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
- 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, you must connect the product to a network. See the product's *User's Guide* for instructions.

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, you must 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

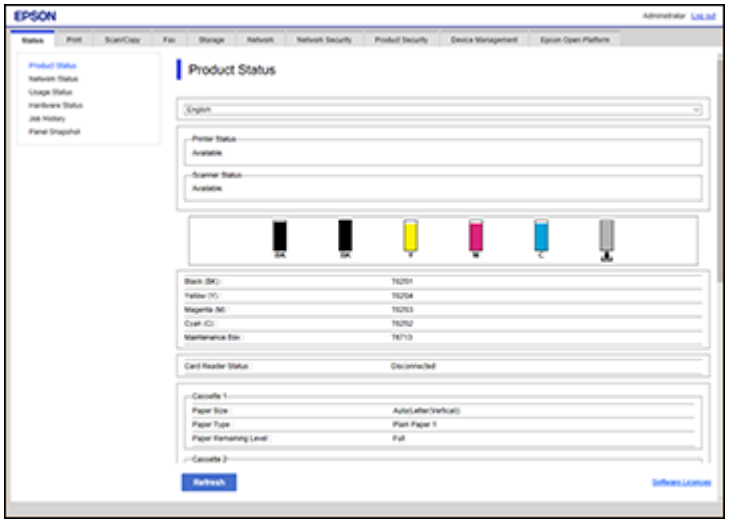
You can access Web Config from your browser using HTTP or HTTPS.

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. 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*]/

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.

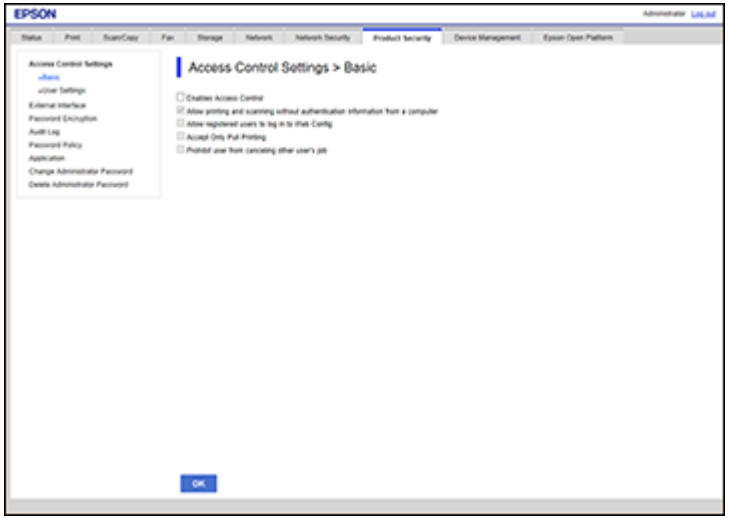
Parent topic: Restricting Features Available for Users

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.

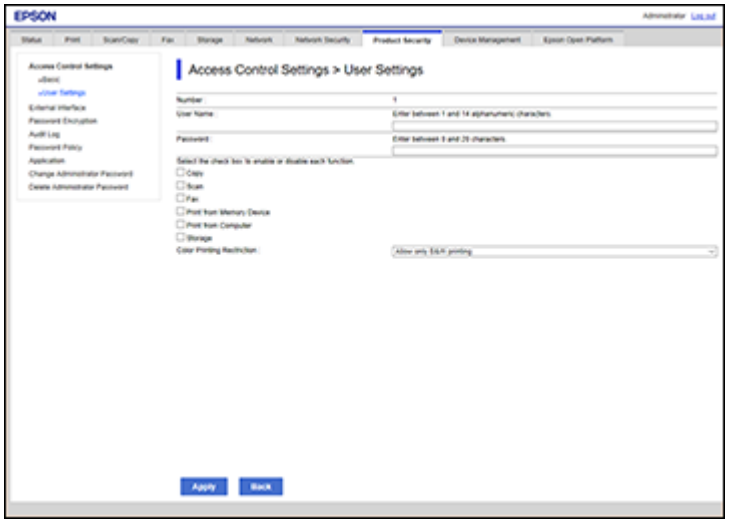
   You see a window like this:



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

3. If you have configured the product for an LDAP server or IEEE 802.1x network, you can deselect the **Allows printing and scanning without authentication information from a computer** 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
   - Smartphones and other mobile devices
4. Click **OK**.
5. Select **User Settings**.
6. Click **Add**.

   You see a window like this:



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

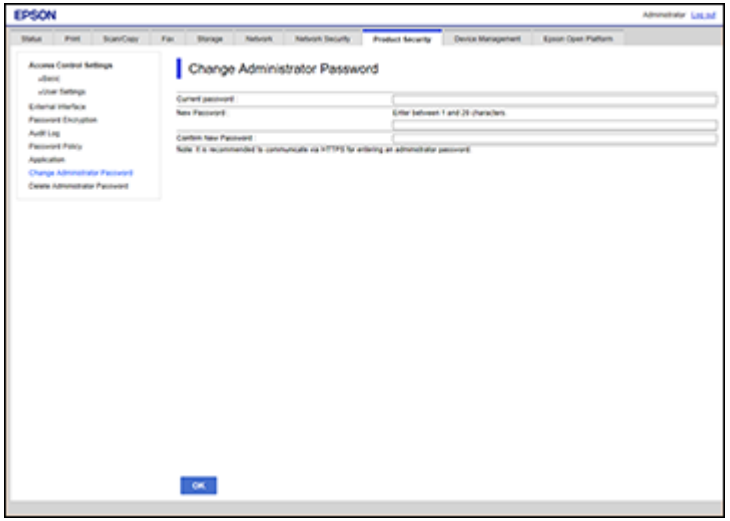
Changing the Administrator Password in Web Config

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:



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
Configuring IPsec/IP Filtering
Configuring SNMPv3 Protocol Settings
Configuring S/MIME Settings

Connecting the Product to an IEEE 802.1X Network
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

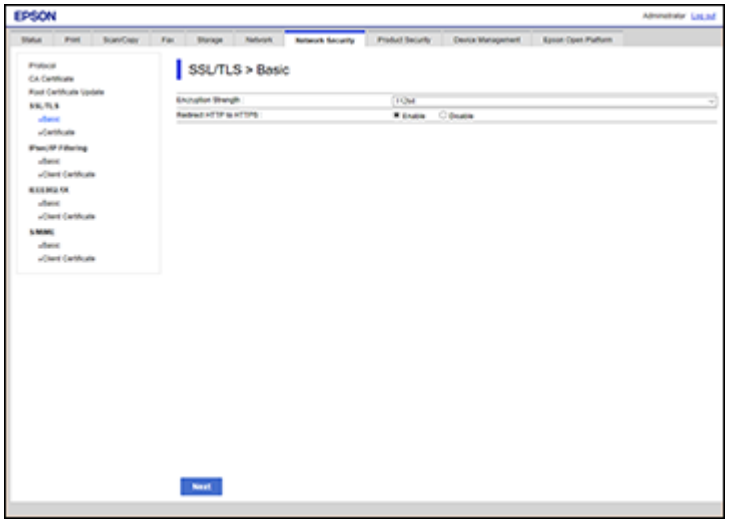
Parent topic: Using Your Product on a Secure Network

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**.

