EPSON
EXCEED YOUR VISION

Administrator's Guide

Contents

Contents

Appendix

Copyright and Trademarks

❏ EPSON is a registered trademark, and EPSON EXCEED YOUR VISION or EXCEED YOUR VISION is a trademark of Seiko Epson Corporation.

❏ Microsoft, Windows, and Windows Vista are registered trademarks of Microsoft Corporation.

❏ Mac OS, OS X, Bonjour, and Safari are registered trademarks of Apple Inc, registered in the U.S. and other countries. AirPrint is a trademark of Apple 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.

About this Manual

Marks and Symbols

> ⚠ *Caution:*
>
> *Instructions that must be followed carefully to avoid bodily injury.*

> ❗ *Important:*
>
> *Instructions that must be observed to avoid damage to your equipment.*

Note:
Instructions containing useful tips and restrictions on printer operation.

➡ Related Information

Clicking this icon takes you to related information.

Artworks

❏ Details of screen shots and illustrations may vary by model, but the instructions are the same.

❏ Screen shots are from Windows 7. Details may vary between OS versions.

❏ Some of the menu items in the screen shots may vary by model.

Operating System References

Windows

In this manual, terms such as "Windows 8.1", "Windows 8", "Windows 7", "Windows Vista", "Windows XP", "Windows Server 2012 R2", "Windows Server 2012","Windows Server 2008 R2", "Windows Server 2008", "Windows Server 2003 R2" and "Windows Server 2003" refer to the following operating systems. Additionally, "Windows" refers to all versions.

❏ Microsoft® Windows® 8.1 operating system

❏ Microsoft® Windows® 8 operating system

❏ Microsoft® Windows® 7 operating system

❏ Microsoft® Windows Vista® operating system

❏ Microsoft® Windows® XP operating system

❏ Microsoft® Windows® XP Professional x64 Edition operating system

❏ Microsoft® Windows Server® 2012 R2 operating system

❏ Microsoft® Windows Server® 2012 operating system

❏ Microsoft® Windows Server® 2008 R2 operating system

About this Manual

❏ Microsoft® Windows Server® 2008 operating system

❏ Microsoft® Windows Server® 2003 R2 operating system

❏ Microsoft® Windows Server® 2003 operating system 6

Mac OS X

In this manual, "Mac OS X v10.9.x" refers to OS X Mavericks and "Mac OS X v10.8.x" refers to OS X Mountain Lion. Additionally, "Mac OS X" refers to "Mac OS X v10.9.x" , "Mac OS X v10.8.x" , "Mac OS X v10.7.x" , "Mac OS X v10.6.x", and "Mac OS X v10.5.8".

Notices

❏ Reproduction of information in this manual is prohibited.

❏ All information in this manual is subject to change without notice.

❏ If you find inaccuracies or have concerns about this manual, contact Epson.

❏ Notwithstanding the preceding article, Epson cannot be held responsible for any effects resulting from the use of the product.

❏ Epson cannot be held responsible for any failures caused by the improper use of the product and the improper repair of the product by a third party.

Introduction

This manual is the common manual for Epson ink jet printers and multifunctional printers and this manual is for an system administrator who manages an office network. A system administrator means a person who is in charge of devices' configuration and authorization to access to a network for clients, printers, and computers. Detailed procedures may be left out depending on the topic and the glossary is not in this manual because this manual is for an administrator. Therefore knowledge about system of networks and computers is required to read.

There are two pieces of software to configure the printer's advanced network settings, Web Config and EpsonNet Config. In this manual, instructions for configuring each feature are basically from Web Config. For information on operations of EpsonNet Config, see the documentation or help of EpsonNet Config. Descriptions of the OS menu items are based on Windows 7 and Mac OS X 10.8.x.

Note:
To configure the system administration features, the printer must be connected to a network. For more information on connecting the printer to a network, see the printer's documentation or the appendix in this manual.

The sections below are the system administration features that Epson products support. The available features vary by model. For information on the availability of features, see the printer's documentation. Choose the features to be used that match your network environment.

SSL/TLS Communication

You can set a server certificate for the printer and encrypt communications between the printer and a computer by an SSL/TLS (Secure Sockets Layer/Transport Layer Security) communication. Use this feature to avoid spoofing and unauthorized access to the printer.
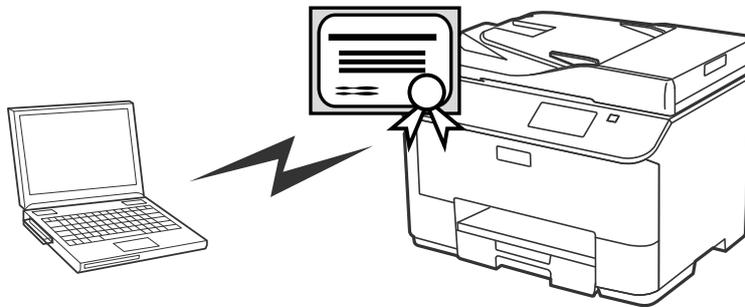
Related Information

➡ "Configuring SSL/TLS Communication" on page 16

Introduction

Encryption of IP Communication and Connection to an Authentication Network

You can encrypt communications and control access to the printer. If you want to avoid interception of communications and data tampering, use the **IPsec/IP Filtering** feature or the SNMPv3 protocol. If you want to authenticate access to the printer, use the IEEE802.1X feature.
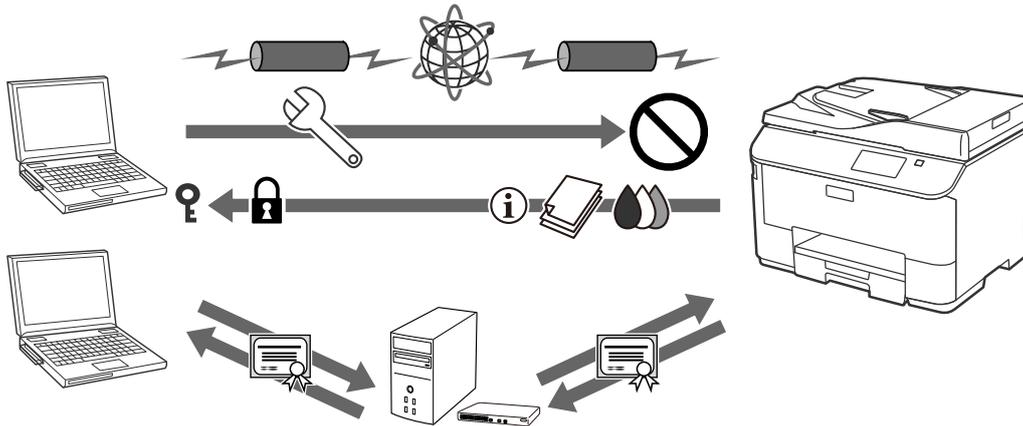
Related Information

➡ "Configuring IPsec/IP Filtering" on page 18

➡ "Using SNMPv3 Protocol" on page 26

➡ "Connecting the Printer to an IEEE802.1X Network" on page 27

Configuration of Scan and Fax Destination

You can use an LDAP server to choose a destination for scans and faxes. If you want to send scan and fax data by an email or avoid faxing errors, configure a mail server and an LDAP server.
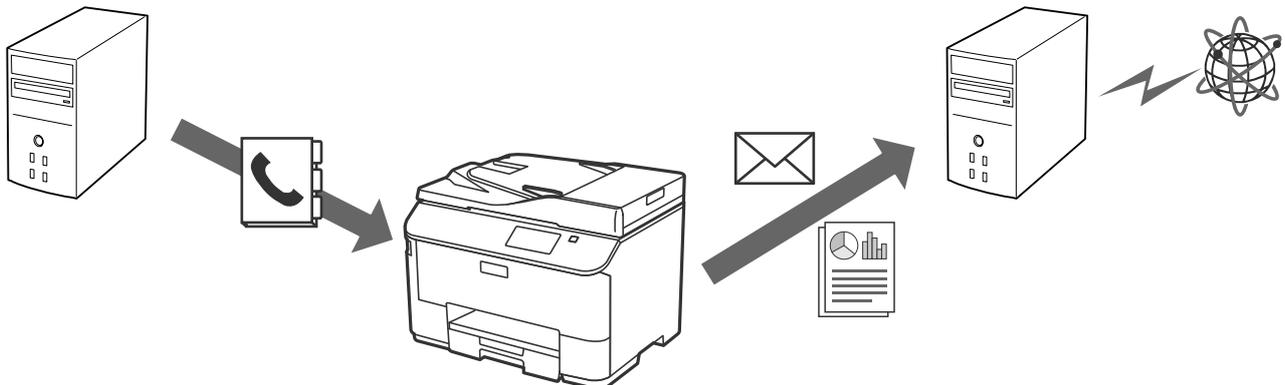
Related Information

➡ "Using the LDAP Server" on page 41

➡ "Using a Mail Server" on page 45

User Features Restriction and the Administrator Password

You can restrict printer features on a per user basis. For example, User A can copy and scan, while User B can only fax.

When you set the administrator password, only an administrator can change the printer's settings. It is recommended that you set the administrator password to improve security.
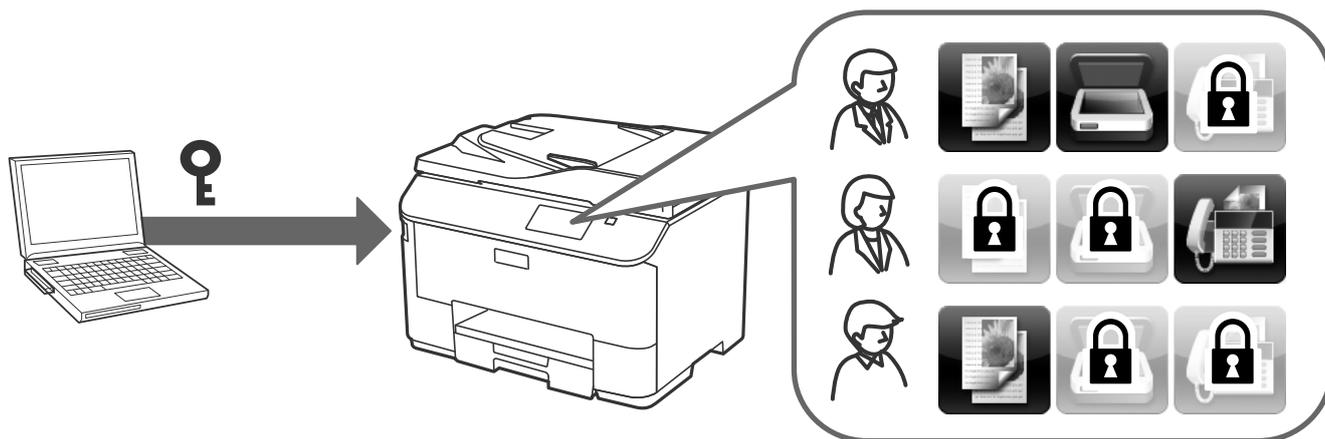
Related Information

➡ "User Features Restriction" on page 48

➡ "Configuring the Administrator Password" on page 50

Using Network Configuration Software

About Web Config

Web Config is a browser-based application for configuring the printer's settings.

To access the printer's Web Config, you need to have first assigned an IP address to the printer.

Note:
You can lock the settings by configuring the administrator password to the printer.

There are two setting pages as below.

❏ **Basic Settings**

You can configure the basic settings for the printer.
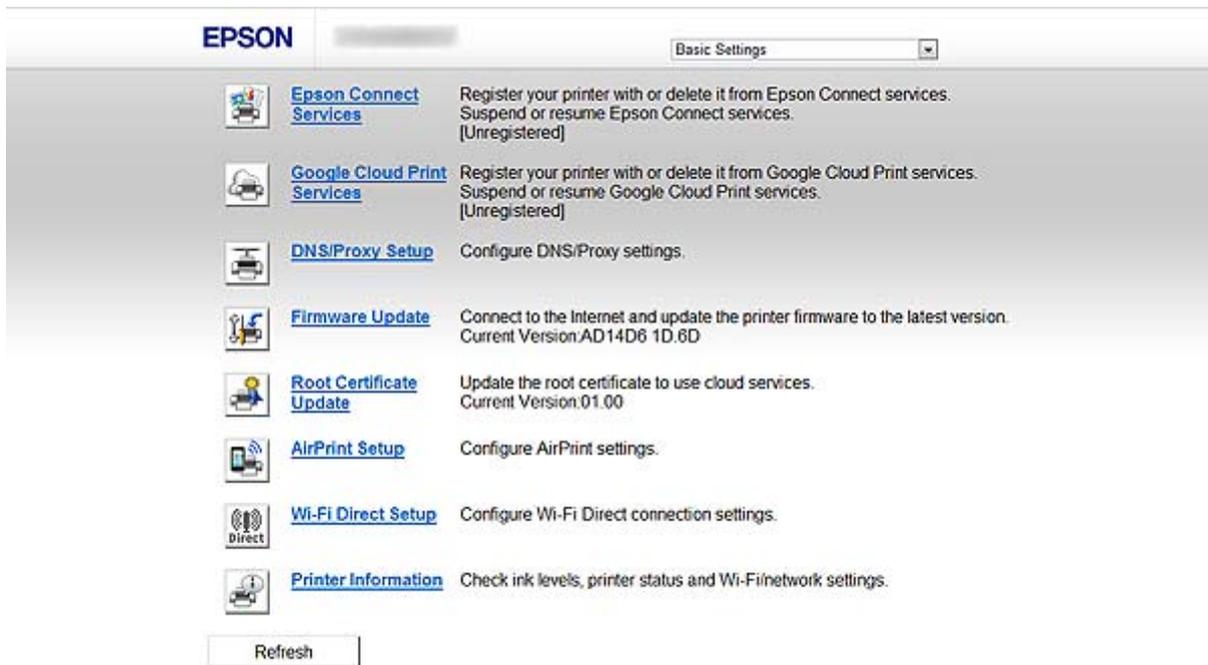
❏ **Advanced Settings**

You can configure the advanced settings for the printer. This page is mainly for an administrator.
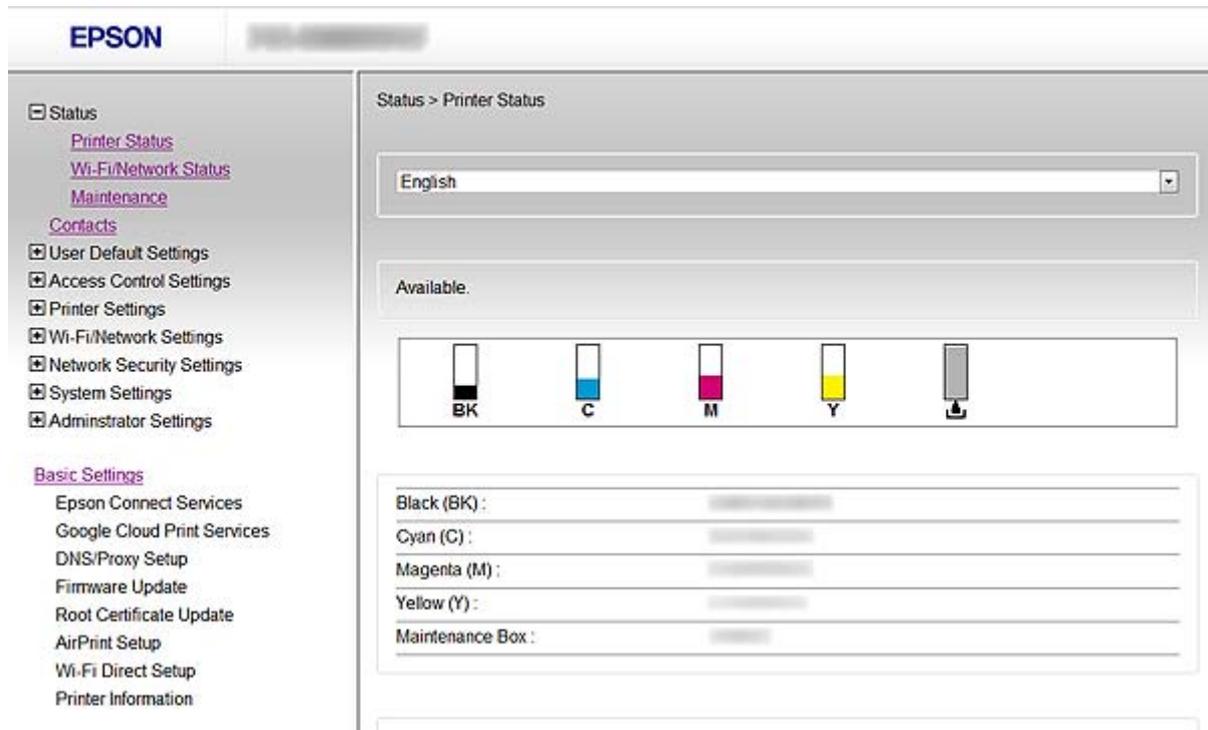
Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 14

Accessing Web Config

Enter the printer's IP address into a web browser. JavaScript must be enabled. When accessing Web Config via HTTPS, a warning message will appear in the browser since a self-signed certificate, stored in the printer, is used.

