

Administrator's Guide

Contents

Administrator's Guide	5
Using Web Config Network Configuration Software	6
About Web Config	6
Accessing Web Config	6
Restricting Features Available for Users	7
User Feature Restriction.....	8
Configuring User Feature Restrictions.....	8
Changing the Administrator Password in Web Config	10
Using Your Product on a Secure Network	11
Configuring SSL/TLS Communication.....	11
Configuring SSL/TLS Settings	11
Configuring a Server Certificate for the Product.....	12
Using a Digital Certificate	13
About Digital Certification.....	14
Obtaining and Importing a CA-signed Certificate	14
CSR Setup Settings	16
CSR Import Settings	16
Deleting a CA-signed Certificate	17
Updating a Self-signed Certificate.....	17
Using an LDAP Server.....	18
Configuring the LDAP Server and Selecting Search Settings	19
LDAP Basic Settings.....	20
LDAP Search Settings	21
Checking the LDAP Server Connection	22
LDAP Connection Report Messages	22
Configuring Protocols in Web Config.....	23
Protocol Settings.....	23
Using an Email Server	26
Configuring an Email Server	26
Email Server Settings	27

Checking the Email Server Connection	28
Email Server Connection Report Messages	28
Using EpsonNet Config Network Configuration Software	31
Installing EpsonNet Config	31
Configuring a Product IP Address Using EpsonNet Config	31
Using Epson Device Admin Configuration Software	33
Solving Problems	34
Solving Network Software Usage Problems	34
Cannot Access Web Config	34
The "Out of Date" Message Appears	35
"The name of the security certificate does not match" Message Appears	35
Model Name or IP Address Not Displayed in EpsonNet Config	35
Solving Network Security Problems	35
Pre-Shared Key was Forgotten	36
Communication was Working, but Stopped	36
Cannot Create the Secure IPP Printing Port	36
Solving Digital Certificate Problems	36
Digital Certificate Warning Messages	37
Cannot Import a Digital Certificate	38
Cannot Update a Certificate or Create a CSR	38
Deleted a CA-signed Certificate	39
Where to Get Help	39
Notices	40
Trademarks	40
Copyright Notice	40
Copyright Attribution	41

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
- Individual protocol control: enable and disable single services
- Remote configuration of scan and fax destinations: use an LDAP server to look up fax and email contacts
- User feature restriction: allow or deny access to printing, scanning, faxing, and copying on a per user basis
- Import and export printer 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 *Start Here* sheet and *User's Guide* for instructions.

[About Web Config](#)

[Accessing Web Config](#)

[Restricting Features Available for Users](#)

[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 *Start Here* sheet and *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

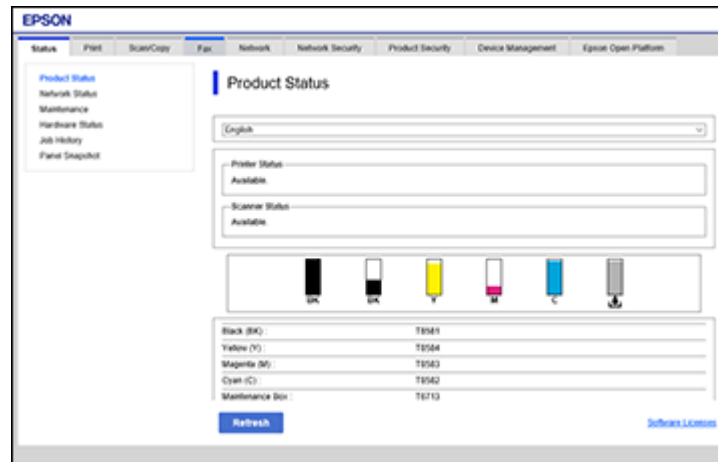
You can access Web Config from your browser using HTTP or HTTPS.

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. Print a network status sheet for your product and identify 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://\[product IP address\]/](http://[product IP address]/)

The Status 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](#)

Restricting Features Available for Users

Follow the instructions in these sections to restrict users from using certain product features and create an administrator password to lock the restrictions using the Web Config software.

