Browse** and select the exported settings file.

4. If necessary, enter the decryption password.

5. Click **Next**.

6. Select the settings to import and click **Next**.

7. Click **OK**.

The selected settings are imported to the product.

Parent topic: Importing and Exporting Web Config Settings

Using EpsonNet Config Network Configuration Software

Follow the instructions in these sections to configure your product's administrator network settings using the EpsonNet Config software.

With Windows, you can configure network settings in a batch operation. See the EpsonNet Config help utility for instructions.

Note: Before you can configure system administration settings, connect the product to a network. See the product's *User's Guide* for instructions.

Installing EpsonNet Config
Configuring a Product IP Address Using EpsonNet Config

Installing EpsonNet Config

To install EpsonNet Config, download the software from the product's support page at epson.com/support (U.S.), epson.ca/support (Canada), or epson.com.jm/support (Caribbean) and follow the on-screen instructions.

Parent topic: Using EpsonNet Config Network Configuration Software

Configuring a Product IP Address Using EpsonNet Config

You can configure the product's IP address using EpsonNet Config.

1. Turn on the product.

2. Connect the product to a network using an Ethernet cable.

3. Do one of the following to start EpsonNet Config:

    *   **Windows 10**: Click [ ] and select **EpsonNet** > **EpsonNet Config**.

    *   **Windows 8.x**: Navigate to the **Apps** screen and select **EpsonNet** > **EpsonNet Config**.

    *   **Windows (other versions)**: Click [ ] or **Start** and select **All Programs** or **Programs**. Select **EpsonNet** > **EpsonNet Config**.

    *   **Mac**: Open the **Applications** folder, open the **Epson Software** folder, and select **EpsonNet** > **EpsonNet Config** > **EpsonNet Config**.

    After a few moments, the program displays the connected products.

4. Double-click the product you are configuring.

   Note: If several products of the same model are connected, you can identify them by their MAC address.

5. From the menu on the left, select **TCP/IP**, and select **Basic**.

   You see a window like this:
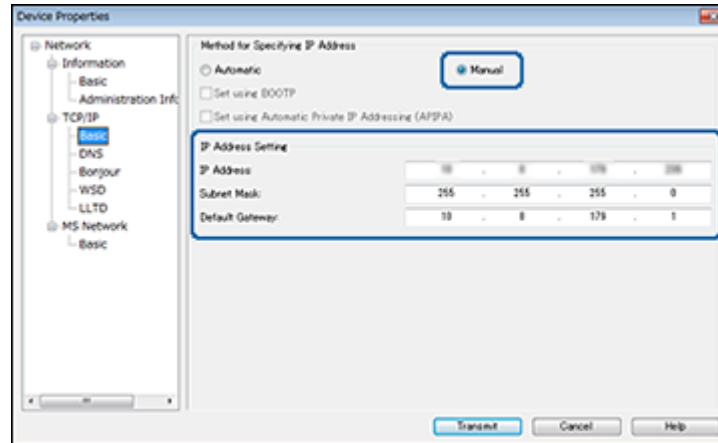
6. Select **Manual**.

7. Enter the product's **IP address**, **Subnet Mask**, and **Default Gateway** settings in the fields provided.

   Note: To connect the product to a secure network, enter a static IP address. You can also configure the DNS settings by selecting **DNS**, and enter proxy settings by selecting **Internet** from the **TCP/IP** menu.

8. Select **Transmit**.

Parent topic: Using EpsonNet Config Network Configuration Software

Using Epson Device Admin Configuration Software

With Windows, you can discover and monitor remote devices, and configure network settings in a batch operation. See the Epson Device Admin help for instructions.

To install Epson Device Admin, download the software from the support page at epson.com/support (U.S.), epson.ca/support (Canada), or epson.com.jm/support (Caribbean) and follow the on-screen instructions.

Solving Problems

Check these sections for solutions to problems you may have with the network configuration software.

Solving Network Software Usage Problems

Solving Network Security Problems

Solving Digital Certificate Problems

Where to Get Help

Solving Network Software Usage Problems

Check these sections if you have problems using the network software.

Cannot Access Web Config

The "Out of Date" Message Appears

"The name of the security certificate does not match" Message Appears

Model Name or IP Address Not Displayed in EpsonNet Config

Parent topic: Solving Problems

Cannot Access Web Config

If you cannot access Web Config on your product, try these solutions:

• Make sure your product is turned on and connected to your network using the correct IP address. Verify connection using your product control panel. See your product's *User's Guide* for instructions.

• If you selected **High** as the **Encryption Strength** setting in Web Config, your browser must support AES (256-bit) or 3DES (168-bit) encryption. Check your browser's encryption support or select a different **Encryption Strength** option.