❏ Accessing via HTTP

IPv4: http://<printer IP address> (without the < >)

IPv6: http://[printer IP address]/ (with the [ ])

❏ Accessing via HTTPS

IPv4: https://<printer IP address> (without the < >)

IPv6: https://[printer IP address]/ (with the [ ])

Using Network Configuration Software

Note:

❏ *Examples*

    IPv4:

    http://192.168.100.201/

    https://192.168.100.201/

    IPv6:

    http://[2001:db8::1000:1]/

    https://[2001:db8::1000:1]/

❏ *If the printer name is registered with the DNS server, you can use the printer name instead of the printer's IP address.*

❏ *Not all menus are displayed when accessing Web Config via HTTP. To see all the menus, access Web Config via HTTPS.*

❏ *You can also access to Web Config from EpsonNet Config. Select the printer from the printer listed screen and click* **Launch Browser**.

Related Information

➡

➡

➡

About EpsonNet Config

EpsonNet Config allows the administrator to configure the printer's network settings, such as assigning an IP address and changing the connection mode. The batch setting feature is supported on Windows. For more information, see the documentation or help of EpsonNet Config.

Related Information

➡

Using EpsonNet Config – Windows

Installing EpsonNet Config – Windows

Install EpsonNet Config from the following folder on the software disc that came with the printer:

\Network\EpsonNetConfig

Running EpsonNet Config - Windows

Select **All Programs** > **EpsonNet** > **EpsonNet Config Vxx** > **EpsonNet Config**.

Note:
If the firewall alert appears, allow access for EpsonNet Config.

Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 14

Uninstalling EpsonNet Config - Windows

Select **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a program** > **EpsonNet Config Vxx** and then click **Uninstall**.

Using EpsonNet Config – Mac OS X

Installing EpsonNet Config – Mac OS X

Download EpsonNet Config from EPSON Software Updater, and then install it by following the on-screen instructions.

Running EpsonNet Config - Mac OS X

Select **Go** > **Applications** > **Epson Software** > **EpsonNet** > **EpsonNet Config Vxx** > **EpsonNet Config**.

Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 14

Uninstalling EpsonNet Config – Mac OS X

Use the Uninstaller to uninstall applications. You can download the Uninstaller using EPSON Software Updater or from Epson support website.

When running the Uninstaller, all the installed Epson applications are displayed. Select EpsonNet Config, and then follow the on-screen instructions.

Note:
*If you do not have the Uninstaller, drag and drop the program folder in **Applications** on the trash icon in the dock.*

Web Config and EpsonNet Config Feature Comparison

There are two pieces of software to configure the printer's network settings, Web Config and EpsonNet Config.

The following are features covered in this manual and a comparison between the two pieces of software.

Features	Web Config	EpsonNet Config
Configuring SSL/TLS communication	✓	✓
Configuring a server certificate for the printer	✓	✓
Configuring IPsec/IP Filtering	✓	✓
Configuring SNMPv3 protocol	✓	–
Connecting the printer to an IEEE802.1X network (Ethernet/Wi-Fi)	✓	✓
Obtaining and importing a CA-signed certificate	✓	–
Updating a self-signed certificate	✓	–
Registering a destination to Contacts	✓	✓
Configuring LDAP server	✓	✓
Configuring a mail server	✓	✓
Restricting available printer features	✓	✓
Configuring the administrator password	✓	✓
Configuring email notification	✓	–
Making batch settings for multiple printers	–	✓ (Windows only)
Importing and exporting Contacts and other settings	–	✓

Related Information

Other Network Software

About EpsonNet Print (Windows Only)

EpsonNet Print is a software to print on the TCP/IP network. There are features and restrictions listed below. For more information, visit your regional Epson website.

❏ The printer's status is displayed on the spooler screen.

❏ If the printer's IP address is changed by DHCP, the printer is still detected.

❏ You can use a printer located on a different network segment.

❏ You can print using one of the following protocols: LPD, Enhanced LPD and RAW.

❏ IPv6 address is not supported.

Related Information

About EpsonNet SetupManager

EpsonNet SetupManager is a software to create a package for a simple printer installation, such as installing the printer driver, installing EPSON Status Monitor and creating a printer port.

This software allows the administrator to create unique software packages and distribute them among groups.

For more information, visit your regional Epson website.

Using the Printer in a Secure Network

In this topic, the security features that Epson products support are explained. The available features vary by model. For information on availability of features, see the printer's documentation.

Configuring SSL/TLS Communication

Configuring Basic SSL/TLS Settings

If the printer supports the HTTPS server feature, you can use an SSL/TLS communication to encrypt communications. You can configure and manage the printer using Web Config while ensuring security.

Configure encryption strength and redirect feature.

1. Access the printer's Web Config and select **Network Security Settings** > **SSL/TLS** > **Basic**.

2. Select a value for each item.

   ❏ **Encryption Strength**

   You can select one of the followings.

   ❏ **High**: AES256/3DES

   ❏ **Middle**: AES256/3DES/AES128/RC4

   ❏ **Redirect HTTP to HTTPS**

   You can configure to redirect to HTTPS when accessing with HTTP.
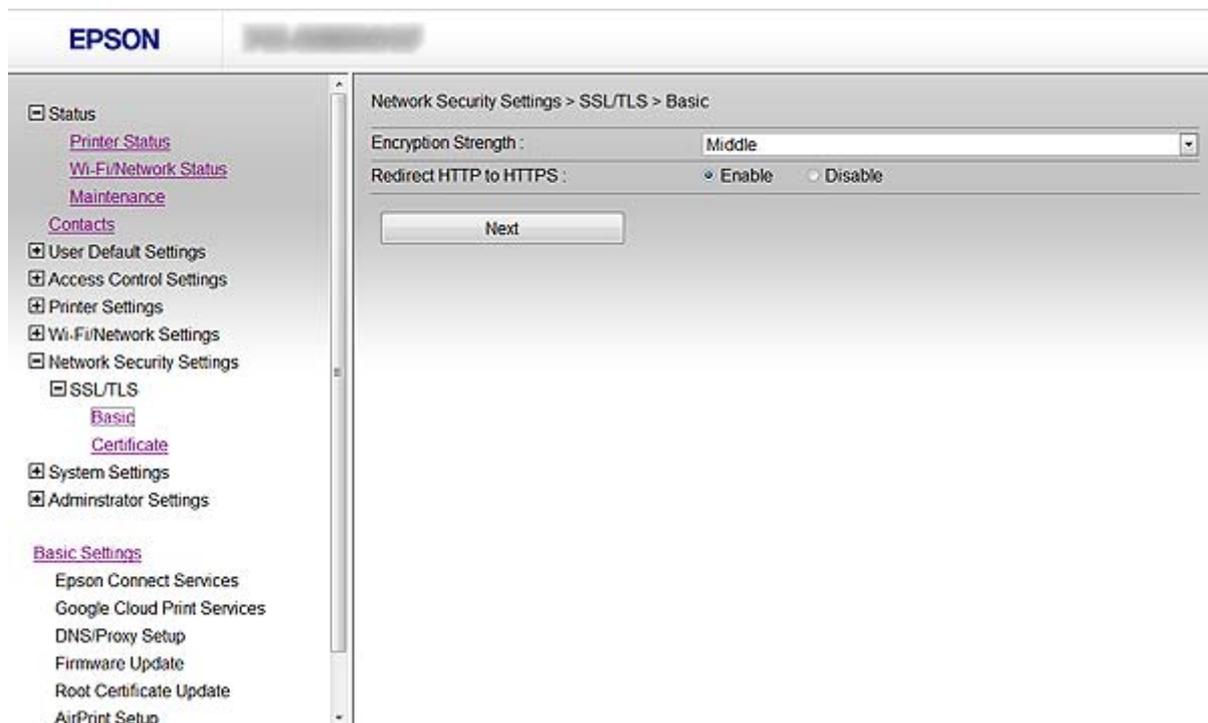
3. Click **Next**.

   A confirmation message is displayed.

4. Click **OK**.

   The printer is updated.

Related Information

➡ "Accessing Web Config" on page 11

Configuring a Server Certificate for the Printer

1. Access the printer's Web Config and select **Network Security Settings** >**SSL/TLS**> **Certificate**.

2. Specify a certificate to use on **Server Certificate**.

   ❏ **Self-signed Certificate**

   A self-signed certificate has been generated by the printer. If you do not obtain a CA-signed certificate, select this.

   ❏ **CA-signed Certificate**

   If you obtain and import a CA-signed certificate in advance, you can specify this.

3. Click **Next**.

   A confirmation message is displayed.

4. Click **OK**.

   The printer is updated.

Related Information

➡

➡

Configuring IPsec/IP Filtering

About IPsec/IP Filtering

If the printer supports IPsec/IP Filtering, you can filter traffic based on IP addresses, services, and port. By combining of the filtering, you can configure the printer to accept or block specified clients and specified data. Additionally, you can improve security level by using an IPsec.

To filter traffic, configure the default policy. The default policy applies to every user or group connecting to the printer. For more fine-grained control over users and groups of users, configure group policies. A group policy is one or more rules applied to a user or user group. The printer controls IP packets that match with configured policies. IP packets are authenticated in the order of a group policy 1 to 10 then a default policy.

Note:
Computers that run Windows Vista or later or Windows Server 2008 or later support IPsec.

Configuring Default Policy

1. Access the printer's Web Config and select **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.

2. Enter a value for each item.

3. Click **Next**.

   A confirmation message is displayed.

4. Click **OK**.

   The printer is updated.

Related Information

➡

➡

Default Policy Setting Items
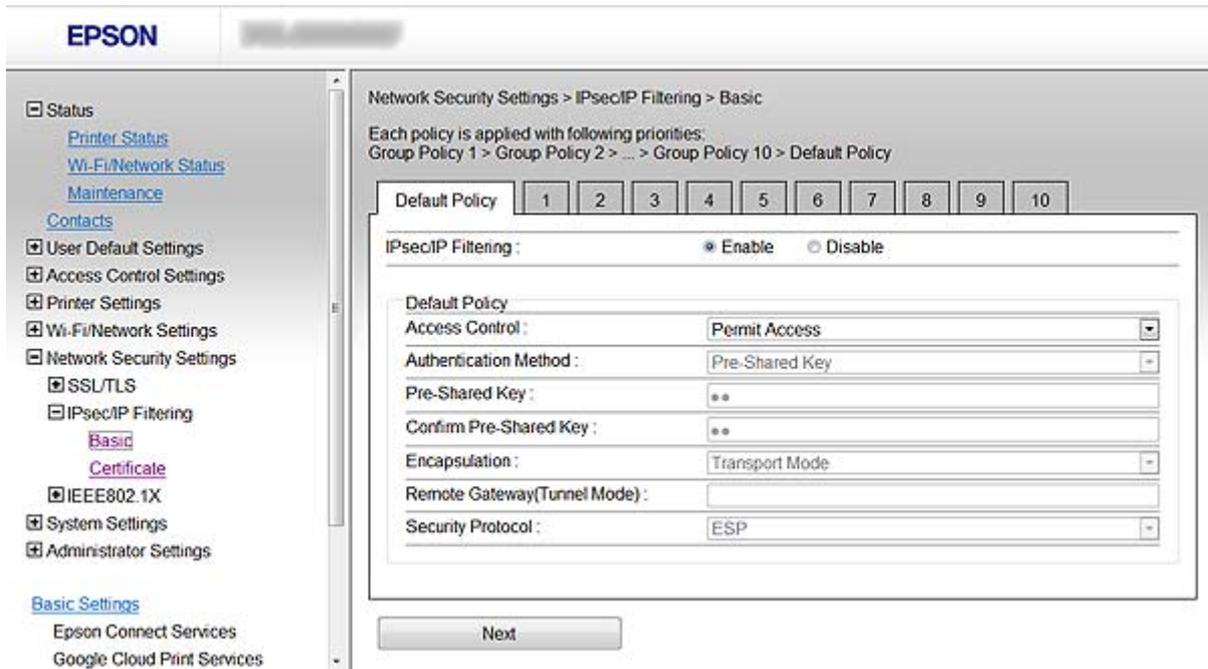
Items	Settings and Explanation	
IPsec/IP Filtering	You can enable or disable an IPsec/IP Filtering feature.	
Access Control	Configure a control method for traffic of IP packets.	
	Permit Access	Select this to permit configured IP packets to pass through.
	Refuse Access	Select this to refuse configured IP packets to pass through.
	IPsec	Select this to permit configured IPsec packets to pass through.
Authentication Method	To select **Certificate**, you need to obtain and import a CA-signed certificate in advance.	
Pre-Shared Key	If you select **Pre-Shared Key** for **Authentication Method**, enter a pre-shared key between 1 and 127 characters.	
Confirm Pre-Shared Key	Enter the key you configured for confirmation.	
Encapsulation	If you select **IPsec** for **Access Control**, you need to configure an encapsulation mode.	
	Transport Mode	If you only use the printer on the same LAN, select this. IP packets of layer 4 or later are encrypted.
	Tunnel Mode	If you use the printer on the Internet-capable network such as IPsec-VPN, select this option. The header and data of the IP packets are encrypted.
Remote Gateway(Tunnel Mode)	If you select **Tunnel Mode** for **Encapsulation**, enter a gateway address between 1 and 39 characters.	

Using the Printer in a Secure Network

Items	Settings and Explanation	
Security Protocol	If you select **IPsec** for **Access Control**, select an option.	
	ESP	Select this to ensure the integrity of an authentication and data, and encrypt data.
	AH	Select this to ensure the integrity of an authentication and data. Even if encrypting data is prohibited, you can use IPsec.

Related Information

➡ "Configuring Default Policy" on page 18

Configuring Group Policy

1. Access the printer's Web Config and select **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.

2. Click a numbered tab you want to configure.

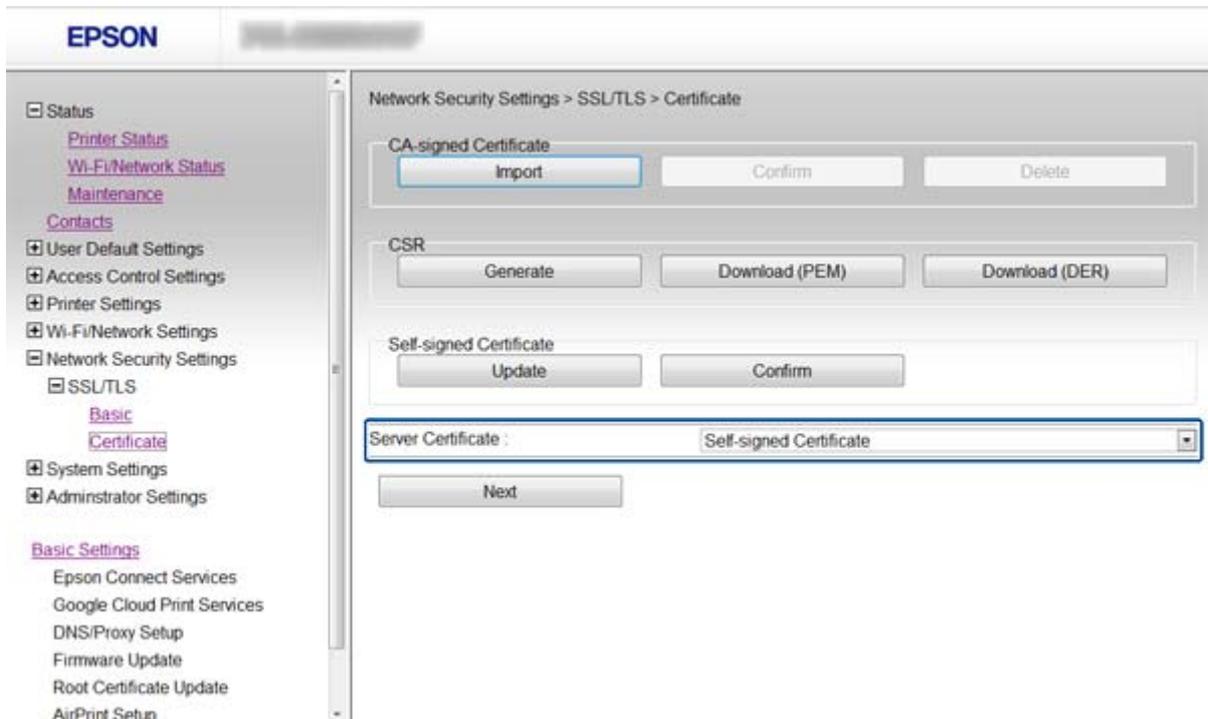3. Enter a value for each item.