[User Feature Restriction](#)

[Configuring User Feature Restrictions](#)

[Changing the Administrator Password in Web Config](#)

Parent topic: [Using Web Config Network Configuration Software](#)

User Feature Restriction

You can restrict available product features for up to 10 individual users, with different features available to each user. This requires users to log into the product control panel with their user name and password before they can use control panel features.

With Windows, you can also restrict printing and scanning from the product software. This requires users to log into the printing or scanning software, and allows the software to authenticate the users before printing or scanning proceeds. For instructions on setting up software restrictions, see the help utility in the printing or scanning software.

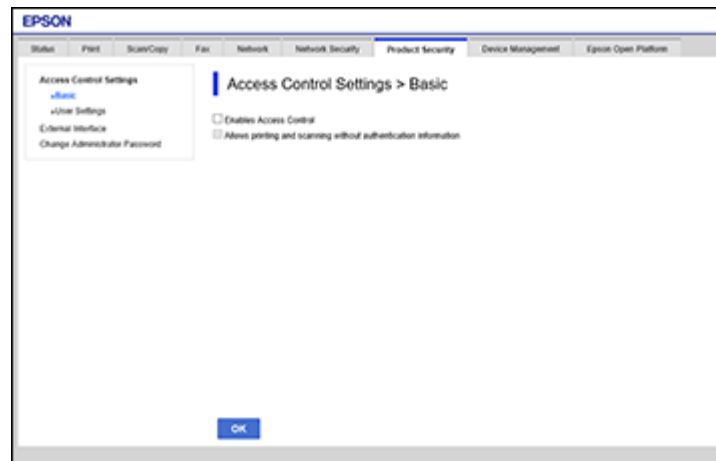
Parent topic: [Restricting Features Available for Users](#)

Configuring User Feature Restrictions

You can create up to 10 user accounts and restrict access to control panel features separately for each one.

1. Access Web Config and select the **Product Security** tab.

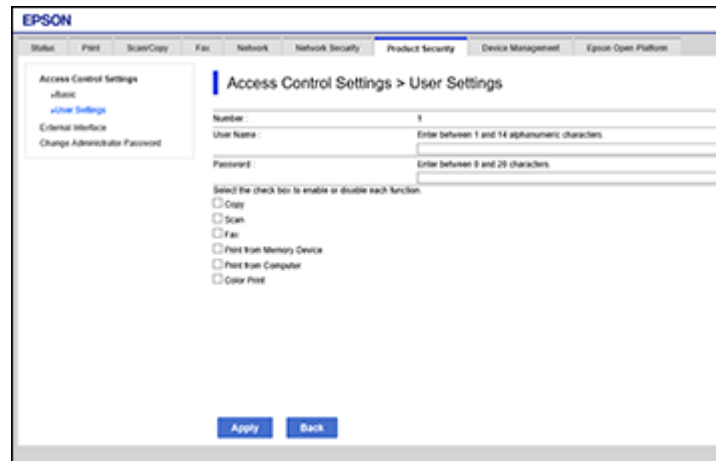
You see a window like this:



2. Select the **Enables Access Controls** checkbox.

3. If you have configured the product for an LDAP server, you can deselect the **Allows printing and scanning without authentication information** checkbox to prevent the product from receiving jobs sent from these sources:
 - The default operating system driver
 - A PCL or PostScript printer driver
 - Web services such as Epson Connect or Google Cloud Print
 - Smartphones and other mobile devices
4. Click **OK**.
5. Select **User Settings**.
6. Click **Add**.

You see a window like this:



The screenshot shows the EPSON Access Control Settings - User Settings window. The window has a navigation bar at the top with tabs for Status, PWT, Scan/Copy, Fax, Network, Network Security, Product Security, Device Management, and Epson Open Platform. The main content area is titled "Access Control Settings > User Settings". On the left, there is a sidebar with links for "Access Control Settings", "Basic", "User Settings", "External Interface", and "Change Administrator Password". The main area contains the following fields and options:

- Number:** A text field with the value "1".
- User Name:** A text field with the placeholder "Enter between 1 and 14 alphanumeric characters".
- Password:** A text field with the placeholder "Enter between 9 and 20 characters".
- Select the check box to enable or disable each function:**
 - Copy
 - Scan
 - Fax
 - Print from Memory Device
 - Print from Computer
 - Color Print

At the bottom of the window, there are two buttons: "Apply" and "Back".