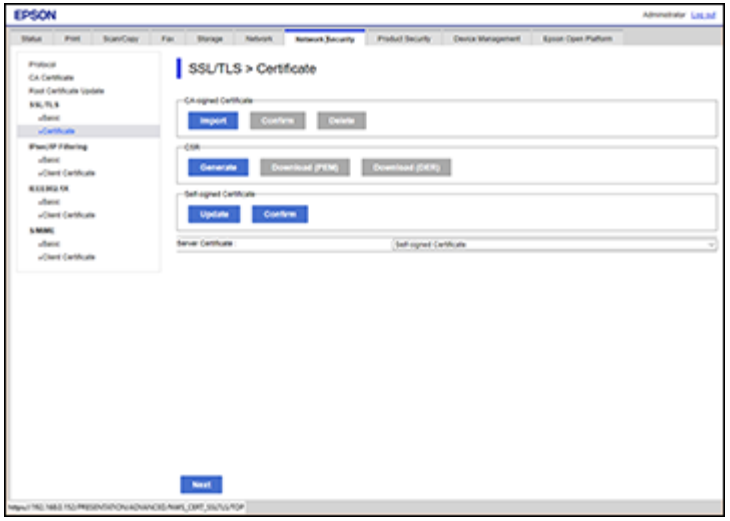
Parent topic: Configuring SSL/TLS Communication

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

Configuring IPsec/IP Filtering

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

About IPsec/IP Filtering
Configuring Default IPsec/IP Filtering Policy
Configuring Group IPsec/IP Filtering Policies
IPsec/IP Filtering Policy Settings
IPsec/IP Filtering Configuration Examples
Configuring an IPsec/IP Filtering Certificate

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.

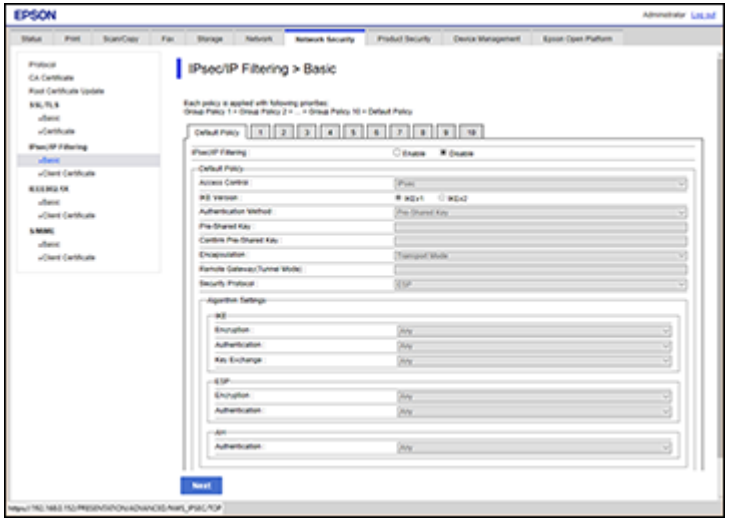
Parent topic: Configuring IPsec/IP Filtering

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 the **Network Security** tab.
2. Under **IPsec/IP Filtering**, 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**.

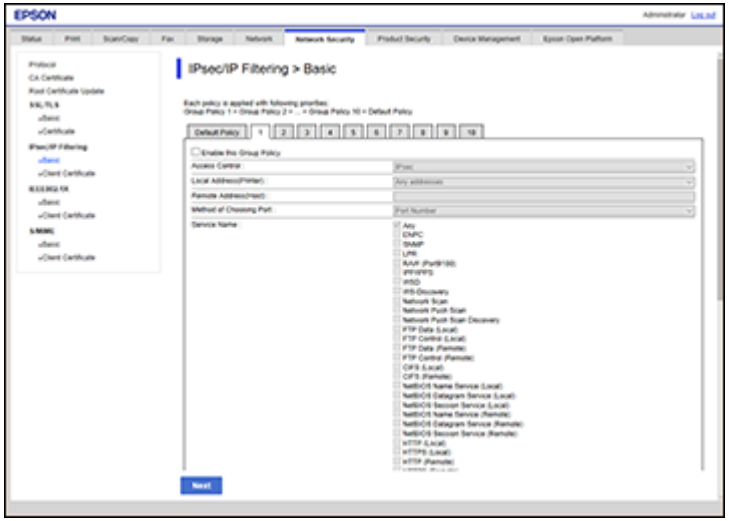
Parent topic: Configuring IPsec/IP Filtering

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 the **Network Security** tab.
2. Under **IPsec/IP Filtering**, 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	**Permit Access** to permit IP packets to pass through **Refuse Access** to prevent IP packets from passing through **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
ID Type	If you selected **IKEv2** as the **IKE Version** setting, select the ID type from the list.
ID	If you selected **IKEv2** as the **IKE Version** setting, enter the necessary ID information
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

Setting	Options/Description
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 Settings

Setting	Options/Description
Access Control	**Permit Access** to permit IP packets to pass through **Refuse Access** to prevent IP packets from passing through **IPsec** to permit IPsec packets to pass through
Local Address(Printer)	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 specifying 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 Group Policy Guidelines 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
ID Type	If you selected **IKEv2** as the **IKE Version** setting, select the ID type from the list
ID	If you selected **IKEv2** as the **IKE Version** setting, enter the necessary ID information

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	Controls these operations
Any	—	—	All services
ENPC	UDP	3289/Any port	Searching for a product from applications such as printer or scanner drivers, or EpsonNet Config
SNMP	UDP	161/Any port	Acquiring and configuring MIB from applications such as printer or scanner drivers, or EpsonNet Config
LPR	TCP	515/Any port	Forwarding LPR data
RAW (Port9100)	TCP	9100/any port	Forwarding RAW data

Service name	Protocol type	Local/Remote port number	Controls these operations
IPP/IPPS	TCP	631/Any port	Forwarding AirPrint data (IPP/IPPS printing)
WSD	TCP	Any port/5357	Controlling WSD
WS-Discovery	UDP	3702/Any port	Searching for a product from WSD
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
FTP Data (Local)	TCP	20/Any port	Forwarding FTP printing data to FTP server
FTP Control (Local)	TCP	21/Any port	Controlling FTP printing to FTP server
FTP Data (Remote)	TCP	Any port/20	Forwarding scan data and received fax data to FTP client; controls only an FTP server that uses remote port 20
FTP Control (Remote)	TCP	Any port/21	Forwarding scan data and received fax data to FTP client
CIFS (Local)*	TCP	445/Any port	Sharing a network folder on CIFS server
CIFS (Remote)*	TCP	Any port/445	Forwarding scan data and received fax data to a folder on CIFS server

Service name	Protocol type	Local/Remote port number	Controls these operations
NetBIOS Name Service (Local)	UDP	137/Any port	Sharing a network folder on CIFS server
NetBIOS Datagram Service (Local)	UDP	138/Any port	
NetBIOS Session Service (Local)	TCP	139/Any port	
NetBIOS Name Service (Remote)	UDP	Any port/137	Forwarding scan data and received fax data to a folder on CIFS server
NetBIOS Datagram (Remote)	UDP	Any port/138	
NetBIOS Session Service (Remote)	TCP	Any port/139	
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 Epson Connect, firmware update, and root certificate update on a HTTP or HTTPS client
HTTPS (Remote)	TCP	Any port/443	

* To control forwarding of scan and received fax data, share a network folder, or receive fax data from PC-Fax, select **Port Number** as the **Method of Choosing Port** option and specify the port numbers for CIFS and NetBIOS.