4. Click **Next**.

    A confirmation message is displayed.

5. Click **OK**.

    The printer is updated.

Related Information

➡ "Accessing Web Config" on page 11
➡ "Group Policy Setting Items" on page 21

Group Policy Setting Items

Items	Settings and Explanation	
Enable this Group Policy	You can enable or disable a group policy.	
Access Control	Configure a control method for traffic of IP packets.	
	Permit Access	Select this to permit configured IP packets to pass through.
	Refuse Access	Select this to refuse configured IP packets to pass through.
	IPsec	Select this to permit configured IPsec packets to pass through.
Local Address(Printer)	Select an IPv4 address or IPv6 address that matches your network environment. If an IP address is assigned automatically, you can select **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Enter a device's IP address to control access. The IP address must be between 0 and 43 characters. If you do not enter an IP address, all addresses are controlled. *Note:* *If an IP address is assigned automatically (e.g. assigned by DHCP), the connection may be unavailable. Configure a static IP address.*	
Method of Choosing Port	Select a method to specify ports.	
Service Name	If you select **Service Name** for **Method of Choosing Port**, select an option.	
Transport Protocol	If you select **Port Number** for **Method of Choosing Port**, you need to configure an encapsulation mode.	
	Any Protocol	Select this to control all protocol types.
	TCP	Select this to control data for unicast.
	UDP	Select this to control data for broadcast and multicast.
	ICMPv4	Select this to control ping command.

21

Using the Printer in a Secure Network

Items	Settings and Explanation	
Local Port	If you select **Port Number** for **Method of Choosing Port** and if you select **TCP** or **UDP** for **Transport Protocol**, enter port numbers to control receiving packets, separating them with commas. You can enter 10 port numbers at the maximum. Example: 20,80,119,5220 If you do not enter a port number, all ports are controlled.	
Remote Port	If you select **Port Number** for **Method of Choosing Port** and if you select **TCP** or **UDP** for **Transport Protocol**, enter port numbers to control sending packets, separating them with commas. You can enter 10 port numbers at the maximum. Example: 25,80,143,5220 If you do not enter a port number, all ports are controlled.	
Authentication Method	If you select **IPsec** for **Access Control**, select an option. Used certificate is common with a default policy.	
Pre-Shared Key	If you select **Pre-Shared Key** for **Authentication Method**, enter a pre-shared key between 1 and 127 characters.	
Confirm Pre-Shared Key	Enter the key you configured for confirmation.	
Encapsulation	If you select **IPsec** for **Access Control**, you need to configure an encapsulation mode.	
	Transport Mode	If you only use the printer on the same LAN, select this. IP packets of layer 4 or later are encrypted.
	Tunnel Mode	If you use the printer on the Internet-capable network such as IPsec-VPN, select this option. The header and data of the IP packets are encrypted.
Remote Gateway(Tunnel Mode)	If you select **Tunnel Mode** for **Encapsulation**, enter a gateway address between 1 and 39 characters.	
Security Protocol	If you select **IPsec** for **Access Control**, select an option.	
	ESP	Select this to ensure the integrity of an authentication and data, and encrypt data.
	AH	Select this to ensure the integrity of an authentication and data. Even if encrypting data is prohibited, you can use IPsec.

Related Information

Combination of Local Address(Printer) and Remote Address(Host) on Group Policy

	Setting of Local Address(Printer)		
	IPv4	IPv6[2]	Any addresses[3]

Using the Printer in a Secure Network

Setting of Remote Address(Host)	IPv4*¹	✓	–	✓
	IPv6*¹*²	–	✓	✓
	Blank	✓	✓	✓

*1If **IPsec** is selected for **Access Control**, you cannot specify in a prefix length.

*2If **IPsec** is selected for **Access Control**, you can select a link-local address (fe80::) but group policy will be disabled.

*3Except IPv6 link local addresses.

References of Service Name on Group Policy

Service Name	Protocol type	Local port number	Remote port number	Features controlled
Any	–	–	–	All services
ENPC	UDP	3289	Any port	Searching for a printer from applications such as EpsonNet Config, a printer driver and the a scanner driver
SNMP	UDP	161	Any port	Acquiring and configuring of MIB from applications such as EpsonNet Config, the Epson printer driver and the Epson scanner driver
LPR	TCP	515	Any port	Forwarding LPR data
RAW (Port9100)	TCP	9100	Any port	Forwarding RAW data
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 printer 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 of push scanning from Document Capture Pro
Network Push Scan Discovery	UDP	2968	Any port	Searching for a computer when push scanning from Document Capture Pro is executed
FTP Data (Local)	TCP	20	Any port	FTP server (forwarding data of FTP printing)
FTP Control (Local)	TCP	21	Any port	FTP server (controlling FTP printing)
FTP Data (Remote)	TCP	Any port	20	FTP client (forwarding scan data and received fax data) However this can control only an FTP server that uses remote port number 20.

Using the Printer in a Secure Network

Service Name	Protocol type	Local port number	Remote port number	Features controlled
FTP Control (Remote)	TCP	Any port	21	FTP client (controlling to forward scan data and received fax data)
CIFS (Local)*	TCP	445	Any port	CIFS server (Sharing a network folder)
CIFS (Remote)*	TCP	Any port	445	CIFS server (forwarding scan data and received fax data to a folder)
HTTP (Local)	TCP	80	Any port	HTTP(S) server (forwarding data of Web Config and WSD)
HTTPS (Local)	TCP	443	Any port	
HTTP (Remote)	TCP	Any port	80	HTTP(S) client (communicating between Epson Connect or Google Cloud Print, firmware updating and root certificate updating)
HTTPS (Remote)	TCP	Any port	443	

*If you want to control features forwarding scan data and received fax data, sharing a network folder or receiving fax from PC-FAX, change the setting of **Method of Choosing Port** to **Port Number** from **Service Name**, and then specify the port numbers for CIFS and NetBIOS.

Configuration Examples of IPsec/IP Filtering

Receiving IPsec packets only

This example is to configure a default policy only.

Default Policy:

❏ **IPsec/IP Filtering: Enable**

❏ **Access Control**: **IPsec**

❏ **Authentication Method**: **Pre-Shared Key**

❏ **Pre-Shared Key**: Enter up to 127 characters.

Group Policy:

Do not configure.

Receiving printing data and printer settings

This example allows communications of printing data and printer configuration from specified services.

Default Policy:

❏ **IPsec/IP Filtering: Enable**

❏ **Access Control**: **Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: Check the box.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: IP address of a client

❏ **Method of Choosing Port**: **Service Name**

❏ **Service Name**: Check the box of **ENPC**, **SNMP**, **HTTP (Local)**, **HTTPS (Local)** and **RAW (Port9100)**.

Receiving access from a specified IP address only

This example allows a specified IP address to access the printer.

Default Policy:

❏ **IPsec/IP Filtering: Enable**

❏ **Access Control:Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: Check the box.

❏ **Access Control: Permit Access**

❏ **Remote Address(Host)**: IP address of an administrator's client

Note:
Regardless of policy configuration, the client will be able to access and configure the printer.

Configuring a Certificate for IPsec/IP Filtering

1. Access the printer's Web Config and select **Network Security Settings** > **IPsec/IP Filtering** > **Certificate**.

2. Specify a certificate to use on **Use the following CA Certificate**.

   You can specify an imported certificate for other features.

3. Specify a certificate to use on **Use the following Client Certificate**.

   You can specify an imported certificate for other features.

4. Click **Next**.

   A confirmation message is displayed.

5. Click **OK**.

   The printer is updated.

Related Information

➡

➡
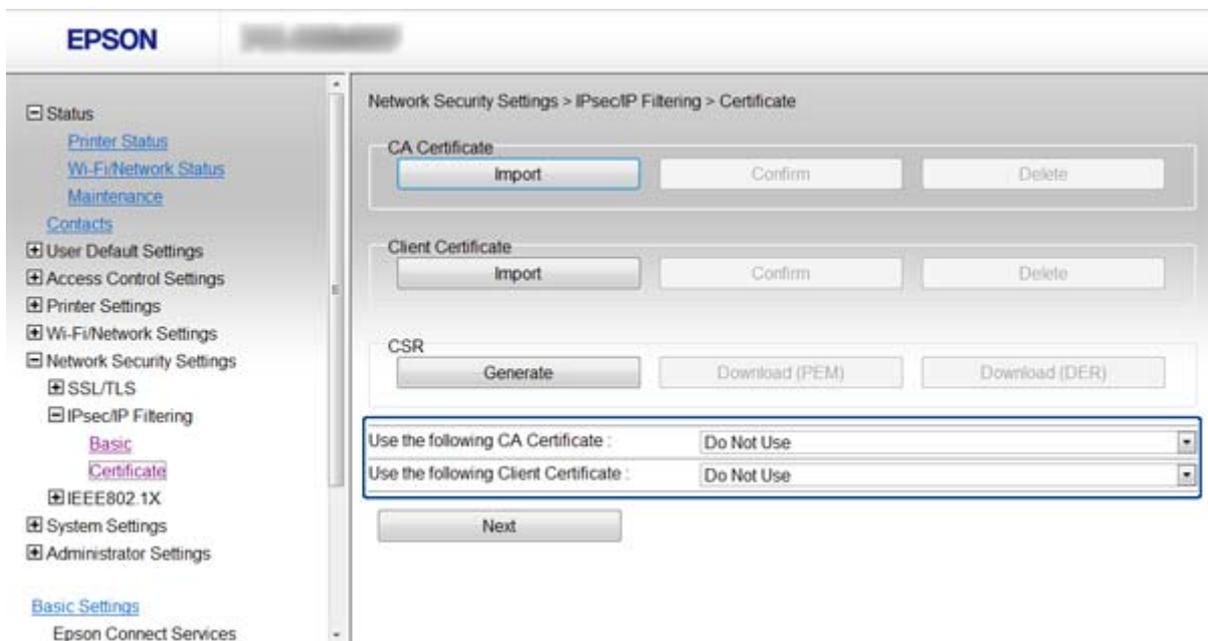
Using SNMPv3 Protocol

Configuring SNMPv3

If the printer supports the SNMPv3 protocol, you can monitor and control accesses to the printer.

1. Access the printer's Web Config and select **Wi-Fi/Network Settings** > **Services** > **Protocol** .

2. Enter a value for each item of **SNMPv3 Settings**.

3. Click **Next**.

   A confirmation message is displayed.

4. Click **OK**.

   The printer is updated.

Related Information

➡

➡

SNMPv3 Setting Items
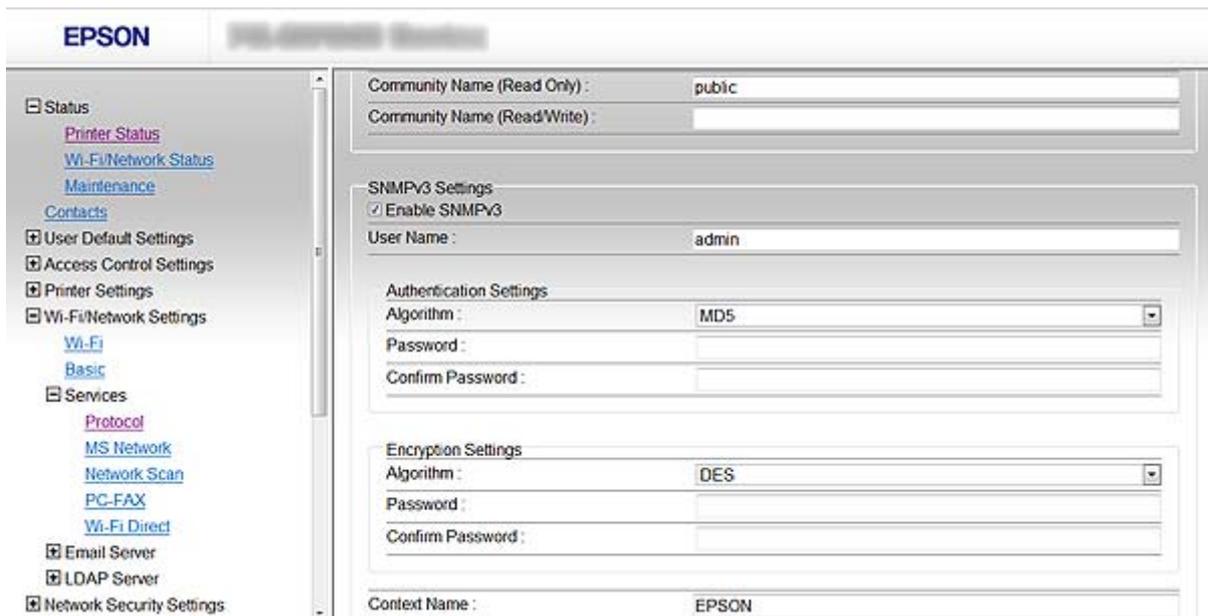
Using the Printer in a Secure Network

Items	Settings and Explanation
Enable SNMPv3	SNMPv3 is enabled when the box is checked.
User Name	Enter between 1 and 32 characters using 1 byte characters.
Authentication Settings	
Algorithm	Select an algorithm for an authentication.
Password	Enter between 8 and 32 characters in ASCII (0x20-0x7E).
Confirm Password	Enter the password you configured for confirmation.
Encryption Settings	
Algorithm	Select an algorithm for an encryption.
Password	Enter between 8 and 32 characters in ASCII (0x20-0x7E).
Confirm Password	Enter the password you configured for confirmation.
Context Name	Enter between 1 and 32 characters using 1 byte characters.

Related Information

➡

Connecting the Printer to an IEEE802.1X Network

Configuring an IEEE802.1X Network

If the printer supports IEEE802.1X, you can use the printer on a network with authentication that is connected to a RADIUS server and a hub as an authenticator.

1. Access the printer's Web Config and select **Network Security Settings** > **IEEE802.1X** > **Basic**.

2. Enter a value for each item.

   If you want to use the printer on a Wi-Fi network, click **Wi-Fi Setup** and select or enter an SSID.

   Note:
   You can share settings between Ethernet and Wi-Fi.

3. Click **Next**.

   A confirmation message is displayed.

4. Click **OK**.

   The printer is updated.