7. Enter a name for a user in the User Name field following the guidelines on the screen. Use ASCII (0x20-0x7E) characters.
8. Enter a password for the user in the Password field following the guidelines on the screen.

Note: If you need to reset a password, leave the password field blank.
9. Select the checkbox for each function you want the user to be able to perform, and deselect the checkbox for each function you want to restrict access to.

10. Click **Apply**.

Note: When you edit a completed user account, you see a **Delete** option. Click it to delete a user, if necessary.

Note: You can import and export a list of user features using EpsonNet Config. See the help utility in the software for instructions.

Parent topic: [Restricting Features Available for Users](#)

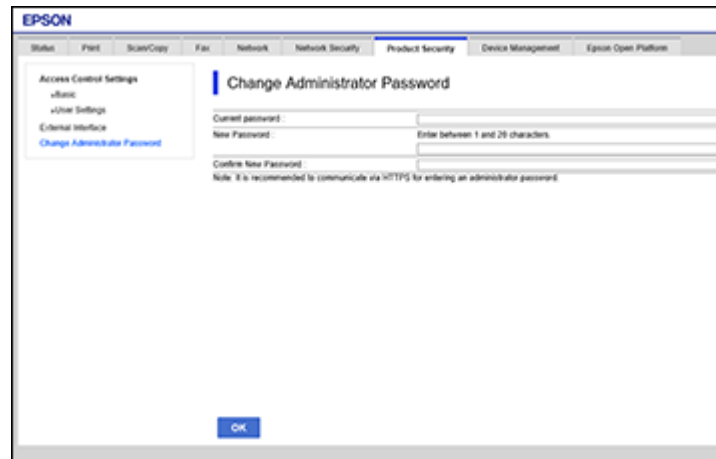
Changing the Administrator Password in Web Config

You can set an administrator password using your product's control panel, 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 and select the **Product Security** tab.
2. Select **Change Administrator Password**.

You see a window like this:



The screenshot shows the Epson Web Config interface. At the top, there is a navigation bar with tabs: Status, Print, Scan/Copy, Fax, Network, Network Security, Product Security (selected), Device Management, and Epson Open Platform. Below the navigation bar, there is a sidebar on the left with a tree view containing: Access Control Settings, Admin Settings, External Interface, and Change Administrator Password (selected). The main content area is titled 'Change Administrator Password' and contains three input fields: 'Current password', 'New Password', and 'Confirm New Password'. The 'New Password' field has a note: 'Enter between 1 and 20 characters'. Below the input fields, there is a note: 'Note: It is recommended to communicate via HTTPS for entering an administrator password.' At the bottom of the window, there is an 'OK' button.

3. Enter a user name, if necessary.
4. 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.
5. Click **OK**.

Parent topic: [Restricting Features Available for Users](#)

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 Communication](#)

[Using a Digital Certificate](#)

[Using an LDAP Server](#)

[Configuring Protocols in Web Config](#)

[Using an Email Server](#)

Parent topic: [Using Web Config Network Configuration Software](#)

Configuring SSL/TLS Communication

Follow the instructions in these sections to configure SSL/TLS communication using Web Config.

[Configuring SSL/TLS Settings](#)

[Configuring a Server Certificate for the Product](#)

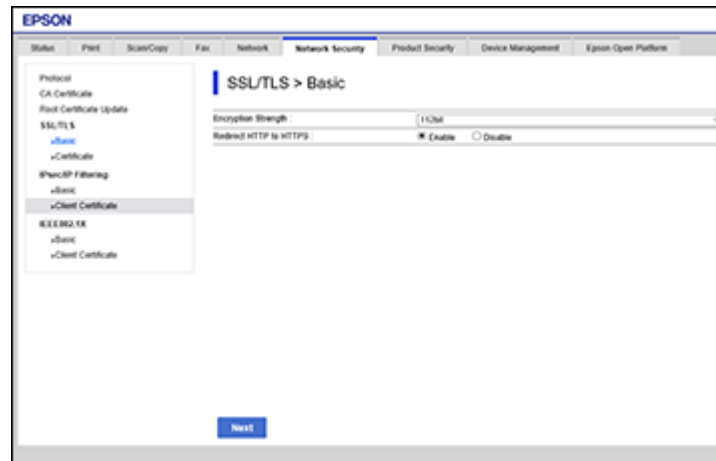
Parent topic: [Using Your Product on a Secure Network](#)

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 the **Network Security** tab.
2. Under **SSL/TLS**, select **Basic**.