Parent topic: Configuring IPsec/IP Filtering

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

Receiving Printing Data and Printer Settings

Use this example to allow communication of printing data and printer settings from specified services.

Default policy:

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

Group policy:

- **Access Control**: **Permit Access**
- **Remote Address(Host)**: Client IP address
- **Method of Choosing Port**: **Service Name**
- **Service Name**: Select **ENPC**, **SNMP**, **HTTP (Local)**, **HTTPS (Local)**, and **RAW (Port9100)**

Receiving Access from Only a Specified Address for Product Access

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:

- **Access Control**: **Permit Access**
- **Remote Address (Host)**: Administrator's client IP address

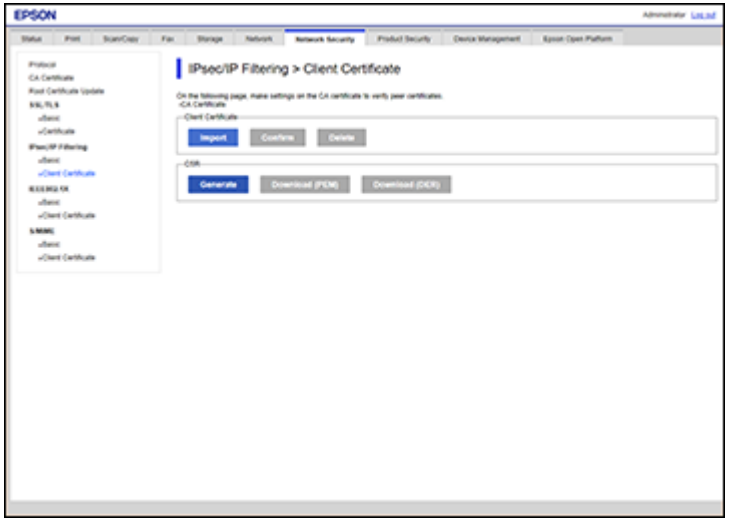
Parent topic: Configuring IPsec/IP Filtering

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 the **Network Security** tab.
2. Under **IPsec/IP Filtering**, select **Client Certificate**.

You see a window like this:



3. Click **Import** to add a new client certificate and enter any necessary settings.
4. Click **OK**.

Parent topic: Configuring IPsec/IP Filtering

Related tasks

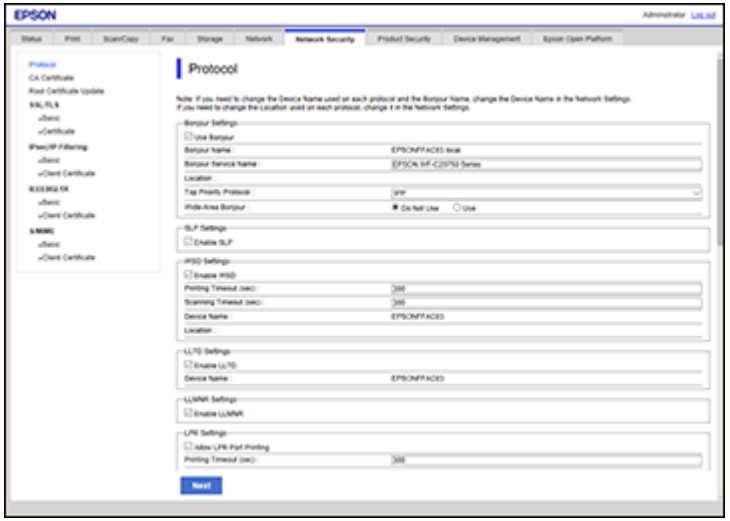
Obtaining and Importing a CA-signed Certificate

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 the **Network Security** tab.

You see a window like this:



2. Scroll down and select the **Enable SNMPv3** checkbox to enable SNMPv3 settings.
3. Select the settings you want in SNMPv3 Settings section.
4. Click **Next**.

   You see a confirmation message.
5. 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

Configuring S/MIME Settings

Follow the instructions in these sections to configure S/MIME settings using Web Config.

Configuring S/MIME Basic Settings
S/MIME Settings
Configuring a Certificate for S/MIME
Importing the Encryption Certificate to an Email Destination

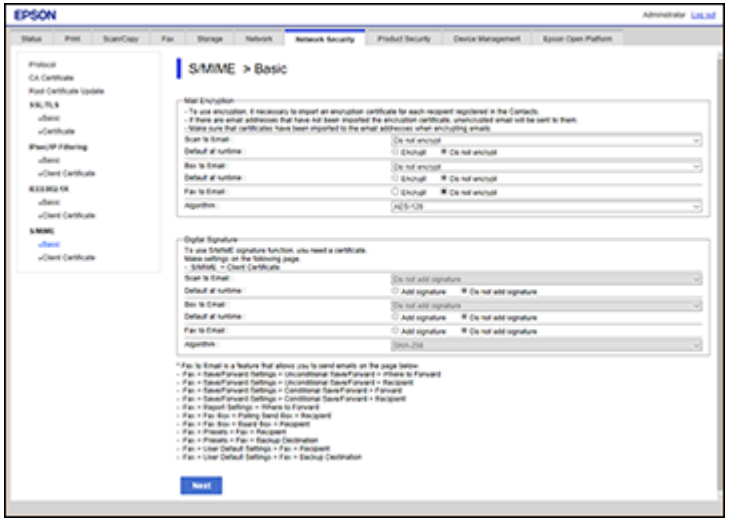
Parent topic: Using Your Product on a Secure Network

Configuring S/MIME Basic Settings

You can configure the email encryption and digital signature attachment to emails as necessary.

1. Access Web Config and select the **Network Security** tab.
2. Under **S/MIME**, select **Basic**.

You see a window like this:



3. Select a setting for each option.
4. Click **Next**.

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

Parent topic: Configuring S/MIME Settings

S/MIME Settings

Mail Encryption

You need to import an encryption certificate for each destination registered in the contacts list. Unencrypted emails are sent to destinations that do not have an imported encryption certificate.