Related Information

➡
➡
➡

IEEE802.1X Network Setting Items
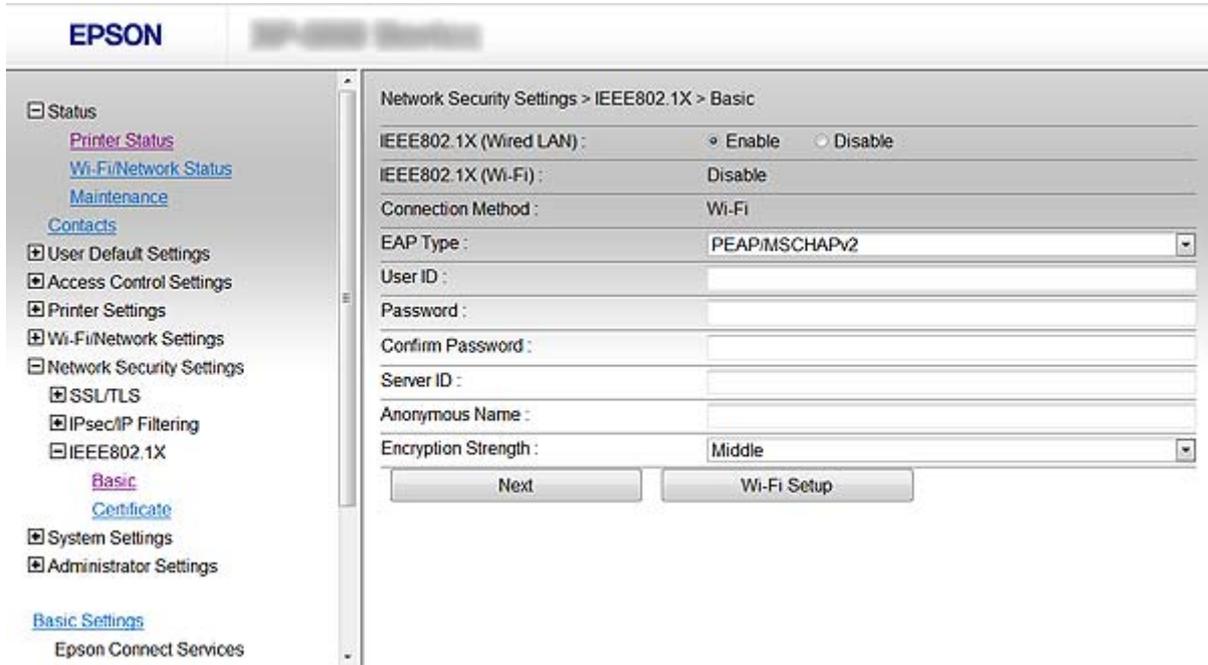
Items	Settings and Explanation	
IEEE802.1X (Wired LAN)	You can enable or disable settings of the page (**IEEE802.1X** > **Basic**) for IEEE802.1X (Wired LAN).	
IEEE802.1X (Wi-Fi)	The connection status of IEEE802.1X (Wi-Fi) is displayed.	
Connection Method	The connection method of a current network is displayed.	
EAP Type	Select an option for an authentication method between the printer and a RADIUS server.	
	EAP-TLS	You need to obtain and import a CA-signed certificate.
	PEAP-TLS	
	PEAP/MSCHAPv2	You need to configure a password.
User ID	Configure an ID to use for an authentication of a RADIUS server.	
Password	Configure a password to authenticate the printer.	
Confirm Password	Enter the password you configured for confirmation.	
Server ID	You can configure a server ID to authenticate with a specified RADIUS server. Authenticator verifies whether a server ID is contained in the subject/subjectAltName field of a server certificate that is sent from a RADIUS server or not.	
Anonymous Name	If you select **PEAP-TLS** or **PEAP/MSCHAPv2** for **Authentication Method**, you can configure an anonymous name instead of a user ID for a phase 1 of a PEAP authentication.	
Encryption Strength	You can select one of the followings.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Related Information

➡

Configuring a Certificate for IEEE802.1X

1. Access the printer's Web Config and select **Network Security Settings** > **IEEE802.1X** > **Certificate**.

2. Specify a certificate to use on **Use the following CA Certificate**.

   You can specify an imported certificate for other features.

3. Specify a certificate to use on **Use the following Client Certificate**.

   You can specify an imported certificate for other features.

4. Click **Next**.

   A confirmation message is displayed.

5. Click **OK**.

   The printer is updated.

Related Information

➡
➡
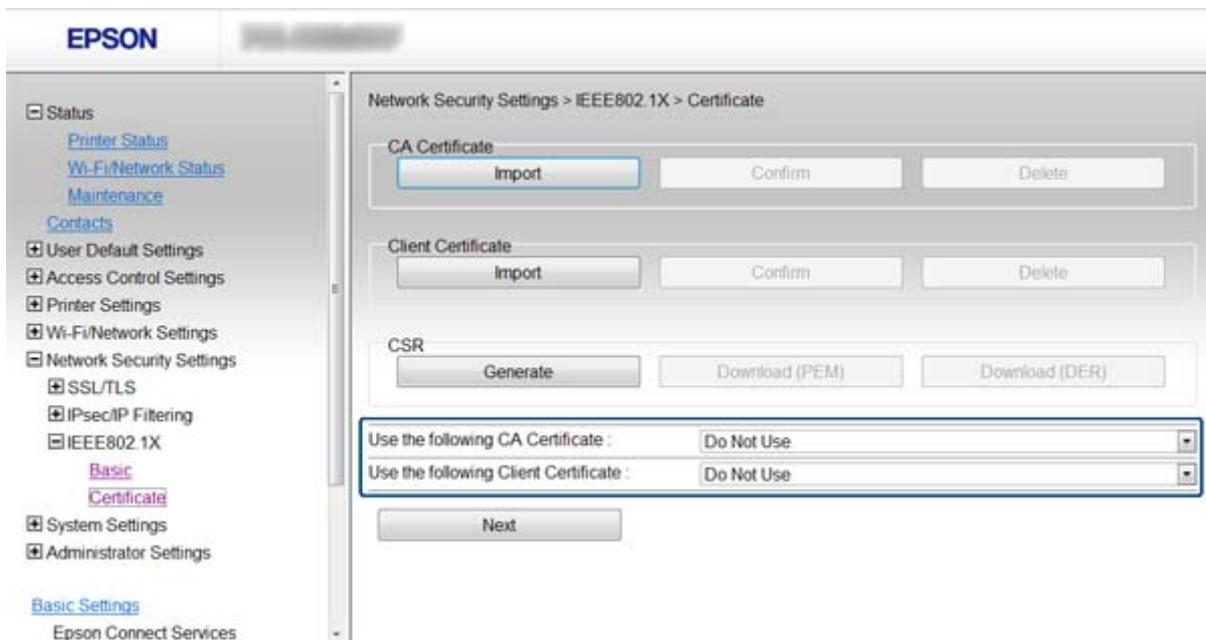
Checking IEEE802.1X Network Status

You can check the IEEE802.1X status by printing a network status sheet. For more information on printing a network status sheet, see the printer's documentation.

Status ID	IEEE802.1X Status
Disable	IEEE802.1X feature is disable.
EAP Success	IEEE802.1X authentication has succeeded and network connection is available.
Authenticating	IEEE802.1X authentication has not been completed.
Config Error	Authentication has failed since the user ID has not been set.
Client Certificate Error	Authentication has failed since the client certificate is out of date.
Timeout Error	Authentication has failed since there is no answer from the RADIUS server and/or authenticator.
User ID Error	Authentication has failed since the printer's user ID and/or certificate protocol is incorrect.
Server ID Error	Authentication has failed since the server ID of the server certificate and the server's ID do not match.
Server Certificate Error	Authentication has failed since there are the following errors in the server certificate. ❑ The server certificate is out of date. ❑ The chain of the server certificate is incorrect.
CA Certificate Error	Authentication has failed since there are the following errors in a CA certificate. ❑ Specified CA certificate is incorrect. ❑ The correct CA certificate is not imported. ❑ CA certificate is out of date.
EAP Failure	Authentication has failed since there are the following errors in the printer settings. ❑ If **Authentication Method** is **EAP-TLS** or **PEAP-TLS**, client certificate is incorrect or has certain problems. ❑ If **Authentication Method** is **PEAP/MSCHAPv2**, user ID or password is not correct.

Using a Digital Certificate

About Digital Certification

❑ Certificate signed by a CA

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

❑ CA certificate

A CA certificate indicates that a third party has verified the identity of a server. This is a key component in a web-of-trust style of security. You need to obtain a CA certificate for server authentication from a CA that issues it.

❏ Self-signed certificate

Self-signed certificate is a certificate that the printer issues and signs itself. This certificate is unreliable and cannot avoid spoofing. If you use this certificate for an SSL/TLS certificate, a security alert may be displayed on a browser. You can use this certificate only for an SSL/TLS communication.

Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 14
➡ "Obtaining and Importing a CA-signed Certificate" on page 31
➡ "Deleting a CA-signed Certificate" on page 34
➡ "Updating a Self-signed Certificate" on page 35

Obtaining and Importing a CA-signed Certificate

Obtaining a CA-signed Certificate

To obtain a CA-signed certificate, create a CSR (Certificate Signing Request) and apply it to certificate authority. You can create a CSR using the printer's Web Config and a computer.

Follow the steps to create a CSR and obtain a CA-signed certificate using Web Config. When creating a CSR using Web Config, a certificate is the PEM/DER format.

1. Access the printer's Web Config and select **Network Security Settings** > **SSL/TLS**, **IPsec/IP Filtering** or **IEEE802.1X** > **Certificate**.

2. Click **Generate** of **CSR**.

   A CSR creating page is opened.

3. Enter a value for each item.

   Note:
   Available key length and abbreviations vary by a certificate authority. Create a request according to rules of each certificate authority.

4. Click **OK**.

   A completion message is displayed.

5. Select **Network Security Settings** > **SSL/TLS**, **IPsec/IP Filtering** or **IEEE802.1X** > **Certificate**.

6. Click one of the download buttons of **CSR** according to a specified format by each certificate authority to download a CSR to a computer.

   > ⚠ *Important:*
   > *Do not generate a CSR again. If you do so, you may not be able to import an issued CA-signed certificate.*

7. Send the CSR to a certificate authority and obtain a CA-signed certificate.

   Follow the rules of each certificate authority on sending method and form.

8. Save the issued CA-signed certificate to a computer connected to the printer.

   Obtaining a CA-signed certificate is complete when you save a certificate to a destination.

Related Information

CSR Setting Items
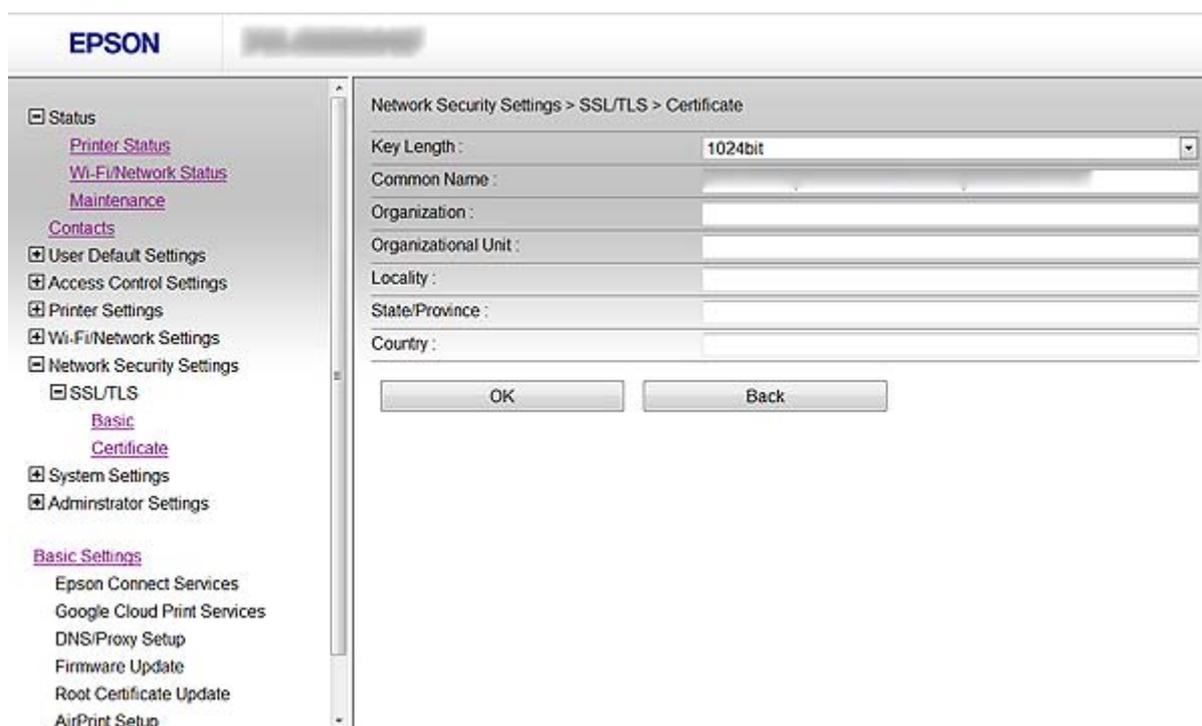
Items	Settings and Explanation
Key Length	Select a key length for a CSR.
Common Name	You can enter between 1 and 128 characters. If this is an IP address, it should be a static IP address. Example: URL for accessing Web Config: https://10.152.12.225 Common name: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	You can enter between 0 and 64 characters in ASCII (0x20-0x7E). You can divide distinguished names with commas.
Country	Enter a country code in two-digit number specified by ISO-3166.

Related Information

Importing a CA-signed Certificate

> ⚠️ *Important:*
> ❏ *Make sure that the printer's date and time is set correctly.*
> ❏ *If you obtain a certificate using a CSR created from Web Config, you can import a certificate one time.*

1. Access the printer's Web Config and select **Network Security Settings** > **SSL/TLS**, **IPsec/IP Filtering** or **IEEE802.1X** > **Certificate**.

2. Click **Import**.

   A certificate importing page is opened.

3. Enter a value for each item.

   Depending on where you create a CSR and the file format of the certificate, required settings may vary. Enter values to required items according to the following.

   ❏ A certificate of the PEM/DER format obtained from Web Config

   ❏ **Private Key**: Do not configure because the printer contains a private key.

   ❏ **Password**: Do not configure.

   ❏ **CA Certificate 1/CA Certificate 2**: Optional

   ❏ A certificate of the PEM/DER format obtained from a computer

   ❏ **Private Key**: You need to set.

   ❏ **Password**: Do not configure.

   ❏ **CA Certificate 1/CA Certificate 2**: Optional

   ❏ A certificate of the PKCS#12 format obtained from a computer

   ❏ **Private Key**: Do not configure.

   ❏ **Password**: Optional

   ❏ **CA Certificate 1/CA Certificate 2**: Do not configure.

4. Click **OK**.

   A completion message is displayed.