You see a window like this:



3. Select one of the options for the **Encryption Strength** setting.
4. Select **Enable** or **Disable** as the **Redirect HTTP to HTTPS** setting as necessary.
5. Click **Next**.

You see a confirmation message.

6. Click **OK**.

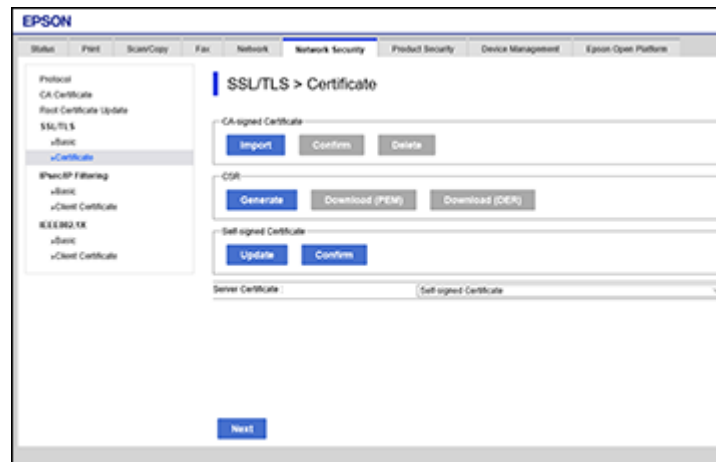
Parent topic: [Configuring SSL/TLS Communication](#)

Configuring a Server Certificate for the Product

You can configure a server certificate for your product.

1. Access Web Config and select the **Network Security** tab.
2. Under **SSL/TLS**, select **Certificate**.

You see a window like this:



3. Select one of the following options:
 - **CA-signed Certificate:** Select **Import** if you have obtained a CA-signed certificate. Choose the file to import and click **OK**.
 - **Self-signed Certificate:** Select **Update** if you have not obtained a CA (Certificate Authority)-signed certificate and want the product to generate a self-signed certificate.
4. Click **Next**.

You see a confirmation message.
5. Click **OK**.

Parent topic: [Configuring SSL/TLS Communication](#)

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

Parent topic: [Using Your Product on a Secure Network](#)

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).

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.

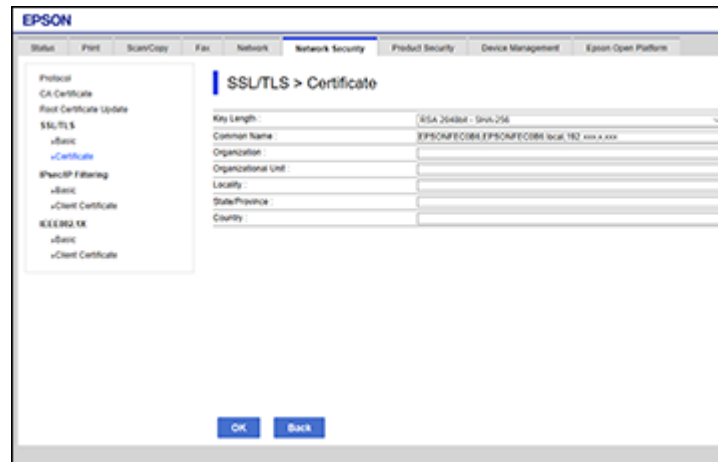
Parent topic: [Using a Digital Certificate](#)

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 the **Network Security** tab.
2. Under **SSL/TLS**, select **Certificate**.
3. In the CSR section, select **Generate**.