Setting	Options/Description
Scan to Email	Select settings for scanning to email **Encrypt**: to configure email encryption **Do not encrypt**: scan to an email destination without encryption **Select at runtime**: decide whether or not to encrypt the email before you send it **Default at runtime**: select the default action when **Select at runtime** is selected
Box to Email	Select settings for uploading files to email **Encrypt**: configure email encryption **Do not encrypt**: upload a file to an email destination without encryption **Select at runtime**: decide whether or not to encrypt the email before you send it **Default at runtime**: select the default action when **Select at runtime** is selected
Fax to Email	Configure email encryption when sending a fax to email
Algorithm	Select the algorithm for email encryption

Digital Signature

You need to configure the client certificate to include a digital signature.

Setting	Options/Description
Scan to Email	Select settings for scanning to email **Add signature**: add a digital signature to emails **Do not add signature**: scan to an email destination without a digital signature **Select at runtime**: decide whether or not to add a digital signature to the email before you send it **Default at runtime**: select the default action when **Select at runtime** is selected
Box to Email	Select settings for uploading files to email **Add signature**: add a digital signature to emails **Do not add signature**: upload a file to an email destination without a digital signature **Select at runtime**: decide whether or not to add a digital signature to the email before you send it **Default at runtime**: select the default action when **Select at runtime** is selected
Fax to Email	Configure the digital signature when sending a fax to email
Algorithm	Select the algorithm for the digital signature

Parent topic: Configuring S/MIME Settings

Related tasks

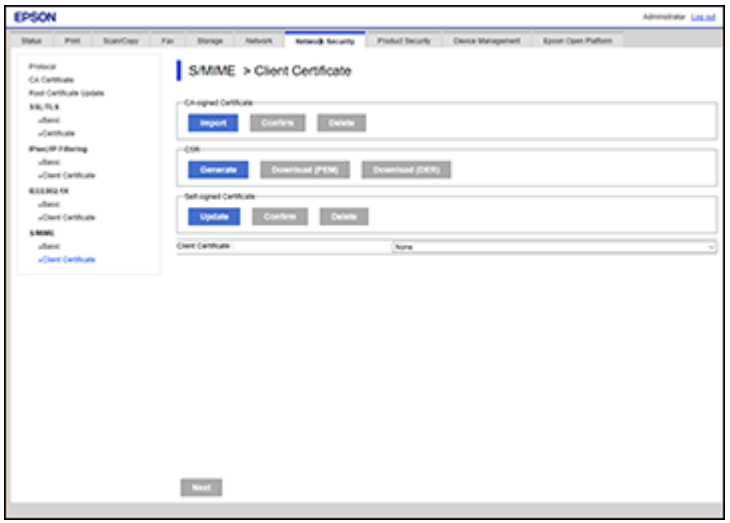
Importing the Encryption Certificate to an Email Destination
Configuring a Certificate for S/MIME

Configuring a Certificate for S/MIME

You can configure a client certificate to use the S/MIME signature feature.

1. Access Web Config and select the **Network Security** tab.
2. Under **S/MIME**, select **Client 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**.

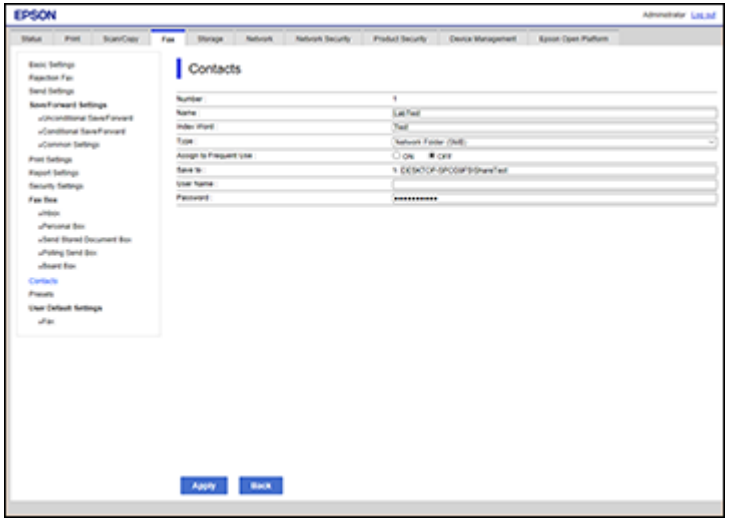
Parent topic: Configuring S/MIME Settings

Importing the Encryption Certificate to an Email Destination

You need to import an encryption certificate for each email destination registered in the contacts list.

1. Access Web Config and select the **Scan/Copy** or **Fax** tab.
2. Select **Contacts**.
3. Select the destination number you want to import the encryption certificate to, and click **Edit**.

You see a window like this:



4. Select **Email** as the **Type** setting.
5. Click **Browse** to select the encryption certificate you want to use.
6. Select any other settings as necessary.
7. Click **Apply** when you are finished.

   A key icon is displayed next to the destination on the contacts list.

Parent topic: Configuring S/MIME Settings

Related references

S/MIME 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
IEEE 802.1X Network Status

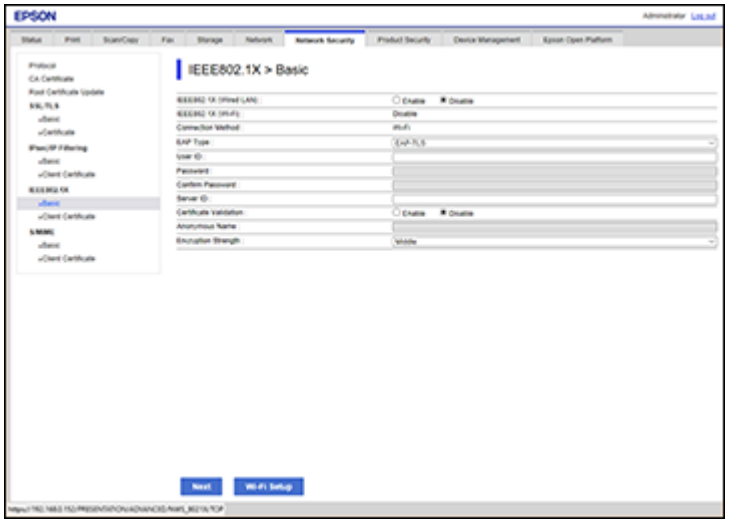
Parent topic: Using Your Product on a Secure Network

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 the **Network Security** tab.
2. Under **IEEE802.1X**, select **Basic**.

   You see a window like this:



3. Select **Enable** as the **IEEE802.1X (Wired LAN)** setting.
4. To use the product on a Wi-Fi network, enable your product's Wi-Fi settings. See your product's *User's Guide* for instructions.

   The status of the connection is shown as the **IEEE802.1X (Wi-Fi)** setting.

   Note: You can share the network settings for Ethernet and Wi-Fi networking.

5. Select the IEEE 802.1X setting options you want to use.
6. Click **Next**.

   You see a confirmation message.