Note:
Click ***Confirm*** *to verify the certificate information.*

Related Information

➡ "Accessing Web Config" on page 11
➡ "CA-signed Certificate Importing Setting Items" on page 34

CA-signed Certificate Importing Setting Items
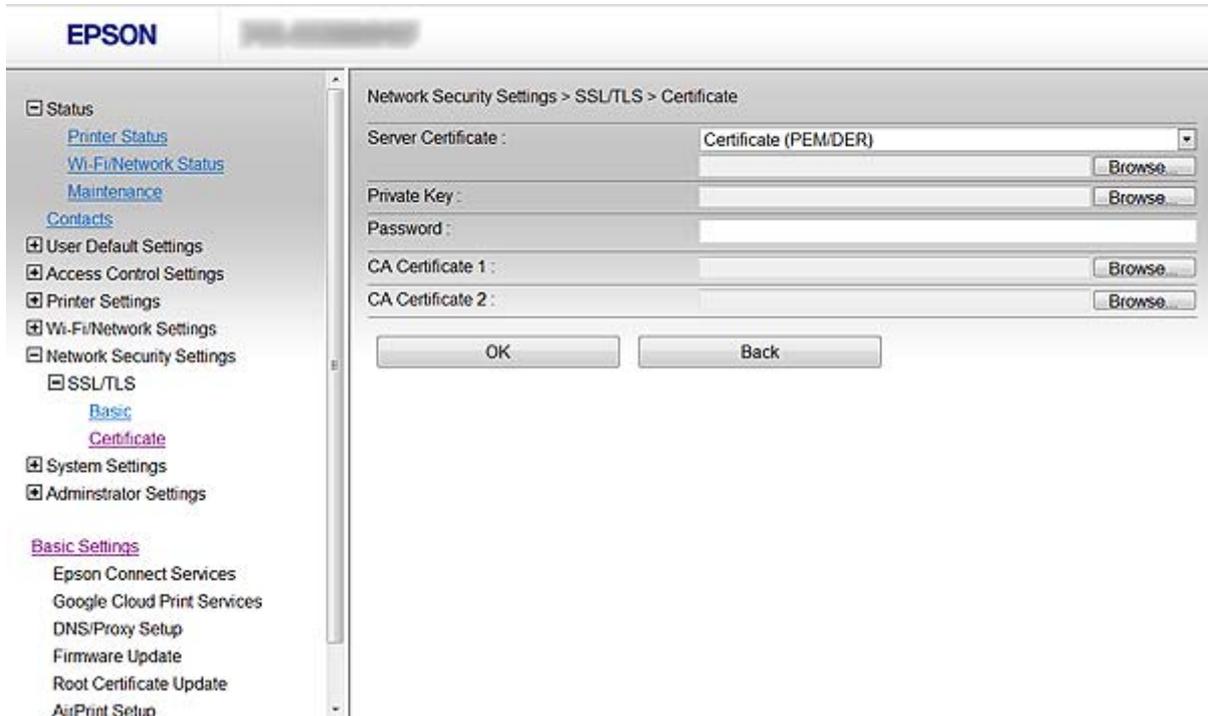
Items	Settings and Explanation
Server Certificate	Select a certificate's format.
Private Key	If you obtain a certificate of the PEM/DER format by using a CSR created from a computer, specify a private key file that is match a certificate.
Password	Enter a password to encrypt a private key.
CA Certificate 1	If your certificate's format is **Certificate (PEM/DER)**, import a certificate of a certificate authority that issues a server certificate. Specify a file if you need.
CA Certificate 2	If your certificate's format is **Certificate (PEM/DER)**, import a certificate of a certificate authority that issues **CA Certificate 1**. Specify a file if you need.

Related Information

Deleting a CA-signed Certificate

You can delete an imported certificate when the certificate has expired or when an encrypted connection is no longer necessary.

> ⚠ *Important:*
>
> *If you obtain a certificate using a CSR created from Web Config, you cannot import a deleted certificate again. In this case, create a CSR and obtain a certificate again.*

1. Access the printer's Web Config and select **Network Security Settings** > **SSL/TLS**, **IPsec/IP Filtering** or **IEEE802.1X** > **Certificate**.

2. Click **Delete**.

   A confirmation message is displayed.

3. Click **OK**.

Related Information

➡

Updating a Self-signed Certificate

If the printer supports the HTTPS server feature, you can update a self-signed certificate. When accessing Web Config using a self-signed certificate, a warning message appears.

Use a self-signed certificate temporarily until you obtain and import a CA-signed certificate.

1. Access the printer's Web Config and select **Network Security Settings** > **SSL/TLS** > **Certificate**.

2. Click **Update**.

3. Enter **Common Name**.

   Enter an IP address, or an identifier such as an FQDN name for the printer. You can enter between 1 and 128 characters.

   Note:
   You can separate distinguished name (CN) with commas.

4. Specify a validity period for the certificate.
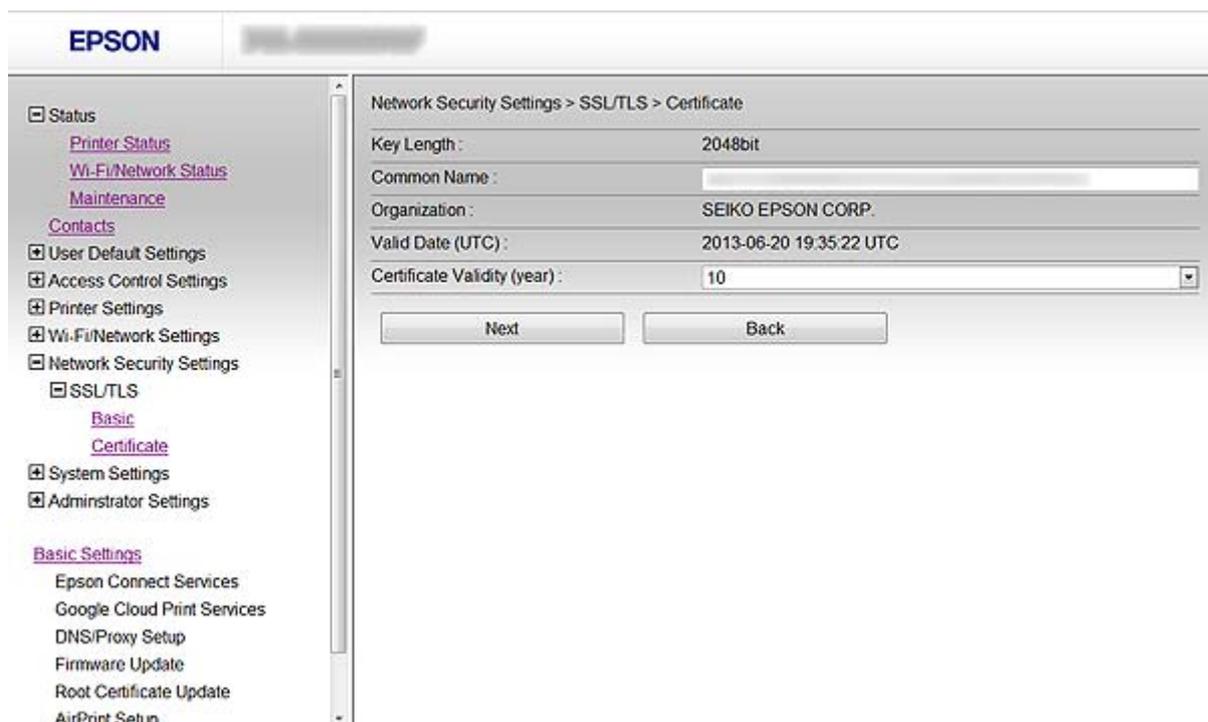
5. Click **Next**.

   A confirmation message is displayed.

6. Click **OK**.

   The printer is updated.

Note:
*Click **Confirm** to verify the certificate information.*

Related Information

➡ "Accessing Web Config" on page 11

Configuring Scan and Fax Destination

Destination Setting Features

You can use the printer's contacts list or the LDAP server to choose the destination for the scan and fax features.

Note:
❏ *The available features may vary by model. For more details, see the printer's documentation.*

❏ *You can switch between your printer's contacts list and the LDAP using the printer's control panel.*

❏ *To use email features, you need to configure a mail server.*

Related Information
➡ "Configuring Contacts" on page 37
➡ "Using the LDAP Server" on page 41
➡ "Using a Mail Server" on page 45

Configuring Contacts

The Contacts list can include the following types of destinations:

❏ **Fax**: Destination for fax

❏ **Email**: Destination for email

❏ **Network Folder (SMB)/FTP**: Destination for scan data and fax forwarding data

Contacts Configuration Comparison

There are three tools for configuring the printer's contacts: Web Config, EpsonNet Config, and the printer's control panel. The differences between three tools are listed in the table below.

Features	Web Config	EpsonNet Config	Printer's control panel
Registering a destination	✓	✓	✓
Editing a destination	✓	✓	✓
Adding a group	✓	✓	✓
Editing a group	✓	✓	✓
Deleting a destination or groups	✓	✓	✓
Deleting all destinations	✓	–	–
Copying destinations or groups	–	✓	–
Importing a file	–	✓	–

Configuring Scan and Fax Destination

Features	Web Config	EpsonNet Config	Printer's control panel
Exporting to a file	–	✓	–

Note:
❏ *EpsonNet Config can import and export information such as contacts lists and user features restriction lists. For more information, see the EpsonNet Config documentation or help menu.*

❏ *You can also configure the fax destination using the FAX Utility.*

Registering a Destination to Contacts

1. Access the printer's Web Config and select **Contacts**.

2. Click **Add** for the number that you want to register.

3. Select the destination type as the **Type** option.

   Note:
   You cannot change the Type option after registration is complete. If you want to change the type, delete the destination and then register again.

4. Select **Next**.

5. Enter a value for each item, and then click **Apply**.

Related Information

➡ "Accessing Web Config" on page 11
➡ "Destination Setting Items" on page 39

Configuring Scan and Fax Destination

Destination Setting Items
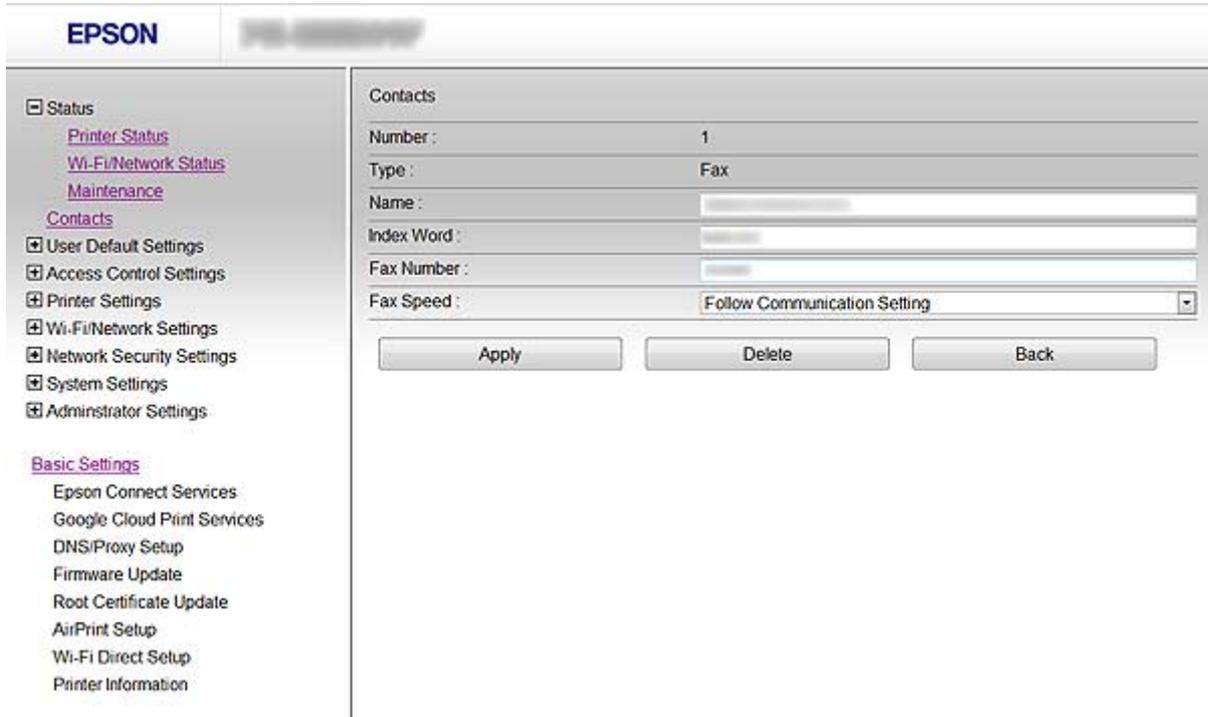
Items	Settings and Explanation
Common Settings	
Name	Enter a name displayed on the contacts between 0 and 30 characters in Unicode (UTF-8).
Index Word	Enter words to search between 0 and 30 characters in Unicode (UTF-8).
Fax	
Fax Number	Enter between 1 and 64 characters using 0-9 - * # and space.
Fax Speed	Select a communication speed for a destination.
Email	
Email Address	Enter between 1 and 255 characters using A-Z a-z 0-9 ! # $ % & ' * + - . / = ? ^ _ {	} ~ @.
Network Folder (SMB)	
Save to	Enter the location where the target folder is located between 1 and 253 characters in Unicode (UTF-8), omitting "\\".
User Name	Enter a user name to access to a network folder between 0 and 30 characters in Unicode (UTF-8).
Password	Enter a password to access to a network folder between 0 and 20 characters in Unicode (UTF-8).
FTP	

Configuring Scan and Fax Destination

Items	Settings and Explanation
Save to	Enter the server name between 1 and 253 characters in ASCII (0x20-0x7E), omitting "ftp://".
User Name	Enter a user name to access to an FTP server between 0 and 30 characters in Unicode (UTF-8). If the server allows anonymous connections, enter a user name such as Anonymous and FTP.
Password	Enter a password to access to an FTP server between 0 and 20 characters in Unicode (UTF-8).
Connection Mode	Select the connection mode from the menu. If a firewall is set between the printer and the FTP server, select **Passive Mode**.
Port Number	Enter the FTP server port number between 1 and 65535.

Related Information

➡

Registering Destinations as a Group

If the destination type is set to **Fax** or **Email**, you can register the destinations as a group.

1. Access the printer's Web Config and select **Contacts**.

2. Click **Add** for the number that you want to register.

3. Select a group from **Type**.

4. Click **Next**.

   The available destinations are displayed.

5. Enter a **Name** and **Index Word**.

6. Select destinations that you want to register from the listed contacts.
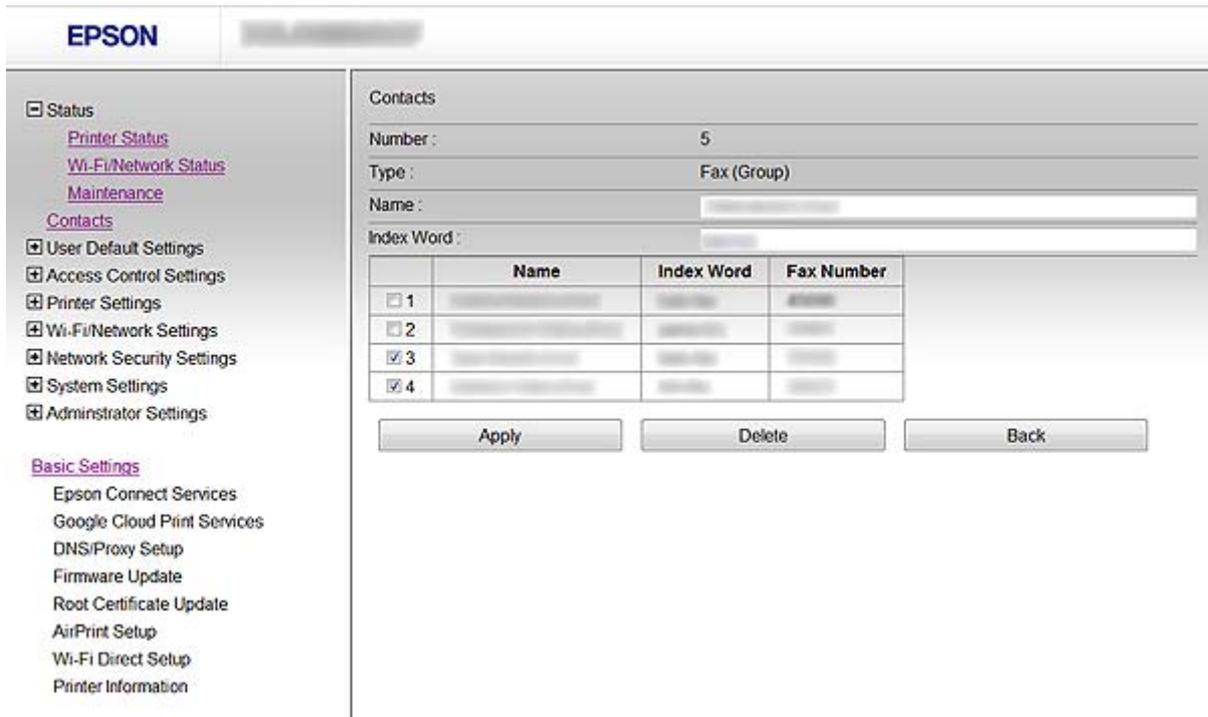
Note:
Destinations can be registered to multiple groups.

7. Click **Apply**.

Related Information

➡ "Accessing Web Config" on page 11

Using the LDAP Server

You can use the LDAP server to provide fax and email destination information. You need to configure the search settings before using the information on your LDAP server.

Configuring the LDAP Server

1. Access the printer's Web Config and select **Wi-Fi/Network Settings** > **LDAP Server** > **Basic**.

2. Enter a value for each item.

3. Select **OK**.

   The settings you have selected are displayed.