You see a window like this:

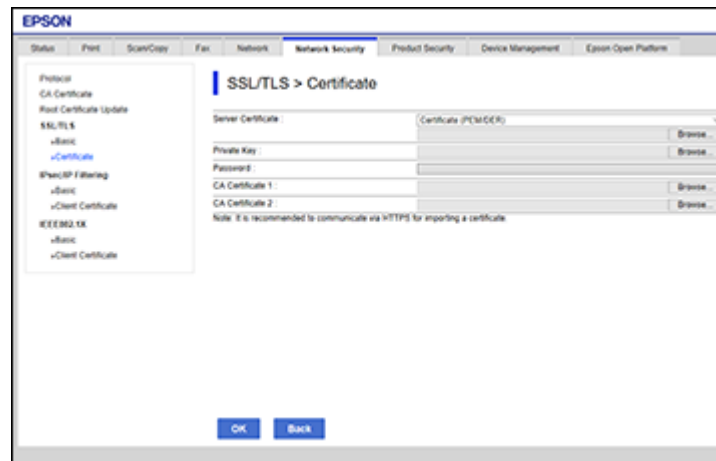


4. Select the CSR setting options you want to use.
5. Click **OK**.
You see a completion message.
6. Select the **Network Security** tab again.
7. Under **SSL/TLS**, select **Certificate** again.
8. In the CSR section, click the **Download** option that matches the format specified by your certificate authority to download the CSR.

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

9. Submit the CSR to the certificate authority following the format guidelines provided by that authority.
10. 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.
11. Select the **Network Security** tab again.
12. Under **SSL/TLS**, select **Certificate** again.
13. In the CA-signed Certificate section, click **Import**.

You see a window like this:



14. Select the format of the certificate as the **Server Certificate** setting.
15. Select the certificate import settings as necessary for the format and the source from which you obtained it.
16. Click **OK**.
You see a confirmation message.
17. 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: [Using a Digital Certificate](#)

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	<p>Private Key: Do not configure because the product contains a private key</p> <p>Password: Do not configure</p> <p>CA Certificate 1/CA Certificate 2: Optional</p>
PEM/DER format obtained from a computer	<p>Private Key: Configure a private key</p> <p>Password: Do not configure</p> <p>CA Certificate 1/CA Certificate 2: Optional</p>
PKCS#12 format obtained from a computer	<p>Private Key: Do not configure</p> <p>Password: Optional</p> <p>CA Certificate 1/CA Certificate 2: Do not configure</p>

Parent topic: [Using a Digital Certificate](#)

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 the **Network Security** tab.
2. Under **SSL/TLS**, select **Certificate**.
3. Click **Delete**.
You see a completion message.
4. Click **OK**.

Parent topic: [Using a Digital Certificate](#)

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 the **Network Security** tab.

2. Under **SSL/TLS**, select **Certificate**.
3. Click **Update**.

You see a window like this:

The screenshot shows the EPSON Web Config interface. The top navigation bar includes: Status, Print, Scan/Copy, Fax, Network, Network Security (selected), Product Security, Device Management, and Epson Open Platform. The left sidebar menu has: Protocol, CA Certificate, Root Certificate Update, SSL/TLS (selected), and IPsec/IP Filtering. The main content area is titled "SSL/TLS > Certificate" and contains the following configuration fields:

Key Length:	RSA 2048bit - SHA-256
Common Name:	EPSON/E0661.EPSON/E0661 local 192.168.1.100
Organization:	SEKIO EPSON CORP.
Valid Date (UTC):	2017-05-05 10:24 UTC
Certificate Validity (year):	10

At the bottom of the configuration area, there are two buttons: "Next" and "Back".

4. Enter an identifier for your product from 1 to 128 characters long in the **Common Name** field.
5. Select a validity period for the certificate as the **Certificate Validity (year)** setting.
6. Click **Next**.
You see a completion message.
7. Click **OK**.
8. Click **Confirm** to verify the certificate information.

Parent topic: [Using a Digital Certificate](#)

Using an LDAP Server

Follow the instructions in these sections to use an LDAP server to provide fax and email destination information using Web Config.

[Configuring the LDAP Server and Selecting Search Settings](#)

[LDAP Basic Settings](#)

[LDAP Search Settings](#)

[Checking the LDAP Server Connection](#)

LDAP Connection Report Messages

Parent topic: Using Your Product on a Secure Network

Configuring the LDAP Server and Selecting Search Settings

You can configure the LDAP server and select search settings for it using Web Config.