7. Click **OK**.

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

Related references

IEEE 802.1X Network Settings

IEEE 802.1X Network Settings

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

Setting	Options/Description
Connection Method	Displays the current network connection method
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** or **EAP-TTLS**: You must configure a password
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 Certificate** option
Anonymous Name	If you selected **EAP-TTLS**, **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

Setting	Options/Description
Encryption Strength	Select one of the following encryption strengths: **High** for AES256/3DES **Middle** for AES256/3DES/AES128/RC4

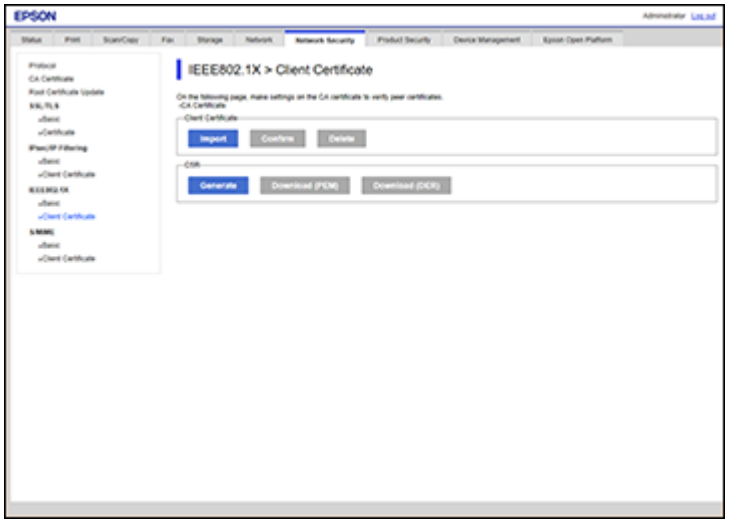
Parent topic: Connecting the Product to an IEEE 802.1X Network

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 the **Network Security** tab.
2. Under **IEEE802.1X**, select **Client Certificate**.

   You see a window like this:



3. Click **Import** to add a new client certificate.
4. Click **OK**.

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

IEEE 802.1X Network Status

You can check the status of the IEEE 802.1X network settings by printing a status sheet from your product. See the product's *User's Guide* for instructions on printing a network status sheet.

The network status sheet displays the information in this table for IEEE 802.1X networks.

Status ID	Status description
Disable	IEEE 802.1X is disabled
EAP Success	IEEE 802.1X authentication is confirmed and the network connection is available
Authenticating	IEEE 802.1X authentication in progress
Config Error	Authentication failed because the user ID was not set
Client Certificate Error	Authentication failed because the client certificate is out of date
Timeout Error	Authentication failed because there is no answer from the RADIUS server and/or authenticator
User ID Error	Authentication failed because the product's user ID and/or certificate protocol is incorrect
Server ID Error	Authentication failed because the server ID on the server certificate and the server's ID do not match
Server Certificate Error	Authentication failed because the server certificate is out of date or the chain of the server certificate is incorrect
CA Certificate Error	Authentication failed because the CA certificate is incorrect, not imported, or out of date
EAP Failure	Authentication failed because the client certificate is incorrect (EAP-TLS or PEAP-TLS), or the user ID or password is incorrect (PEAP/MSCHAPv2 or EAP-TTLS)

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

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.

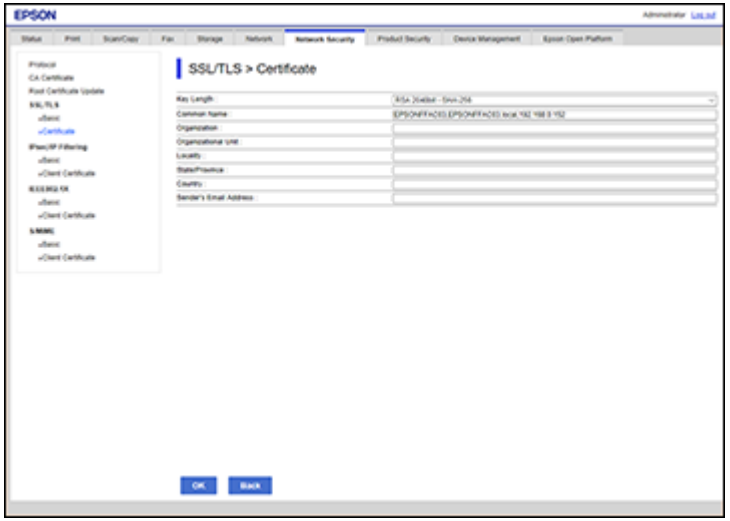
Parent topic: Using a Digital Certificate

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 one of the following network security options, select the corresponding certificate:
   - **SSL/TLS** and **Certificate**
   - **IPsec/IP Filtering** and **Client Certificate**
   - **IEEE802.1X** and **Client Certificate**
3. In the CSR section, select **Generate**.

You see a window like this:



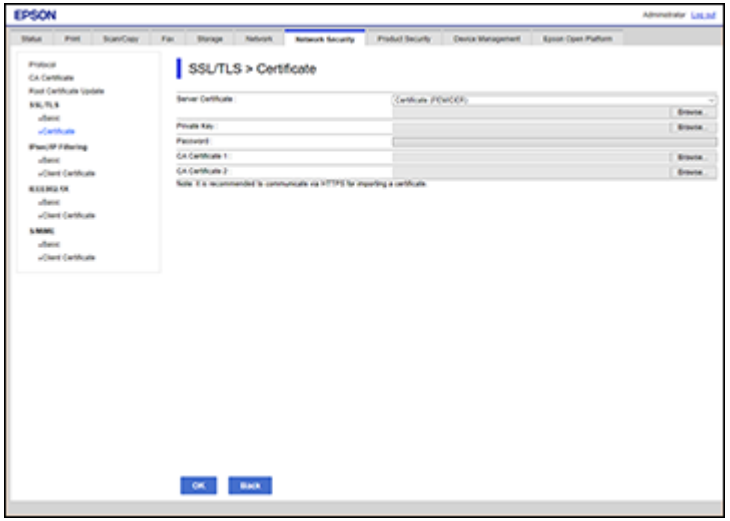
4. Select the CSR setting options you want to use.
5. Click **OK**.

   You see a completion message.
6. Select the **Network Security** tab again, and select your network security option and the corresponding 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 the **Network Security** tab again, and select your network security option and the corresponding certificate.
11. In the CA-signed 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

Related references

CSR Setup Settings

CSR Import Settings

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
Sender's Email Address	Enter the sender's email address for the mail server setting

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	**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: 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 one of the following network security options, select the corresponding certificate:
   - **SSL/TLS** and **Certificate**
   - **IPsec/IP Filtering** and **Client Certificate**
   - **IEEE802.1X** and **Client Certificate**
   - **S/MIME** and **Client Certificate**
3. Click **Delete**.