• If you are using a proxy server with your product, configure the browser's proxy settings as follows:

   • **Windows 10**: Click [icon] and select **Settings** > **Network and Internet** > **Proxy**. Scroll down and set **Use a proxy server** to **On**. Select **Don't use proxy server for local (Intranet) addresses**.

   • **Windows 8.x**: Navigate to the **Apps** screen and select **PC Settings** > **Network** > **Proxy**. Scroll down and set **Use a proxy server** to **On**. Select **Don't use proxy server for local (Intranet) addresses**.

   • **Windows (other versions)**: Click [icon] or **Start** and select **Control Panel** > **Network and Internet** > **Internet Options** > **Connections** > **LAN settings** > **Proxy server** > **Bypass proxy server for local addresses**.

- **Mac**: Select **System Preferences** > **Network** > **Advanced** > **Proxies**. Register the local address under **Bypass proxy settings for these Hosts & Domains**. For example, 192.168.1.*: Local address 192.168.1.XXX, subnet mask 255.255.255.0.

Parent topic: Solving Network Software Usage Problems

The "Out of Date" Message Appears

If the "Out of Date" message appears when you access Web Config using SSL communication (HTTPS), the certificate is out of date. Make sure that the product date and time are configured correctly, and obtain a new certificate.

Parent topic: Solving Network Software Usage Problems

"The name of the security certificate does not match" Message Appears

If a message beginning with "The name of the security certificate does not match . . ." appears when you access Web Config using SSL communication (HTTPS), the product's IP address on the CSR or self-signed certificate does not match what you entered in the browser. Change the IP address you entered for the **Common Name** setting, and obtain and import a certificate again, or change the product name.

Parent topic: Solving Network Software Usage Problems

Model Name or IP Address Not Displayed in EpsonNet Config

If the product model name and/or IP address is not displayed in EpsonNet Config, try these solutions:

- If you selected the block, cancel, or shut down option on a Windows security or firewall screen, the IP address and model name cannot display in EpsonNet Config. Register EpsonNet config as an exception in your firewall or security software, or close the security software and try running EpsonNet Config again.

- The operation may have timed out. Select **Tools**, select **Options**, select **Timeout**, and increase the time option for the **Communication Error** setting. This may cause EpsonNet Config to run slower, however.

Parent topic: Solving Network Software Usage Problems

Solving Network Security Problems

Check these sections if you have problems using the network security features.

Pre-Shared Key was Forgotten
Cannot Communicate with the Product Using IPsec Communication
Communication was Working, but Stopped

Parent topic: Solving Problems

Pre-Shared Key was Forgotten

If you forget a pre-shared key, change the key using Web Config for the default or group policy.

Parent topic: Solving Network Security Problems

Cannot Communicate with the Product Using IPsec Communication

Make sure your computer is using one of these supported algorithms for communicating with the product:

Security method	Supported algorithms
IKE encryption algorithm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE authentication algorithm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE key exchange algorithm	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*
ESP encryption algorithm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP authentication algorithm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH authentication algorithm	

* Available for IKEv2 only

Parent topic: Solving Network Security Problems

Communication was Working, but Stopped

If network communication was working, but suddenly stopped, the product's and/or computer's IP address may have changed or is invalid. Try these solutions:

- Disable IPsec using the product control panel.
- If DHCP is out of date, or the IPv6 address is out of date or was not obtained, you may not be able to find the IP address registered in Web Config.
- If that does not solve the problem, enter a static IP address using Web Config.

Parent topic: Solving Network Security Problems

Cannot Connect After Configuring IPsec/IP Filtering

The set value may be incorrect. Disable IPsec/IP filtering from the product's control panel. Connect from the computer and configure the IPsec/IP Filtering settings again.

Parent topic: Solving Network Security Problems

Cannot Access the Product After Configuring IEEE 802.1X

If you cannot access the product after configuring it for IEEE 802.1X, disable IEEE 802.1X using the product control panel. Then connect the product to a computer and configure IEEE 802.1X using Web Config again.

Parent topic: Solving Network Security Problems

Solving Digital Certificate Problems

Check these sections if you have problems using a digital certificate.

Digital Certificate Warning Messages
Cannot Import a Digital Certificate
Cannot Update a Certificate or Create a CSR
Deleted a CA-signed Certificate

Parent topic: Solving Problems

Digital Certificate Warning Messages

If you see a warning message when using a digital certificate, check for solutions in this table.