1. Access Web Config and select the **Network** tab.
2. Under **LDAP Server**, select **Basic**.

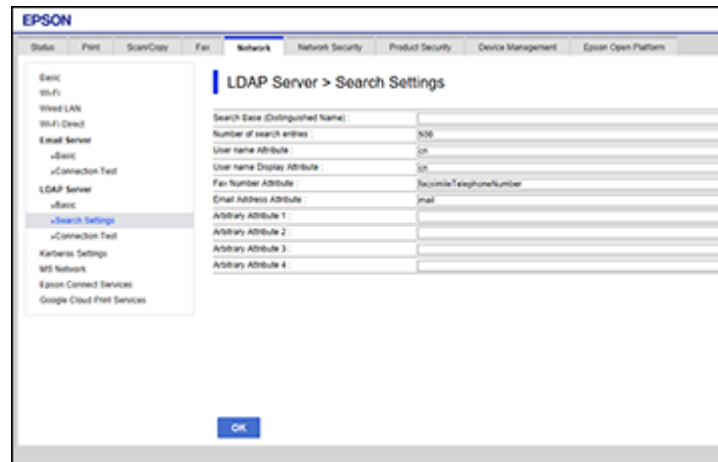
You see a window like this:



The screenshot shows the EPSON Web Config interface. The top navigation bar includes tabs for Status, Print, Scan/Copy, Fax, Network, Network Security, Product Security, Device Management, and Epson Open Platform. The left sidebar lists various configuration categories, with 'LDAP Server' selected. The main content area is titled 'LDAP Server > Basic'. It contains a warning message: 'The certificate is required to use a secure function of the LDAP server. Make settings on the following page.' Below this, there are several configuration fields: 'Use LDAP Server' (radio buttons for 'Use' and 'Do Not Use'), 'LDAP Server Address', 'LDAP server Port Number', 'Secure Connection' (dropdown menu set to 'None'), 'Certificate Validation' (radio buttons for 'Enable' and 'Disable'), 'Search Timeout (sec)', 'Authentication Method' (dropdown menu set to 'Anonymous Authentication'), 'Kerberos Realm to be Used' (dropdown menu set to 'Null Set'), 'User Name', and 'Password'. At the bottom, there is an 'OK' button.

3. Select **Use** as the **Use LDAP Server** setting.
4. Select the LDAP server settings.
5. Click **OK**.
6. Select the **Network** tab.
7. Under **LDAP Server**, select **Search Settings**.

You see a window like this:



8. Select the LDAP search settings you want to use.
9. Click **OK**.

Parent topic: [Using an LDAP Server](#)

LDAP Basic Settings

You can configure these LDAP basic settings in Web Config.

Setting	Options/Description
LDAP Server Address	Enter the address of the LDAP server as necessary, depending on the format of the server: <ul style="list-style-type: none"> • IPv4 or IPv6 format: Enter from 1 to 255 characters • FQDN format: Enter from 1 to 255 alphanumeric characters in ASCII; you can use "-", except at the beginning or end of the address
LDAP server Port Number	Enter an LDAP server port number between 1 and 65535
Search Timeout (sec)	Enter a search time interval before timeout from between 5 and 300 seconds
Authentication Method	Select one of the available authentication methods listed

Setting	Options/Description
Kerberos Realm to be Used	If you selected Kerberos Authentication as the Authentication Method option, select the correct realm of Kerberos authentication
User Name	Leave this blank or enter a user name for the LDAP server from 0 to 128 characters long in Unicode (UTF-8); do not use control characters such as 0x00-0x1F or OX7F (not available when you selected Anonymous Authentication as the Authentication Method option)
Password	Leave this blank or enter a password from 1 to 128 characters long in Unicode (UTF-8) for LDAP server authentication; do not use control characters such as 0x00-0x1F or OX7F (not available when you selected Anonymous Authentication as the Authentication Method option)

Parent topic: [Using an LDAP Server](#)

LDAP Search Settings

You can configure these LDAP search settings in Web Config.