Related Information

➡ "Accessing Web Config" on page 11
➡ "LDAP Server Setting Items" on page 42

Configuring Scan and Fax Destination

LDAP Server Setting Items

Items	Settings and Explanation
Connection Settings	
Use LDAP Server	Select **Use** or **Do Not Use**.
LDAP Server Address	Enter the address of the LDAP server. Enter between 1 and 255 characters of either IPv4, IPv6, or FQDN format. For the FQDN format, you can use alphanumeric characters in ASCII (0x20-0x7E) and "- " except for the beginning and end of the address.
LDAP server Port Number	Enter the LDAP server port number between 1 and 65535.
Search Timeout (sec)	Set the length of time for searching before timeout occurs between 5 and 300.
Authentication Method	Select one of the methods.
User Name	Enter the user name for the LDAP server between 0 and 128 characters in Unicode (UTF-8). You cannot use the control characters, such as 0x00-0x1F and 0X7F. This setting is not used when **Anonymous Authentication** is selected as the **Authentication Method**.
Password	Enter the password for the LDAP server authentication between 0 and 128 characters in Unicode (UTF-8). You cannot use the control characters, such as 0x00-0x1F and 0X7F. This setting is not used when **Anonymous Authentication** is selected as the **Authentication Method**.
Kerberos Settings	
If you select **Kerberos Authentication** for **Authentication Method**, enter a value for each item:	
Kerberos Server Address	Enter the address of the Kerberos authentication server. Enter between 1 and 255 characters in either IPv4, IPv6 or FQDN format.

Configuring Scan and Fax Destination

Items	Settings and Explanation
Kerberos Server Port Number	Enter the Kerberos server port number between 1 and 65535.
Kerberos Server Realm	Enter the realm of the Kerberos authentication between 0 and 255 characters in ASCII (0x20-0x7E).

Related Information

➡

Configuring the LDAP Server Search Settings

1. Access the printer's Web Config and select **Wi-Fi/Network Settings** > **LDAP Server** > **Search Settings**.

2. Enter a value for each item.
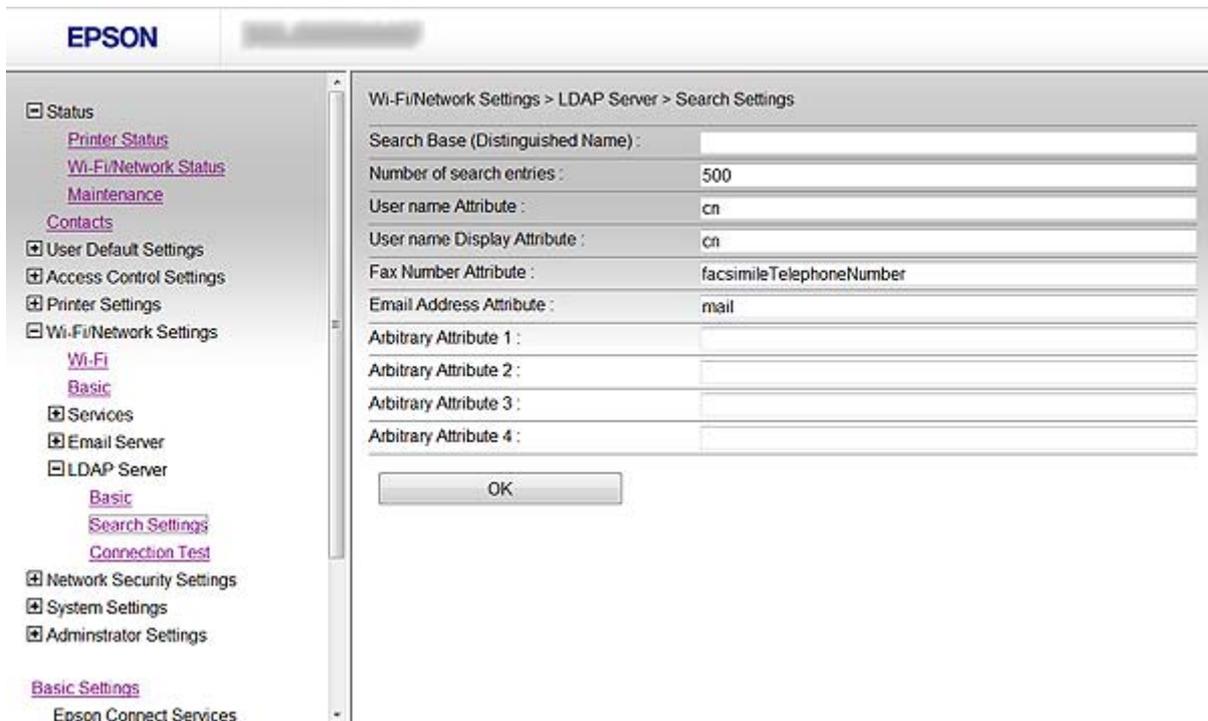
3. Click **OK** to display the setting result.

   The settings you have selected are displayed.

Related Information

➡
➡

LDAP Server Search Setting Items

Configuring Scan and Fax Destination

Items	Settings and Explanation
Search Base (Distinguished Name)	If you want to search an arbitrary domain, specify the domain name of the LDAP server. Enter between 0 and 128 characters in Unicode (UTF-8). If you do not search for arbitrary attribute, leave this blank. Example for the local server directory: dc=server,dc=local
Number of search entries	Specify the number of search entries between 5 and 500. The specified number of the search entries is saved and displayed temporarily. Even if the number of the search entries is over the specified number and an error message appears, the search can be completed.
User name Attribute	Specify the attribute name to display when searching for user names. Enter between 1 and 255 characters in Unicode (UTF-8). The first character should be a-z or A-Z. Example: cn, uid
User name Display Attribute	Specify the attribute name to display as the user name. Enter between 0 and 255 characters in Unicode (UTF-8). The first character should be a-z or A-Z. Example: cn, sn
Fax Number Attribute	Specify the attribute name to display when searching for fax numbers. Enter a combination of between 1 and 255 characters using A-Z, a-z, 0-9, and -. The first character should be a-z or A-Z. Example: facsimileTelephoneNumber
Email Address Attribute	Specify the attribute name to display when searching for email addresses. Enter a combination of between 1 and 255 characters using A-Z, a-z, 0-9, and -. The first character should be a-z or A-Z. Example: mail
Arbitrary Attribute 1 - Arbitrary Attribute 4	You can specify other arbitrary attributes to search for. Enter between 0 and 255 characters in Unicode (UTF-8). The first character should be a-z or A-Z. If you do not want to search for arbitrary attributes, leave this blank. Example: o, ou

Related Information

➡ "Configuring the LDAP Server Search Settings" on page 43

Checking the LDAP Server Connection

1. Access the printer's Web Config and select **Wi-Fi/Network Settings** > **LDAP Server** > **Connection Test**.

2. Select **Start**.

   The connection test is started. After the test, the check report is displayed.

Related Information

➡ "Accessing Web Config" on page 11
➡ "LDAP Server Connection Test References" on page 45

LDAP Server Connection Test References

Messages	Explanation
Connection test was successful.	This message appears when the connection with the server is successful.
Connection test failed. Check the settings.	This message appears for the following reasons: ❏ The LDAP server address or the port number is incorrect. ❏ A timeout has occurred. ❏ **Do Not Use** is selected as the **Use LDAP Server**. ❏ If **Kerberos Authentication** is selected as the **Authentication Method**, settings such as **Kerberos Server Address**, **Kerberos Server Port Number** and **Kerberos Server Realm** are incorrect.
Connection test failed. Check the date and time on your printer or server.	This message appears when the connection fails because the time settings for the printer and the LDAP server are mismatched.
Authentication failed. Check the settings.	This message appears for the following reasons: ❏ **User Name** and/or **Password** is incorrect. ❏ If **Kerberos Authentication** is selected as the **Authentication Method**, the time/date may not be configured.
Cannot access the printer until processing is complete.	This message appears when the printer is busy.

Related Information

➡

Using a Mail Server

If you want to send scan and fax data by email or if you want to use the email notification feature, you need to configure a mail server.

Configuring a Mail Server

1. Access the printer's Web Config and select **Wi-Fi/Network Settings** > **Email Server** > **Basic**.

2. Enter a value for each item.

3. Select **OK**.

    The settings you have selected are displayed.

Related Information

➡
➡

Configuring Scan and Fax Destination

Mail Server Setting Items

Items	Settings and Explanation	
Authentication Method	Specify the authentication method for the printer to access the mail server.	
	Off	Authentication is disabled when communicating with a mail server.
	SMTP AUTH	Requires that a mail server supports SMTP Authentication.
	POP before SMTP	Configure the POP3 server when selecting this method.
Authenticated Account	If you select **SMTP AUTH** or **POP before SMTP** as the **Authentication Method**, enter the authenticated account name between 0 and 30 characters in ASCII (0x20-0x7E).	
Authenticated Password	If you select **SMTP AUTH** or **POP before SMTP** as the **Authentication Method**, enter the authenticated password between 0 and 20 characters using A-Z a-z 0-9 ! # $ % & ' * + - . / = ? ^ _ {	} ~ @.	
Sender's Email Address	Enter the sender's email address. Enter between 0 and 255 characters in ASCII (0x20-0x7E) except for : ( ) < > [ ] ; ¥. A period "." cannot be the first character.	
SMTP Server Address	Enter between 0 and 255 characters using A-Z a-z 0-9 . - . You can use IPv4 or FQDN format.	
SMTP Server Port Number	Enter a number between 1 and 65535.	
POP3 Server Address	If you select **POP before SMTP** as the **Authentication Method**, enter the POP3 server address between 0 and 255 characters using A-Z a-z 0-9 . - . You can use IPv4 or FQDN format.	
POP3 Server Port Number	If you select **POP before SMTP** as the **Authentication Method**, enter a number between 1 and 65535.	

46

Related Information

➡

Checking a Mail Server Connection

1. Access the printer's Web Config and select **Wi-Fi/Network Settings** > **Email Server** > **Connection Test**.

2. Select **Start**.

   The connection test is started. After the test, the check report is displayed.

Related Information

➡

➡

Mail Server Connection Test References

Messages	Explanation
Connection test was successful.	This message appears when the connection with the server is successful.
Connection test failed. Check the settings.	This message appears for the following reasons: ❑ The mail server address or the port number is incorrect. ❑ A timeout has occurred.
Cannot access the printer until processing is complete.	This message appears when the printer is busy.

Related Information

➡

Restricting Available Features and Configuring the Administrator Password

User Features Restriction

You can create up to 10 unique users and restrict available printer features for each user. Users have to log in with a username and password using the printer's control panel. Users can log out manually or the printer will log them out automatically after a period of time.

If you want to restrict printing from the printer driver and the scanner driver, use the dedicated driver for the printer.

If you use the printer from a Windows computer, you can assign the user name and password to the printer driver and the scanner driver in advance. The printer will authenticate the user automatically when using the computer and you will not need to enter a password each time. For more information on configuring the driver, see the driver's help.

You cannot use this feature with Mac OS X.

Configuring User Features

1.   Access the printer's Web Config and select **Access Control Settings** > **Basic**.

2. Check the **Enables Access Control** box and click **OK**.

> ❗ *Important:*
>
> *If you un-check the **Allows printing and scanning without authentication information** box, unauthenticated jobs sent from the following sources will not be received:*
>
> ❑ *The OS default driver*
>
> ❑ *The PCL printer driver/ PostScript printer driver*
>
> ❑ *Web services such as Epson Connect and Google Cloud Print*
>
> ❑ *Smartphones and other mobile devices*
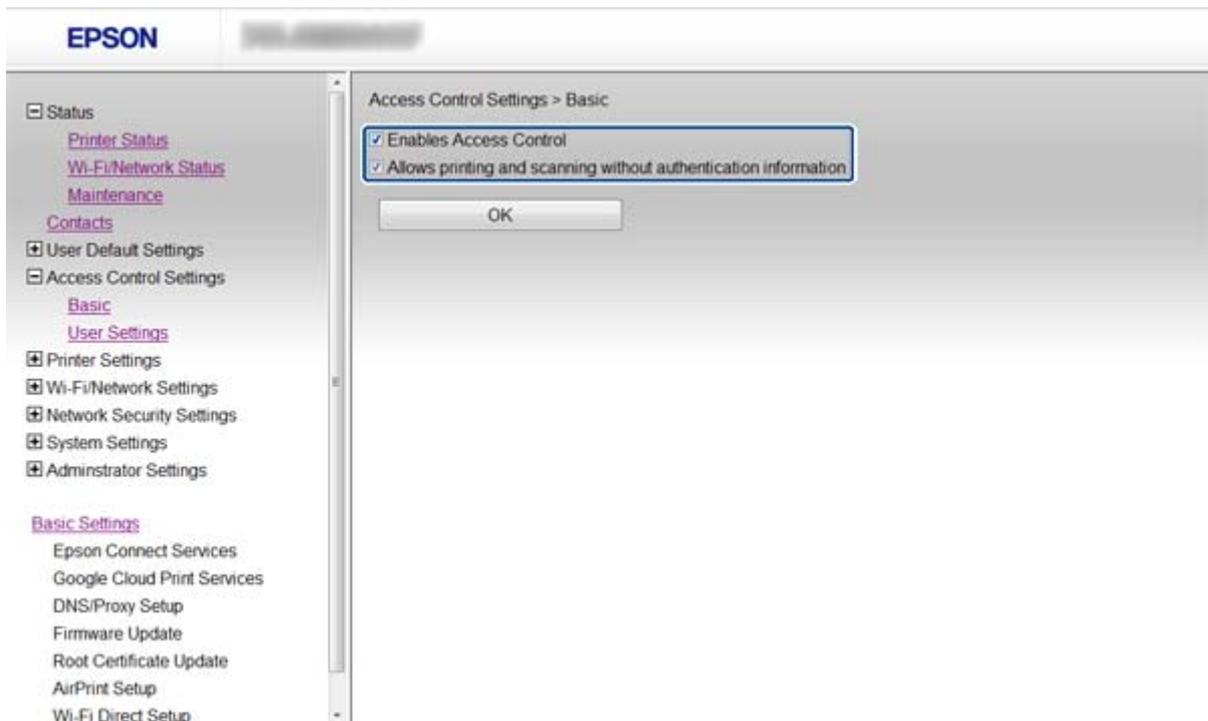
3. Select **Access Control Settings** > **User Settings**.

4. Click **Add**, then enter a value for each item.

5. Click **Apply**.

   Note:
   ***Delete** is displayed when you edit a registered user. Click it to delete a user.*

   EpsonNet Config can import and export a list of user features. For more information, see the EpsonNet Config documentation or help menu.