Message	Solution
Enter a Server Certificate.	Select a certificate file and click **Import**.
CA Certificate 1 is not entered.	Import CA certificate 1 before importing additional certificates.
Invalid value below.	Remove any unsupported characters in the file path and password.
Invalid date and time.	Set the date and time on the product using Web Config, EpsonNet Config, or the product control panel.
Invalid password	Enter the password that matches the password set for the CA certificate.
Invalid file	Try the following: • Import only certificate files in X509 format sent by a trusted certificate authority. • Make sure the file size is 5KB or less and is not corrupted or fabricated. • Make sure the chain in the certificate is valid; check the certificate authority's website.
Cannot use the Server Certificates that include more than three CA certificates.	Import certificate files in PKCS#12 format that contains one or two CA certificates, or convert each certificate to PRM format and import them again.
The certificate has expired. Check if the certificate is valid, or check the date and time on your printer.	Make sure the product time and date are set correctly and, if the certificate is out of date, obtain and import a new certificate.

Message	Solution
Private key is required.	Do one of the following to pair a private key with the certificate: • For PEM/DER format certificates obtained from a CSR using a computer, specify the private key file. • For PKCS#12 format certificates obtained from a CSR using a computer, create a file containing the private key. If you re-imported a PEM/DER format certificate obtained from a CSR using Web Config, you can only import it once. You must obtain and import a new certificate.
Setup failed.	Make sure the computer and product are connected, and the certificate file is not corrupted, then import the certificate file again.

Parent topic: Solving Digital Certificate Problems

Cannot Import a Digital Certificate

If you cannot import a digital certificate, try these solutions:

• Make sure the CA-signed certificate and the CSR have the same information. If they do not match, import the certificate to a device that matches the information or use the CSR to obtain the CA-signed certificate again.

• Make sure the CA-signed certificate file size is 5KB or less.

• Make sure you are entering the correct password.

Parent topic: Solving Digital Certificate Problems

Cannot Update a Certificate or Create a CSR

If you cannot update a self-signed certificate or create a CSR for a CA-signed certificate, try these solutions:

• Make sure that you entered a **Common Name** setting in Web Config.

• Make sure the **Common Name** setting does not contain unsupported characters or is divided by a comma. Correct the setting and update the certificate again.

Parent topic: Solving Digital Certificate Problems

Deleted a CA-signed Certificate

If you accidentally deleted a CA-signed certificate, try these solutions:

- If you retained a backup file, import the CA-signed certificate again.
- If you obtained the certificate using a CSR created in Web Config, you cannot import a deleted certificate. Create a new CSR and obtain a new certificate.

Parent topic: Solving Digital Certificate Problems

Where to Get Help

If you need to contact Epson for technical support services, use the following support options.

Internet Support

Visit Epson's support website at epson.com/support (U.S.), epson.ca/support (Canada), or epson.com.jm/support (Caribbean) and select your product for solutions to common problems. You can download drivers and documentation, get FAQs and troubleshooting advice, or e-mail Epson with your questions.

Speak to a Support Representative

Before you call Epson for support, please have the following information ready:

- Product name
- Product serial number (located on a label on the product)
- Proof of purchase (such as a store receipt) and date of purchase
- Computer configuration
- Description of the problem

Then see your product's *User's Guide* for contact information.

Parent topic: Solving Problems

Notices

Check these sections for important notices.

Trademarks

Copyright Notice

Trademarks

EPSON® is a registered trademark and EPSON Exceed Your Vision is a registered logomark of Seiko Epson Corporation.

Mac is a trademark of Apple Inc., registered in the U.S. and other countries.

General Notice: Other product names used herein are for identification purposes only and may be trademarks of their respective owners. Epson disclaims any and all rights in those marks.

EPSON®
EXCEED YOUR VISION

Parent topic: Notices

Copyright Notice

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Seiko Epson Corporation. The information contained herein is designed only for use with this Epson product. Epson is not responsible for any use of this information as applied to other products.

Neither Seiko Epson Corporation nor its affiliates shall be liable to the purchaser of this product or third parties for damages, losses, costs, or expenses incurred by purchaser or third parties as a result of: accident, misuse, or abuse of this product or unauthorized modifications, repairs, or alterations to this product, or (excluding the U.S.) failure to strictly comply with Seiko Epson Corporation's operating and maintenance instructions.

Seiko Epson Corporation shall not be liable for any damages or problems arising from the use of any options or any consumable products other than those designated as Original Epson Products or Epson Approved Products by Seiko Epson Corporation.

Seiko Epson Corporation shall not be held liable for any damage resulting from electromagnetic interference that occurs from the use of any interface cables other than those designated as Epson approved Products by Seiko Epson Corporation.

This information is subject to change without notice.

Copyright Attribution

Parent topic: Notices

Copyright Attribution

Parent topic: Copyright Notice