Setting	Options/Description
Search Base (Distinguished Name)	Leave blank or search for an arbitrary domain name on the LDAP server using 1 to 128 characters Unicode (UTF-8)
Number of search entries	Specify the maximum number of search entries before an error message appears, from 1 to 500
User name Attribute	Enter the attribute name to display when searching for users names from 1 to 255 characters long in Unicode (UTF-8); the first character must be a-z, or A-Z
User name Display Attribute	Leave blank or enter the attribute name to display as the user name from 1 to 255 characters long in Unicode (UTF-8); the first character must be a-z, or A-Z
Fax Number Attribute	Enter the attribute name to display when searching for fax numbers from 1 to 255 characters long using A-Z, a-z, 0-9, and "-" in Unicode (UTF-8); the first character must be a-z, or A-Z

Setting	Options/Description
Email Address Attribute	Leave blank or enter the attribute name to display when searching for email addresses from 1 to 255 characters long in Unicode (UTF-8); the first character must be a-z, or A-Z
Arbitrary Attribute 1 through Arbitrary Attribute 4	Leave blank or specify other arbitrary attributes to search for from 1 to 255 characters long in Unicode (UTF-8); the first character must be a-z, or A-Z

Parent topic: [Using an LDAP Server](#)

Checking the LDAP Server Connection

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

1. Access Web Config and select the **Network** tab.
2. Under **LDAP Server**, select **Connection Test**.
3. Click **Start**.

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

Parent topic: [Using an LDAP Server](#)

LDAP Connection Report Messages

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

Message	Description
Connection test was successful.	Connection to the server is successful
Connection test failed. Check the settings.	One of the following occurred: <ul style="list-style-type: none"> • The LDAP server address or port number is incorrect • A timeout occurred • You selected Do Not Use as the Use LDAP Server setting • If you selected Kerberos Authentication as the Authentication Method setting, the Kerberos server settings are incorrect
Connection test failed. Check the date and time on your printer or server.	Connection failed because the time settings for the product and the LDAP server do not match

Message	Description
Authentication failed. Check the settings.	Authentication failed because the User Name and Password settings are incorrect or, if you selected Kerberos Authentication as the Authentication Method setting, the time and date are not configured correctly
Cannot access the printer until processing is complete.	The product is busy

Parent topic: [Using an LDAP Server](#)

Configuring Protocols in Web Config

You can enable or disable protocols using Web Config.

1. Access Web Config and select the **Network Security** tab.
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**.

After the protocols restart, the changes are applied.

[Protocol Settings](#)

Parent topic: [Using Your Product on a Secure Network](#)

Protocol Settings

Protocols

Name	Description
Bonjour	Bonjour is used to search for devices and AirPrint
SLP	SLP is used 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

Name	Description
LPR	Print from to the LPR port
RAW(Port9100)	Print from the RAW port (Port 9100)
IPP	Print over the Internet, including AirPrint

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
Top Priority Protocol	Selects the protocol that is the top priority for Bonjour printing

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
Printing Timeout (sec)	Enter the communication timeout value for WSD printing between 3 and 3,600 seconds
Scanning Timeout (sec)	Enter the communication timeout value for WSD scanning between 3 and 3,600 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

LPR Settings

Setting	Options/Description
Allow LPR Port Printing	Allow printing from the LPR port
Printing Timeout (sec)	Enter the timeout value for LPR printing between 0 and 3,600 seconds

RAW (Port9100) Settings

Setting	Options/Description
Allow RAW (Port9100) Printing	Allow printing from the RAW port (Port 9100)
Printing Timeout (sec)	Enter the timeout value for RAW (Port 9100) printing between 0 and 3,600 seconds

IPP Settings

Setting	Options/Description
Enable IPP	Enable IPP communication for products that support IPP are displayed (you cannot use AirPrint if disabled)
Allow Non-secure Communication	Allow the printer to communicate without any security measures (IPP)

Setting	Options/Description
Communication Timeout (sec)	Enter the timeout value for IPP printing between 0 and 3,600 seconds
URL(Network)	Displays IPP URLs (http and https) when the product is connected using wired LAN or Wi-Fi (the URL is a combined value of the product's IP address, Port number, and IPP printer name)
URL(Wi-Fi Direct)	Displays IPP URLs (http and https) when the product is connected using Wi-Fi Direct (the URL is a combined value of the product's IP address, Port number, and IPP printer name)
Printer Name	Displays the IPP printer name
Location	Displays the IPP location

Parent topic: [Configuring Protocols in Web Config](#)

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](#)