Related Information

➡ "Accessing Web Config" on page 11
➡ "User Features Setting Items" on page 50

User Features Setting Items
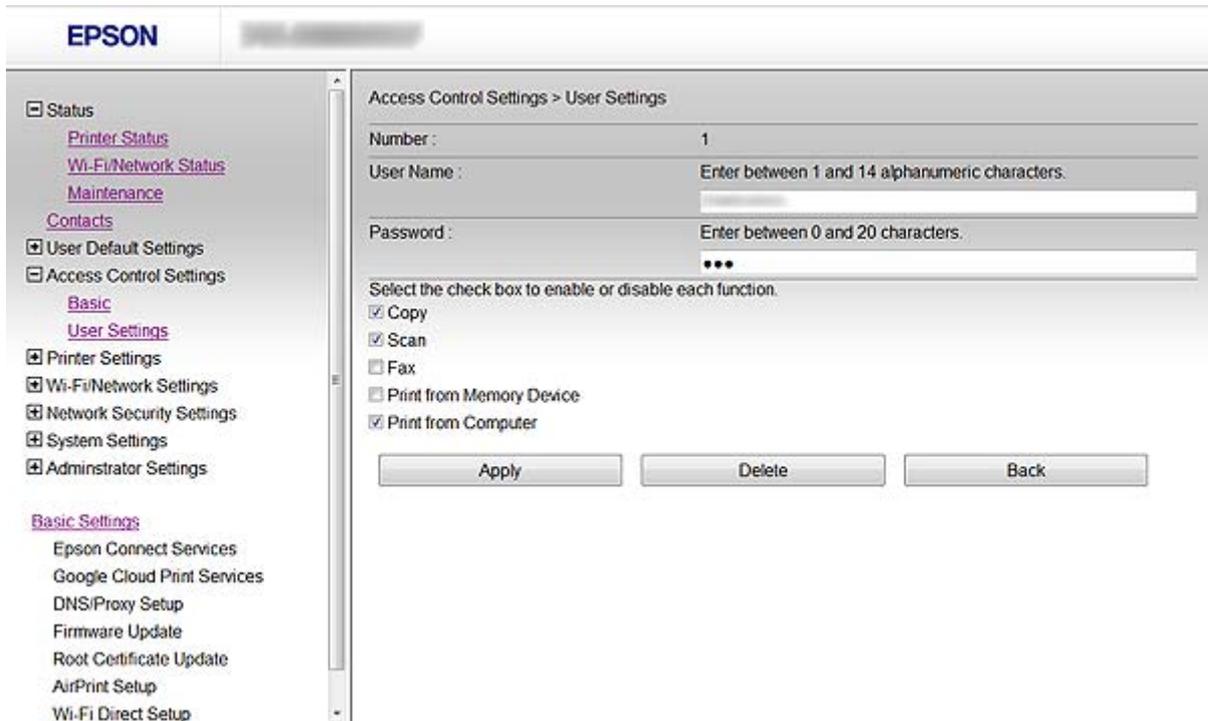
Items	Settings and Explanation
User Name	Enter a display name on the list between 1 and 14 characters in ASCII (0x20-0x7E).
Password	Enter between 0 and 20 characters in ASCII (0x20-0x7E). If you want to restore a password to the default, leave the field blank.
Select the check box to enable or disable each function.	Checked functions are allowed for use.

Related Information

➡

Configuring the Administrator Password

When you set the administrator password, clients will not be able to change the settings.

1. Access the printer's Web Config and select **Administrator Settings** > **Change Administrator Password**.

2. Enter a password to **New Password** and **Confirm New Password**.

   If you want to change the password to new one, enter a current password.
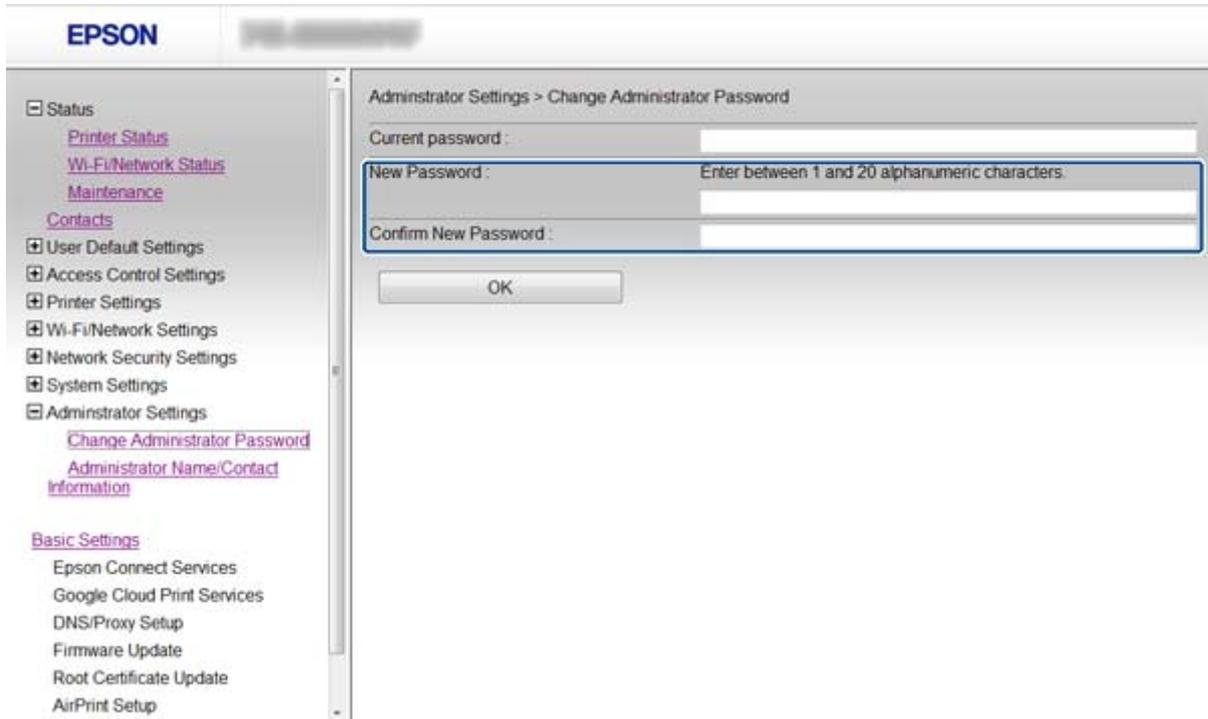
3. Select **OK**.

   Note:
   The administrator password is the same for Web Config, EpsonNet Config and the printer's control panel.

   If you forget the administrator password, contact Epson support. For the contact information, see the printer's documentation.

Related Information

➡

Solving Problems

Tips for Solving Problems

You can find more information in the following manuals.

❏ User's Guide (PDF manual)

Provides instructions on using the printer, replacing ink cartridges, maintenance, and solving problems.

❏ Network Guide (PDF manual)

Provides instructions on network settings for your computer, smartphone or the printer, and solving problems.

❏ Epson Connect portal website

https://www.epsonconnect.com/

Provides information on Epson Connect features and solving problems.

Problems Using Network Software

Cannot Access Web Config

Is the IP address of the printer properly configured?

Configure the IP address using EpsonNet Config or the printer's control panel. You can confirm the current setting information with a network status sheet or from the printer's control panel.

Is the Encryption Strength for SSL/TLS set to High?

If **High** is selected for **Encryption Strength**, Web Config can only be accessed in a browser supporting AES (256-bit) or 3DES (168-bit) encryption. Check your browser's encryption support.

The message "Out of date" appears when accessing Web Config using SSL communication (https).

If the certificate is out of date, obtain the certificate again. If the message appears before its expiration date, make sure that the printer's date is configured correctly.

The message "The name of the security certificate does not match…" appears when accessing Web Config using SSL communication (https).

The printer's IP address entered for **Common Name** for creating a self-signed certificate or CSR does not match with the address entered into the browser. Obtain and import a certificate again or change the printer name.

The printer is being accessed via a proxy server.

If you are using a proxy server with your printer, you need to configure your browser's proxy settings.

❏ Windows:

Select **Control Panel** > **Network and Internet** > **Internet Options** > **Connections** > **LAN settings** > **Proxy server**, and then configure not to use the proxy server for local addresses.

❏ Mac OS X:

Select **System Preferences** > **Network** > **Advanced** > **Proxies**, and then register the local address for **Bypass proxy settings for these Hosts & Domains**.

Example:

192.168.1.*: Local address 192.168.1.XXX, subnet mask 255.255.255.0

192.168.*.*: Local address 192.168.XXX.XXX, subnet mask 255.255.0.0

Related Information

➡

Model name and/or IP address are not displayed on EpsonNet Config

Did you select Block, Cancel, or Shut down when a Windows security screen or a firewall screen was displayed?

If you select **Block**, **Cancel**, or **Shut down**, the IP address and model name will not display on EpsonNet Config or EpsonNet Setup.

To correct this, register EpsonNet Config as an exception using Windows firewall and commercial security software. If you use an antivirus or security program, close it and then try to use EpsonNet Config.

Is the communication error timeout setting too short?

Run EpsonNet Config and select **Tools** > **Options** > **Timeout**, and then increase the length of time for the **Communication Error** setting. Note that doing so can cause EpsonNet Config to run more slowly.

Related Information

➡
➡

Problems Using Network Security Features

Forgot a Pre–shared Key

Configure the key again using Web Config.

To change the key, access the printer's Web Config and select **Network Security Settings** > **IPsec/IP Filtering** > **Default Policy** or **Group Policy**.

Cannot Communicate with IPsec Communication

Are you using an unsupported algorithm for the computer settings?

The printer supports the following algorithms.

Solving Problems

Security Methods	Algorithms
Consistency Algorithm	AES-CBC 128
	AES-CBC 192
	AES-CBC 256
	3DES-CBC
	DES-CBC
Hash Algorithm	SHA-1
	SHA2-256
	SHA2-384
	SHA2-512
	MD5
Algorithm Compatible with a key	Diffie-Hellman Group2
	Diffie-Hellman Group1*, Diffie-Hellman Group14*, Elliptic Curve Diffie-Hellman P-256* and Elliptic Curve Diffie-Hellman P-384*

*Available method may vary by models.

Related Information

➡ "Configuring IPsec/IP Filtering" on page 18

Cannot Communicate Suddenly

Is the printer's IP address invalid or has it changed?

Disable IPsec using the printer's control panel.

If the DHCP is out of date, rebooting or the IPv6 address is out of date or has not been obtained, then the IP address registered for the printer's Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Group Policy** > **Local Address(Printer)**) may not be found.

Use a static IP address.

Is the computer's IP address invalid or has it changed?

Disable IPsec using the printer's control panel.

If the DHCP is out of date, rebooting or the IPv6 address is out of date or has not been obtained, then the IP address registered for the printer's Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Group Policy** > **Remote Address(Host)**) may not be found.

Use a static IP address.

Related Information

➡ "Configuring IPsec/IP Filtering" on page 18

Cannot Create the Secure IPP Printing Port

Is the correct certificate specified as the server certificate for SSL/TLS communication?

If the specified certificate is not correct, creating a port may fail. Make sure you are using the correct certificate.

Is a CA certificate imported to the computer accessing the printer?

If a CA certificate is not imported to the computer, creating a port may fail. Make sure a CA certificate is imported.

Related Information

➡

Cannot Access the Printer after Configuring IEEE802.1X

The settings may be incorrect.

Disable IEEE802.1X and Wi-Fi from the printer's control panel. Connect the printer and a computer, and then configure IEEE802.1X again.

Related Information

➡

Problems on Using a Digital Certificate

Cannot Import a CA-signed Certificate

Does the CA-signed certificate and the information on the CSR match?

If the CA-signed certificate and CSR do not have the same information, the CSR cannot be imported. Check the following:

❏ Are you trying to import the certificate to a device that does not have the same information?

Check the information of the CSR and then import the certificate to a device that has the same information.

❏ Did you overwrite the CSR saved into the printer after sending the CSR to a certificate authority?

Obtain the CA-signed certificate again with the CSR.

Is the CA-signed certificate more than 5KB?

You cannot import a CA-signed certificate that is more than 5KB.

Is the password for importing the certificate correct?

If you forget the password, you cannot import the certificate.

Related Information

➡

Cannot Update a Self-Signed Certificate

Has the Common Name been entered?

Common Name must be entered.

Have unsupported characters been entered to Common Name? For example, Japanese is not supported.

Enter between 1 and 128 characters of either IPv4, IPv6, host name, or FQDN format in ASCII (0x20-0x7E).

Is a comma or space included in the Common Name?

If a comma is entered, the **Common Name** is divided at that point. If only a space is entered before or after a comma, an error occurs.

Related Information

➡ "Updating a Self-signed Certificate" on page 35

Cannot Create a CSR

Has the Common Name been entered?

The **Common Name** must be entered.

Have unsupported characters been entered to Common Name, Organization, Organizational Unit, Locality, State/Province? For example, Japanese is not supported.

Enter characters of either IPv4, IPv6, host name, or FQDN format in ASCII (0x20-0x7E).

Is a comma or space included in the Common Name?

If a comma is entered, the **Common Name** is divided at that point. If only a space is entered before or after a comma, an error occurs.

Related Information

➡ "Obtaining a CA-signed Certificate" on page 31

Warning Relating to a Digital Certificate Appears

Messages	Cause/What to do
Enter a Server Certificate.	**Cause:** You have not selected a file to import. **What to do:** Select a file and click **Import**.

Solving Problems

Messages	Cause/What to do
CA Certificate 1 is not entered.	**Cause:** CA certificate 1 is not entered and only CA certificate 2 is entered. **What to do:** Import CA certificate 1 first.
Invalid value below.	**Cause:** Unsupported characters are contained in the file path and/or password. **What to do:** Make sure that the characters are entered correctly for the item.
Invalid date and time.	**Cause:** Date and time for the printer have not been set. **What to do:** Set date and time using Web Config, EpsonNet Config or the printer's control panel.
Invalid password.	**Cause:** The password set for CA certificate and entered password do not match. **What to do:** Enter the correct password.
Invalid file.	**Cause:** You are not importing a certificate file in X509 format. **What to do:** Make sure that you are selecting the correct certificate sent by a trusted certificate authority.
	Cause: The file you have imported is too large. The maximum file size is 5KB. **What to do:** If you select the correct file, the certificate might be corrupted or fabricated.
	Cause: The chain contained in the certificate is invalid. **What to do:** For more information on the certificate, see the website of the certificate authority.
Cannot use the Server Certificates that include more than three CA certificates.	**Cause:** The certificate file in PKCS#12 format contains more than 3 CA certificates. **What to do:** Import each certificate as converting from PKCS#12 format to PEM format, or import the certificate file in PKCS#12 format that contains up to 2 CA certificates.

Solving Problems

Messages	Cause/What to do
The certificate has expired. Check if the certificate is valid, or check the date and time on your printer.	**Cause:** The certificate is out of date. **What to do:** ❏ If the certificate is out of date, obtain and import the new certificate. ❏ If the certificate is not out of date, make sure the printer's date and time are set correctly.
Private key is required.	**Cause:** There is no paired private key with the certificate. **What to do:** ❏ If the certificate is the PEM/DER format and it is obtained from a CSR using a computer, specify the private key file. ❏ If the certificate is the PKCS#12 format and it is obtained from a CSR using a computer, create a file that contains the private key.
	Cause: You have re-imported the PEM/DER certificate obtained from a CSR using Web Config. **What to do:** If the certificate is the PEM/DER format and it is obtained from a CSR using Web Config, you can only import it once.
Setup failed.	**Cause:** Cannot finish the configuration because the communication between the printer and computer failed or the file cannot be read by some errors. **What to do:** After checking the specified file and communication, import the file again.

Related Information

➡ "About Digital Certification" on page 30

Delete a CA-signed Certificate by Mistake

Is there a backup file for the certificate?

If you have the backup file, import the certificate again.

If you obtain a certificate using a CSR created from Web Config, you cannot import a deleted certificate again. Create a CSR and obtain a new certificate.

Related Information

➡ "Deleting a CA-signed Certificate" on page 34

Printing Problems

Cannot Print with AirPrint

Is AirPrint disabled?

To enable AirPrint, access the printer's Web Config and select **AirPrint Setup** and then click **Enable AirPrint**.

Printed Random Characters

Is the setting for the print port correct?

Make sure that the print port of the installed driver and the printer match.

Related Information

Appendix

## Receiving Email Notifications When Events Occur

About Email Notifications

You can use this feature to receive alerts by email when events occur, such as your printer running out of paper. You can register up to 5 email addresses and choose which events you want to receive notifications for.

Configuring Email Notification

To use the feature, you need to configure a mail server.