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

Parent topic: Using a Digital Certificate

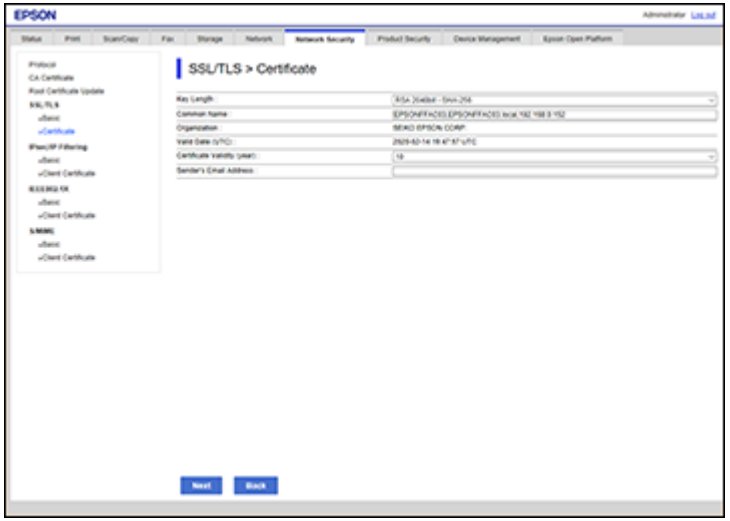
Updating a Self-signed Certificate

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 one of the following network security options, select the corresponding certificate:
   - **SSL/TLS** and **Certificate**
   - **S/MIME** and **Client Certificate**

     Note: When you update a self-signed certificate for S/MIME, you cannot change the sender's email address on the **Network** > **Email Server** > **Basic** tab. You must change all signature settings to **Do not add signature** on the **Network Security** > **S/MIME** > **Basic** tab, and then delete the self-signed certificate for S/MIME.
3. Under **Self-signed Certificate**, click **Update**.

You see a window like this:



4. Enter an identifier for your product from 1 to 128 characters long in the **Common Name** field.

   Note: You can add up to 5 IPv4 addresses, IPv6 addresses, host names, or FQDNs; separated by commas. The first value is assigned to the Common Name field, and the rest are added to the Alias field of the certificate subject. You cannot enter a space before or after a comma.

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 Server Settings
LDAP Search Settings
Checking the LDAP Server Connection
LDAP Connection Report Messages

Parent topic: Using Your Product on a Secure Network

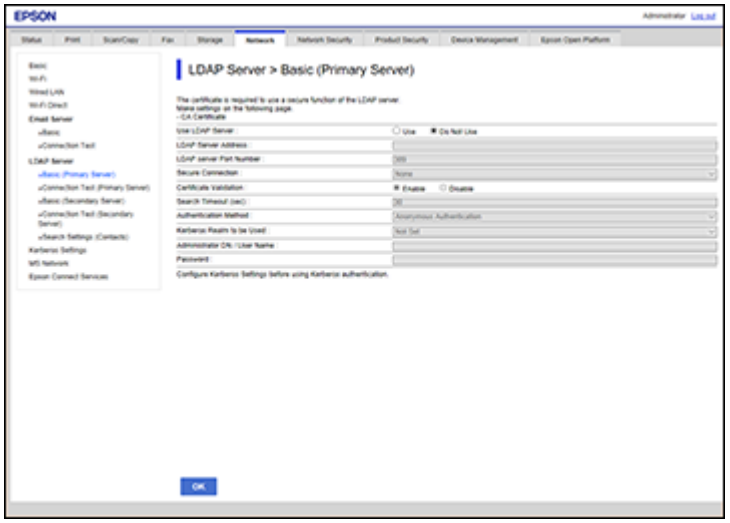
Configuring the LDAP Server and Selecting Search Settings

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**.

   Note: You can select the primary or secondary server as necessary.

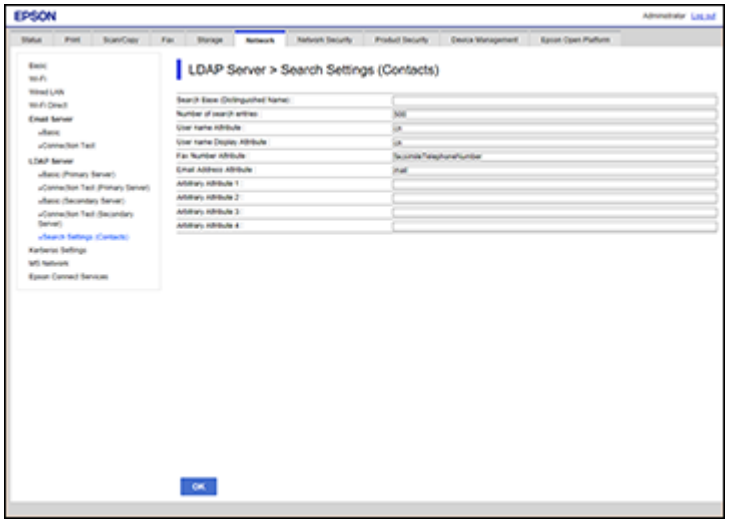
   You see a window like this:



3. Select **Use** as the **Use LDAP Server** setting.
4. Select the LDAP server settings.
5. Click **OK**.
6. Select the **Network** tab, if necessary.

7. Under **LDAP Server**, select **Search Settings (Contacts)**.

   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

Related references

LDAP Server Settings

LDAP Search Settings

LDAP Server Settings

You can configure these LDAP server 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: • 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
Secure Connection	Select the encryption method for connecting to the LDAP server
Certificate Validation	Select **Enable** to validate the certificate when connecting to the LDAP server
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
Kerberos Realm to be Used	If you selected **Kerberos Authentication** as the **Authentication Method** option, select the correct realm of Kerberos authentication from the realms defined under the **Kerberos Settings** menu entry.
Administrator DN/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)
Kerberos Settings	

Setting	Options/Description
Realm (Domain)	If you selected **Kerberos Authentication** as the **Authentication Method** option, enter the realm of Kerberos authentication from 0 to 255 characters long in ASCII; you can define up to 10 realms with associated addresses and port numbers
KDC Address	Leave this blank or, if you selected **Kerberos Authentication** as the **Authentication Method** option, enter the Kerberos server address from 0 to 255 characters long in IPv4, IPv6, or FQDN format
Port Number (Kerberos)	Leave this blank or, if you selected **Kerberos Authentication** as the **Authentication Method** option, enter the Kerberos server port number between 1 and 65535

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**.

   Note: You can select the primary or secondary server as necessary.

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: • 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

Message	Description
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
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

Name	Description
LLTD	Displays the product on the Windows network map
LLMNR	Use name resolution without NetBIOS even if you cannot use DNS
LPR	Print from to the LPR port
RAW(Port9100)	Print from the RAW port (Port 9100)
RAW(Custom Port)	Print from the RAW port (custom port)
IPP	Print over the Internet, including AirPrint
FTP	Print over FTP
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
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
Wide-Area Bonjour	Enables the Wide-Area Bonjour protocol; register all products on the DNS server to locate them over the segment

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 (Port 9100) printing between 0 and 3,600 seconds

RAW (Custom Port) Settings

Setting	Options/Description
Allow RAW (Custom Port) Printing	Allow printing from the RAW port (custom port)
Port Number	Enter the port number for RAW printing between 1024 and 65535 (except 9100, 1865, and 2968)
Printing Timeout (sec)	Enter the timeout value for RAW port (custom port) 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)
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

FTP Settings

Setting	Options/Description
Enable FTP Server	Enable FTP printing for products that support FTP printing
Communication Timeout (sec)	Enter the timeout value for FTP communication between 0 and 3,600 seconds

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 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.