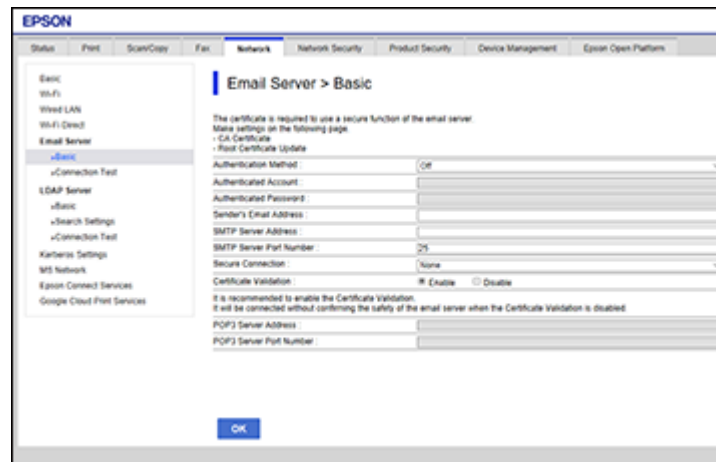
Parent topic: [Using Your Product on a Secure Network](#)

Configuring an Email Server

You can configure an email server using Web Config.

1. Access Web Config and select the **Network** tab.
2. Under **Email Server**, select **Basic**.

You see a window like this:



3. Select the email server settings.
4. Click **OK**.

Parent topic: [Using an Email Server](#)

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 the **Network** tab.
2. Under **Email Server**, 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 printer until processing is complete.	The product is busy

Parent topic: [Using an Email Server](#)

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 *Start Here* sheet and *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  > **All Apps** > **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**.

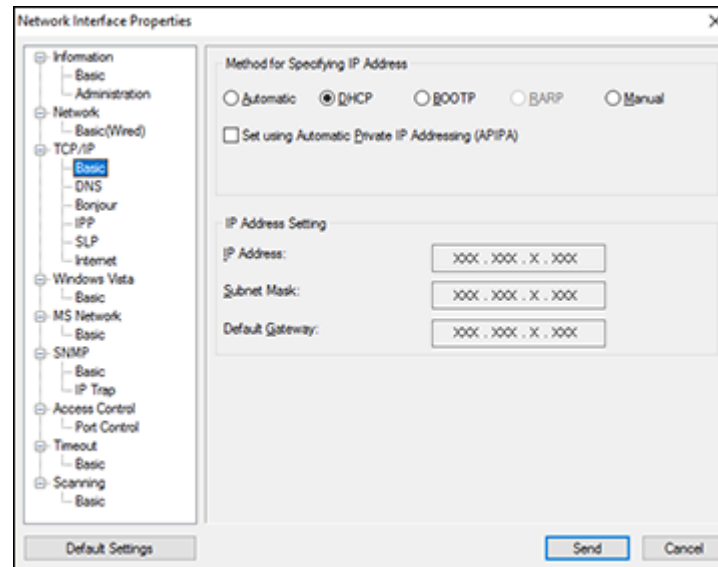
After a few moments, the program displays the connected products.

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, under **TCP/IP**, 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 **Send**.

Enter the current administrator password if necessary, and click **OK**.

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](https://www.epson.com/support) (U.S.), [epson.ca/support](https://www.epson.ca/support) (Canada), or [epson.com.jm/support](https://www.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 or print a network status sheet. 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  > **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  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](#)
[Communication was Working, but Stopped](#)
[Cannot Create the Secure IPP Printing Port](#)

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](#)

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:

- 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 Create the Secure IPP Printing Port

If you cannot create the secure IPP printing port, try these solutions:

- Make sure you specified the correct server certificate for SSL/TLS communication using Web Config.
- If you are using a CA certificate, make sure it is imported to the computer that is accessing the product.

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: <ul style="list-style-type: none"> • 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.	<p>Do one of the following to pair a private key with the certificate:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Setup failed.	<p>Make sure the computer and product are connected, and the certificate file is not corrupted, then import the certificate file again.</p>

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.

Google Cloud Print™ is a trademark of Google Inc.

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.



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

© 2017 Epson America, Inc.

11/17

CPD-55000

Parent topic: [Copyright Notice](#)