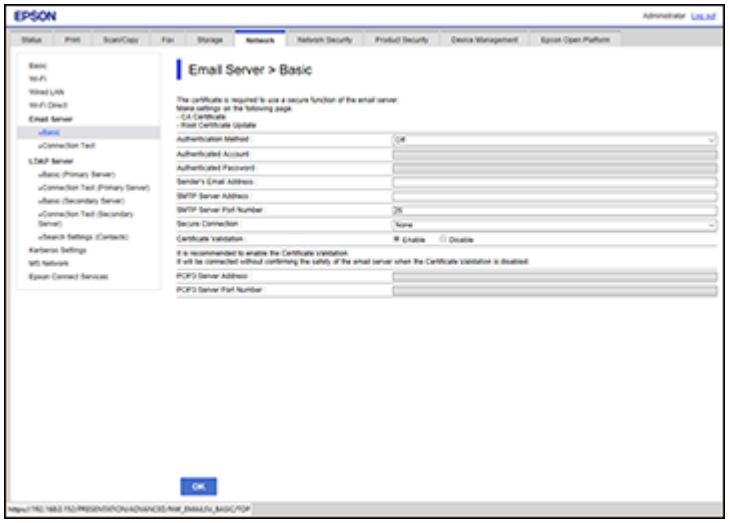
Parent topic: Using Your Product on a Secure Network

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

Related references

Email Server Settings

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: ( ) < > [ ] ;
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
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 a POP3 server failed
SMTP server authentication error. Check the following - Authentication Method - Authenticated Account - Authenticated Password	SMTP server authentication failed

Message	Description
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	The communication protocol is unsupported
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

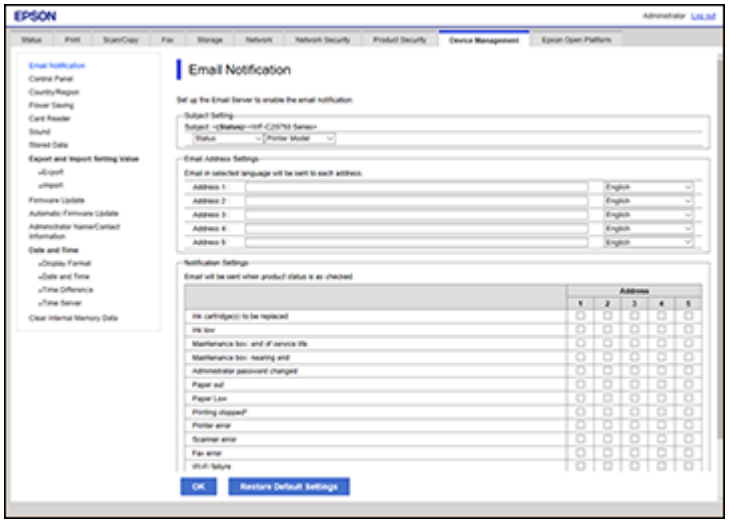
Parent topic: Using an Email Server

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, such as running out of paper. 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 the **Device Management** tab.

   You see a window like this:



2. Enter an email address in the **Address 1** field.
3. Select the language in which you want to receive the email notifications from the drop-down menu for the first email address.
4. Enter additional email addresses in each field as necessary, and select a language for each.
5. Select the checkboxes to indicate the events for which you want to receive email notifications.
6. Click **OK**.

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 *User's Guide* for instructions.

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**.

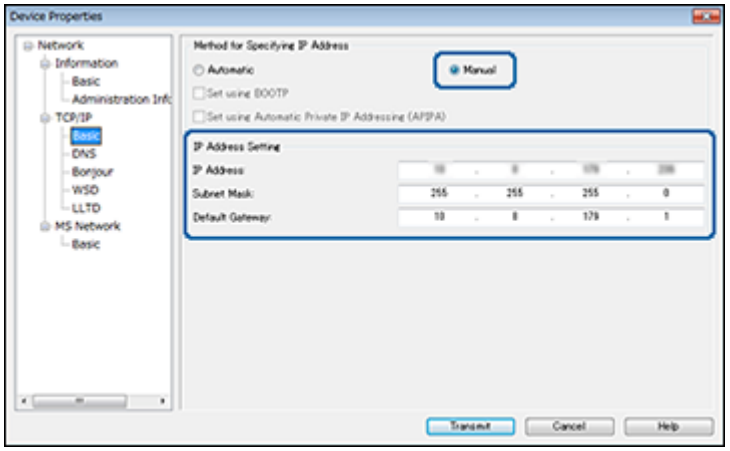
   After a few moments, the program displays the connected products.

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. Enter the current administrator password if necessary, and click **OK**.
6. From the menu on the left, under **TCP/IP**, select **Basic**.

   You see a window like this:



7. Select **Manual**.
8. 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.

9. 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.

Encrypting Passwords

Follow the instructions in these sections to encrypt confidential information stored in the product, such as passwords and private keys for your certificates.

Setting Up Password Encryption

You can set up password encryption to protect confidential information stored in the product. You can also back up the encryption key that is stored in your product's Trusted Platform Module (TPM) chip to a USB flash drive.

Note: Make sure you have a USB flash drive with at least 1MB of storage space to back up the encryption key.

Caution: If the TPM chip fails, you cannot replace it or access any confidential information stored on your product. Printer functions are still available, but the password encryption feature cannot be used. Contact Epson for support.

1. Press the ⌂ home button, if necessary.
2. Select **Settings** > **General Settings** > **System Administration** > **Security Settings**.

You see a screen like this:

3. Select **Password Encryption**.
4. Select **On**.

   A message appears about restarting the product. Select **OK**.
5. Select **Proceed to Backup**.

   You see the encryption key backup screen.
6. Insert your USB flash drive into the external USB port on the front of the product.
7. Select **Start Backup**.

   The product begins backing up the encryption key to the USB flash drive. Any previously stored encryption key is overwritten.
8. When the backup completion message appears, select **Close**.
9. Turn the product off and then on again to apply the password encryption setting.

   Note: The product may take longer than usual to turn on. This is normal.

Parent topic: Encrypting Passwords

Related references

Where to Get Help

Related tasks

Restoring the Password Encryption Key

Restoring the Password Encryption Key

If the TPM chip fails, you can restore the encryption key from its backup stored on your USB flash drive.

1. If you see a message on the control panel that the TPM has been replaced when you turn on the product, select **Restore from Backup**. Enter the administrator password, if necessary.
2. Insert your USB flash drive containing the stored encryption key into the external USB port on the front of the product.
3. Select **Restore from Backup**.

   The stored encryption key is restored to the TPM chip.
4. When the completion message appears, select **OK**.

   The product restarts.

Parent topic: Encrypting Passwords

Managing Data Retention

Follow the instructions in these sections to configure your product's data retention settings or to erase any stored data from the product.

Erasing All Data from the Product
Changing the Auto Erase Settings

Erasing All Data from the Product

If you are giving away or disposing of your product, we recommend that you erase all data from the product.

1. Press the home button, if necessary.
2. Select **Settings** > **General Settings** > **System Administration** > **Reset**.

   You see a screen like this:

3. Select **Erase All Data and Settings**.

4. Do one of the following:
   - Select **High Speed** to perform a quick format on the encrypted hard drive. Data recovery is still possible if you select this option.
   - Select **Overwrite** to perform a full format on the encrypted hard drive and rewrite all data with zeroes. This process takes approximately 2.5 hours and data recovery is not possible. Select this option to fully erase anything you have stored, such as sensitive data.
   - Select **Triple Overwrite** to erase all data with a dedicated erase command. This process takes approximately 2.5 hours and data recovery is not possible. Select this option to perform an additional level of data erasure.
5. Select **Yes**.

   When all settings have been restored, a message appears about restarting the product. Select **Close** and the **System Administration** screen returns.
6. Select **Clear Internal Memory Data** > **Delete All Internal Memory Jobs** > **Yes**.

   When the memory has been cleared, a completion message appears.
7. Select the back arrow.
8. Select **HDD Erase Settings** > **Erase All Memory**.
9. Do one of the following:
   - Select **High Speed** to perform a quick format on the encrypted hard drive. Data recovery is still possible if you select this option.
   - Select **Overwrite** to perform a full format on the encrypted hard drive and rewrite all data with zeroes. This process takes approximately 2.5 hours and data recovery is not possible. Select this option to fully erase anything you have stored, such as sensitive data.
   - Select **Triple Overwrite** to erase all data with a dedicated erase command. This process takes approximately 2.5 hours and data recovery is not possible. Select this option to perform an additional level of data erasure.
10. Select **Yes** to continue.
11. Press the ⌂ home button to return to the home screen.
12. Turn the product off and on again to ensure the data is erased.

Parent topic: Managing Data Retention

Changing the Auto Erase Settings

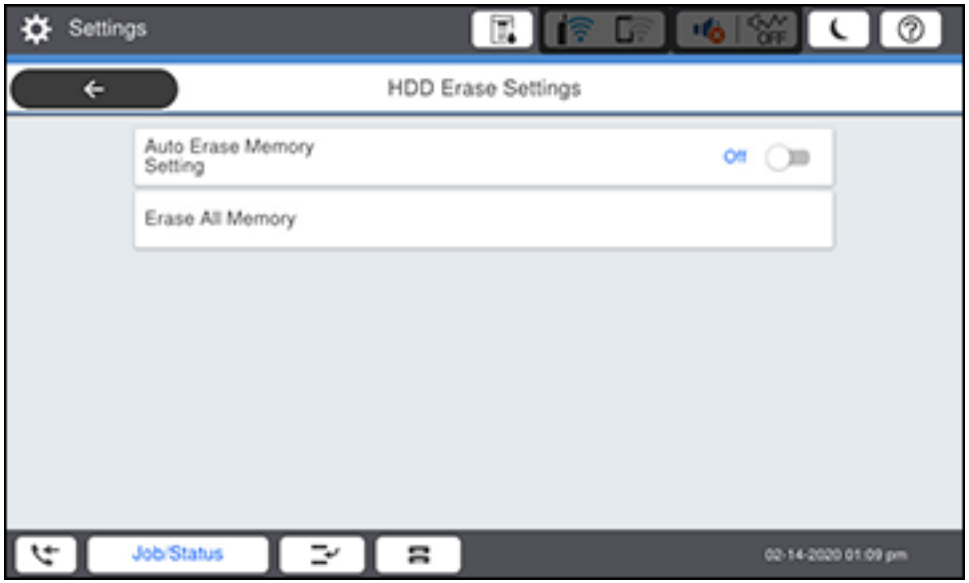
Your product can automatically delete data after it completes a print or copy job with the **Auto Erase Memory Setting** option. The following data is erased after each job:

- Copy buffer
- Printing buffer
- User Authenticated print area

Note: Enabling this option may affect the performance of your product.

1. Press the home button, if necessary.
2. Select **Settings** > **General Settings** > **System Administration** > **HDD Erase Settings**.

   You see a screen like this:



3. Select the **Auto Erase Memory Setting** field to turn the setting on.
4. Press the home button to return to the home screen.

Parent topic: Managing Data Retention

Solving Problems

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

Scanning Error Messages

If you see an error message when scanning images to a shared folder, check for solutions in this table.

Message	Solution
DNS error. Check DNS settings.	Try the following: • Make sure the address in the contacts list on the printer and the address of the shared folder are the same. • If the computer's IP address is static or set manually, change the computer name in the network path to the IP address. For example, change \\EPSON02\SCAN to \\192.168.xxx.xxx\SCAN. • Make sure your computer is turned on and not running in a power-saving mode, such as sleep or standby. If your computer is in sleep mode, you cannot save scanned images to the shared folder. • Temporarily disable your computer's firewall and security software. If this clears the error, check the settings in the security software. • You cannot save scanned images to a shared folder when using a public network. • If the IP address changes when reconnecting using DHCP on a laptop, obtain the IP address again. • Check the DNS on your product and on the server, computer, or router. • Make sure the computer name and IP address are correct.
Authentication error. Please check the Email Server Settings.	If user restrictions have been enabled, make sure you enter in the correct user name and password. Also, make sure that the password has not expired.

Message	Solution
Communication error. Check the Wi-Fi/network connection.	Try the following: • Make sure MS Network is enabled. • Make sure the address in the contacts list on the printer and the address of the shared folder are the same. • Access rights for the user in the contacts list should be added to the Sharing and Security tabs of the shared folder's properties. Access permissions should also be enabled for the user. • Print a network connection report to check if the printer is connected to the network.
The file name is already in use. Rename the file and scan again.	Check if there is a file with the same name as the file you want to save in the shared folder. Delete the saved file or select a different file name.
Scanned file(s) are too large. Only XX page(s) have been sent. Check if the destination has enough space.	Try the following: • Increase the storage space in the specified folder. • Reduce the number of documents. • Lower the scanning resolution or increase the compression ratio to reduce the size of the scanned image.

Parent topic: Solving Problems

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 the 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
Cannot Communicate with the Product Using IPsec Communication
Communication was Working, but Stopped
Cannot Create the Secure IPP Printing Port
Cannot Connect After Configuring IPsec/IP Filtering
Cannot Access the Product After Configuring IEEE 802.1X

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

Security method	Supported algorithms
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 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

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 and Wi-Fi 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.

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.

Message	Solution
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.
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

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

Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Mac and OS X are trademarks 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.

Parent topic: Notices

Copyright Notice

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

4/20

CPD-58931

Parent topic: Copyright Notice