1. Access the printer's Web Config and select **Administrator Settings** > **Email Notification**.

2. Enter an email address that you want to receive email notifications.

3. Select the language for the email notifications.

4. Check the boxes for the notifications you want to receive.
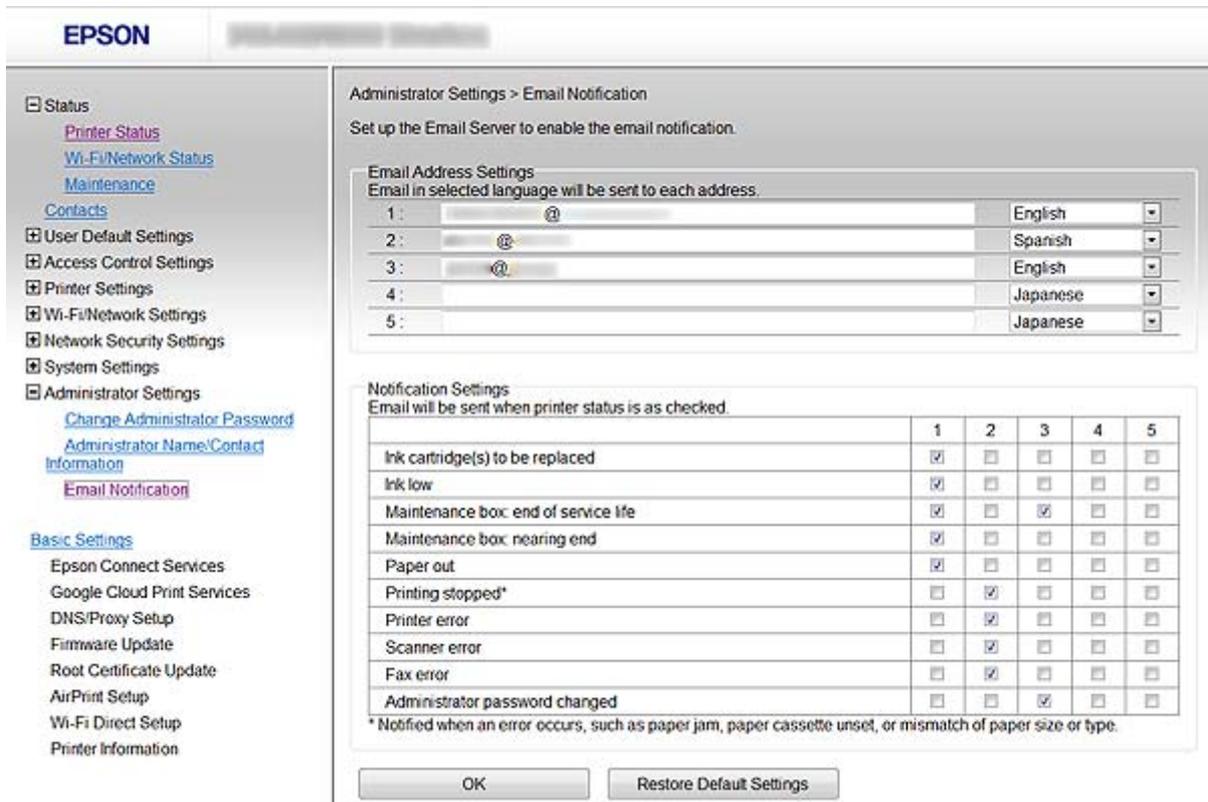
5. Click **OK**.

Appendix

Related Information

Configuring a Network for the Printer Individually

If you want to configure a network setup to the printer individually, use the installer on the software disc that came with the printer or the website for a product setup. For more information, see the printer's documentation.

Configuring a Network Interface - Ethernet

Follow the steps to configure the printer's IP address using EpsonNet Config.

1. Turn on the printer.

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

3. Run EpsonNet Config.

   Connected printer(s) are displayed. It may take some time for all available printers to show up.
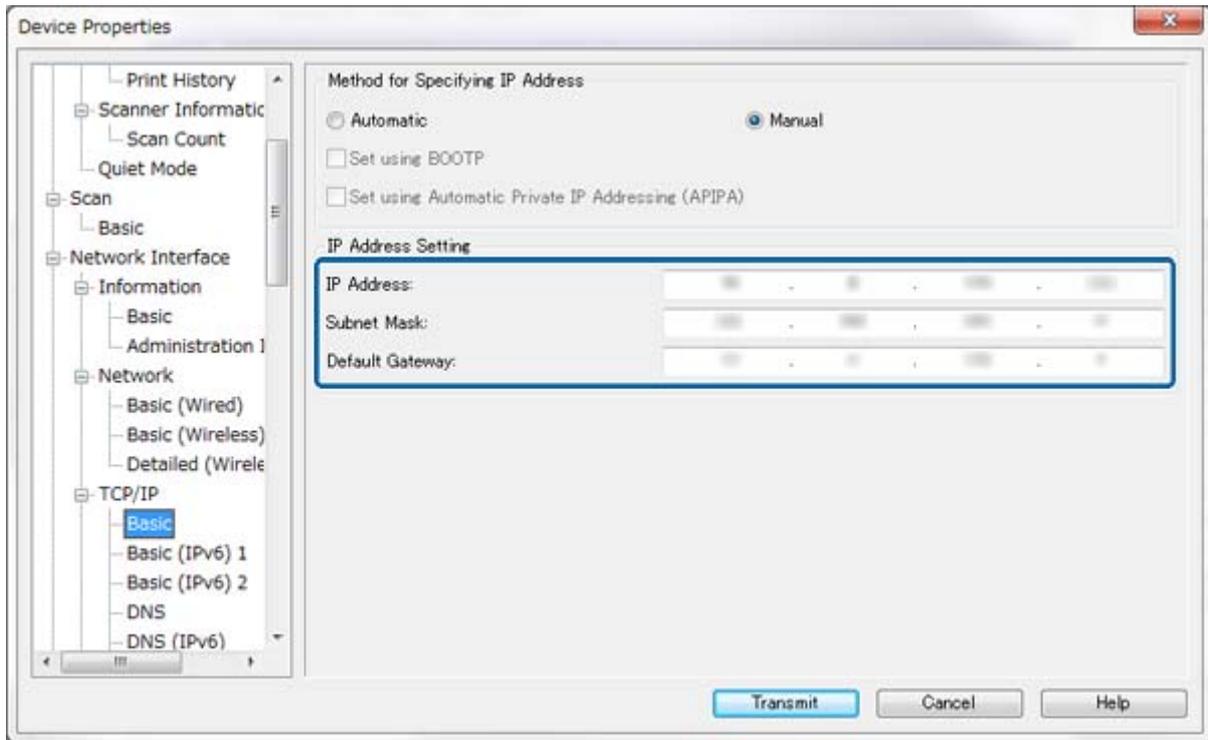
4. Double-click the printer.

   Note:
   You can identify the printer by a MAC address even if multiple printers of the same model are connected.

5. Select **Network Interface** > **TCP/IP** > **Basic** from the menu on the left.

6. Configure **IP Address**, **Subnet Mask**, and **Default Gateway**.

Note:
❏ *If you want to connect the printer to a secure network, configure a static IP address.*

❏ *You can also configure the DNS settings in the **DNS** section and the proxy settings in the **Internet** section of the **TCP/IP** menu.*

7. Click **Transmit**.

Related Information

➡
➡

Configuring a Network Interface - Wi-Fi

Follow the steps to configure the printer's IP address using EpsonNet Config.

1. Turn on the printer.

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

3. Run EpsonNet Config.

   Connected printer(s) are displayed. It may take a while for all available printer to be showed up.

4. Double-click the printer.

   Note:
   You can identify the printer by a MAC address even if multiple printers of the same model are connected.

Appendix

5. Select **Network Interface** > **TCP/IP** > **Basic** from the menu on the left.

6. Configure **IP Address**, **Subnet Mask**, and **Default Gateway**.
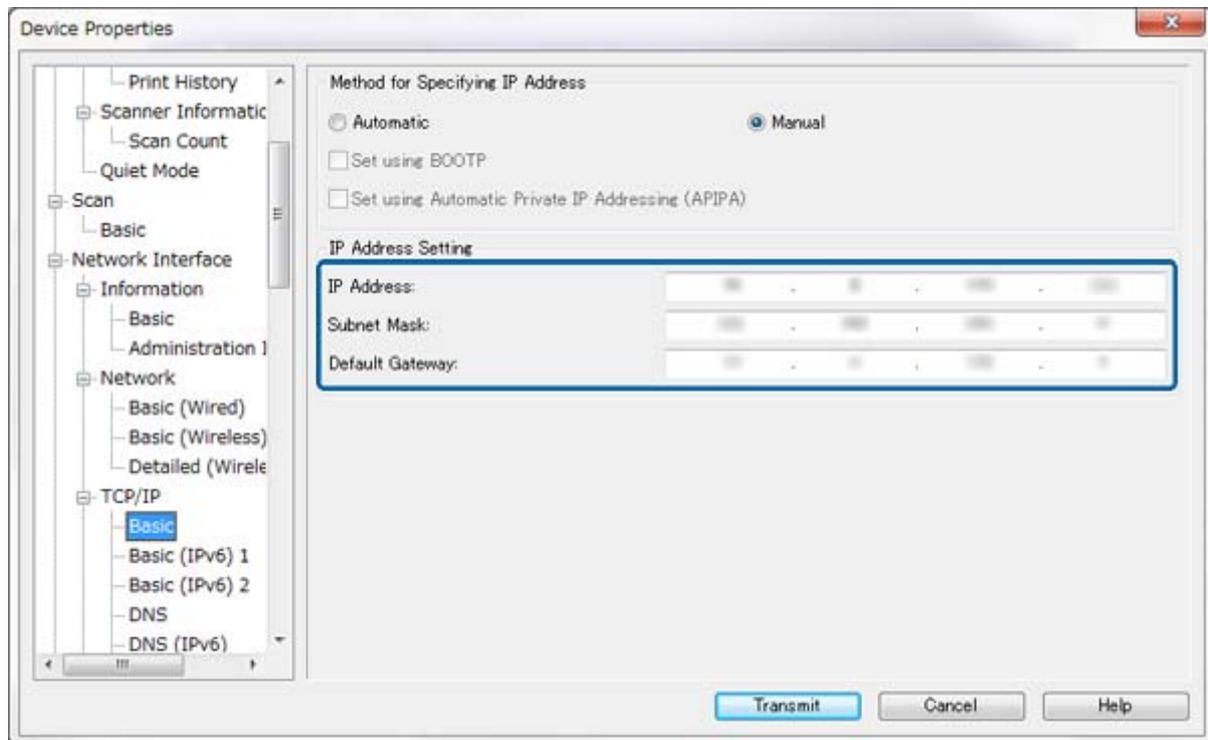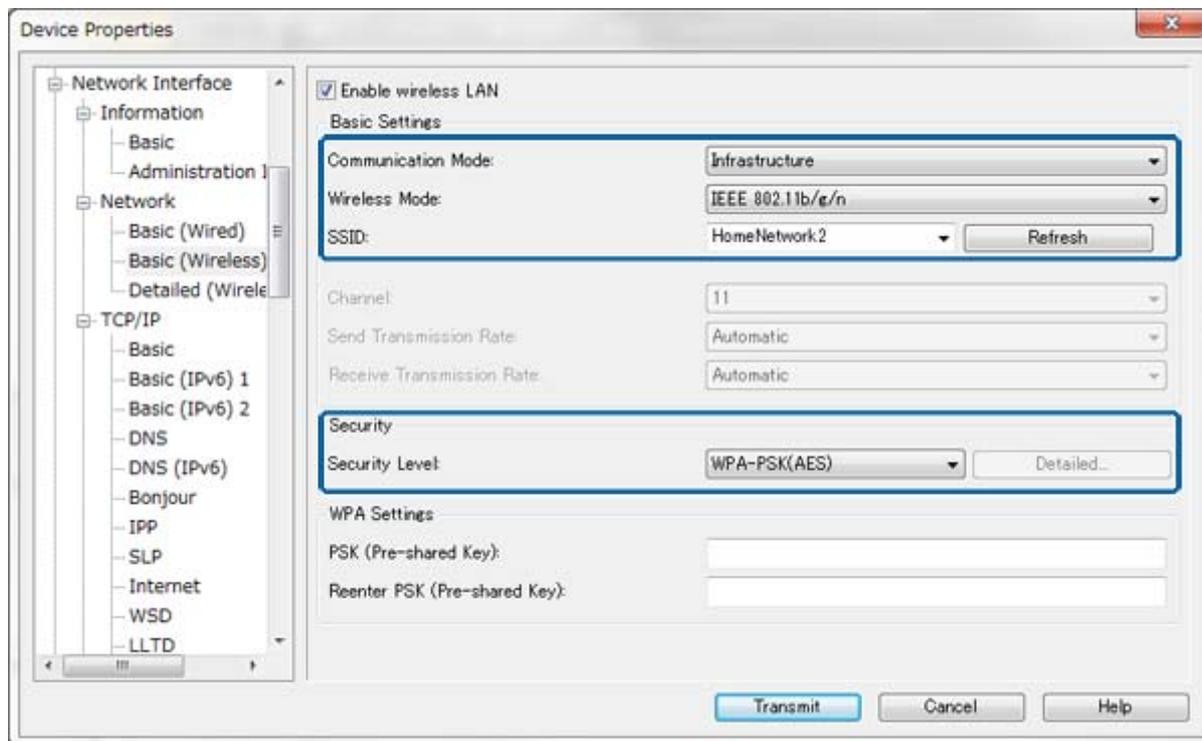

Note:

❏ *If you want to connect the printer to a secure network, configure a static IP address.*

❏ *You can also configure the DNS settings in the **DNS** section and the proxy settings in the **Internet** section of the **TCP/IP** menu.*

Appendix

7. Select **Network Interface** > **Network** > **Basic (Wireless)**, and then configure a communication mode, SSID and security.

8. Click **Transmit**.

    Confirm that a Wi-Fi connection is enabled with the printer and then disconnect the Ethernet cable.

Related Information

➡
➡

Configuring a Computer Connected to the Printer

Installing the Printer Driver - Windows

Install the printer driver to configure a printer port.

If the printer supports the PostScript or PCL and you want to install the Epson PostScript printer driver or PCL printer driver, see the printer's documentation.

1. Turn on the printer.

2. Install the printer driver on a computer.

    The printer drivers are located on the software disc that came with the printer.

    ❏ 32-bit Windows: \Driver\Printer\Driver\WINX86\setup

    ❏ 64-bit Windows: \Driver\Printer\Driver\WINX64\setup

    Double-click Setup.exe or Setup64.exe to start installing the driver. Follow the on-screen instructions.

Note:
If you do not have the software disc or if a computer does not have a disc drive, download the driver from the Epson support website.

Related Information

➡ "Configuring a Network Interface - Ethernet" on page 61

➡ "Configuring a Network Interface - Wi-Fi" on page 62

➡ "Restricting Available Features and Configuring the Administrator Password" on page 48

➡ "Configuring to Share the Printer - Windows" on page 68

Installing the Printer Driver - Mac OS X

Add the printer and install the printer driver to a computer via the Internet. Make sure the computer has an Internet connection.

If the printer supports the PostScript and you want to install the Epson PostScript printer driver, see the printer's documentation.

1. Turn on the printer.

2. Select **System Preferences** > **Print & Scan**.

3. Select **+** > **Add Printer or Scanner**.

4. Make sure the **Default** is selected, and then select the printer that you want to add from the list.

5. Specify a product name for **Driver**, and then select **Add**.

   The printer driver is downloaded automatically and the printer is added.

   Note:
   ❏ *If the installation of the driver does not start, download the driver manually from the Epson support website. If you are using Mac OS X 10.5.8, the driver is not installed automatically. You must download it from the Epson support website.*

   ❏ *Do not specify driver names with "AirPrint" and "Secure AirPrint", or the driver will not be installed.*

Related Information

➡ "Configuring a Network Interface - Ethernet" on page 61

➡ "Configuring a Network Interface - Wi-Fi" on page 62

Using the Scanner on a Network

Install the scanner driver on the computer to use the scanner on the network.

1. Install EPSON Scan.

   ❏ Windows: The scanner driver is located on the software disc that came with the printer.

      \Driver\Scanner\Driver

Note:
❏ *For Windows Server 2008 or later, the additional installation of Desktop Experience is required before installing EPSON Scan.*

❏ *If you do not have the software disc or if a computer does not have a disc drive, download the driver from the Epson support website.*

❏ *Mac OS X: Download EPSON Scan using EPSON Software Updater or from the Epson support website, and then install it.*

2. Run EPSON Scan Settings.

   ❏ Windows: Select **All Programs** > **EPSON** > **EPSON Scan** > **EPSON Scan Settings**.

   ❏ Mac OS X: Select **Go** > **Applications** > **Epson Software** > **EPSON Scan Settings**.

3. Select the scanner from **Select Scanner** and select **Network** for **Connection**, and then click **Add**.
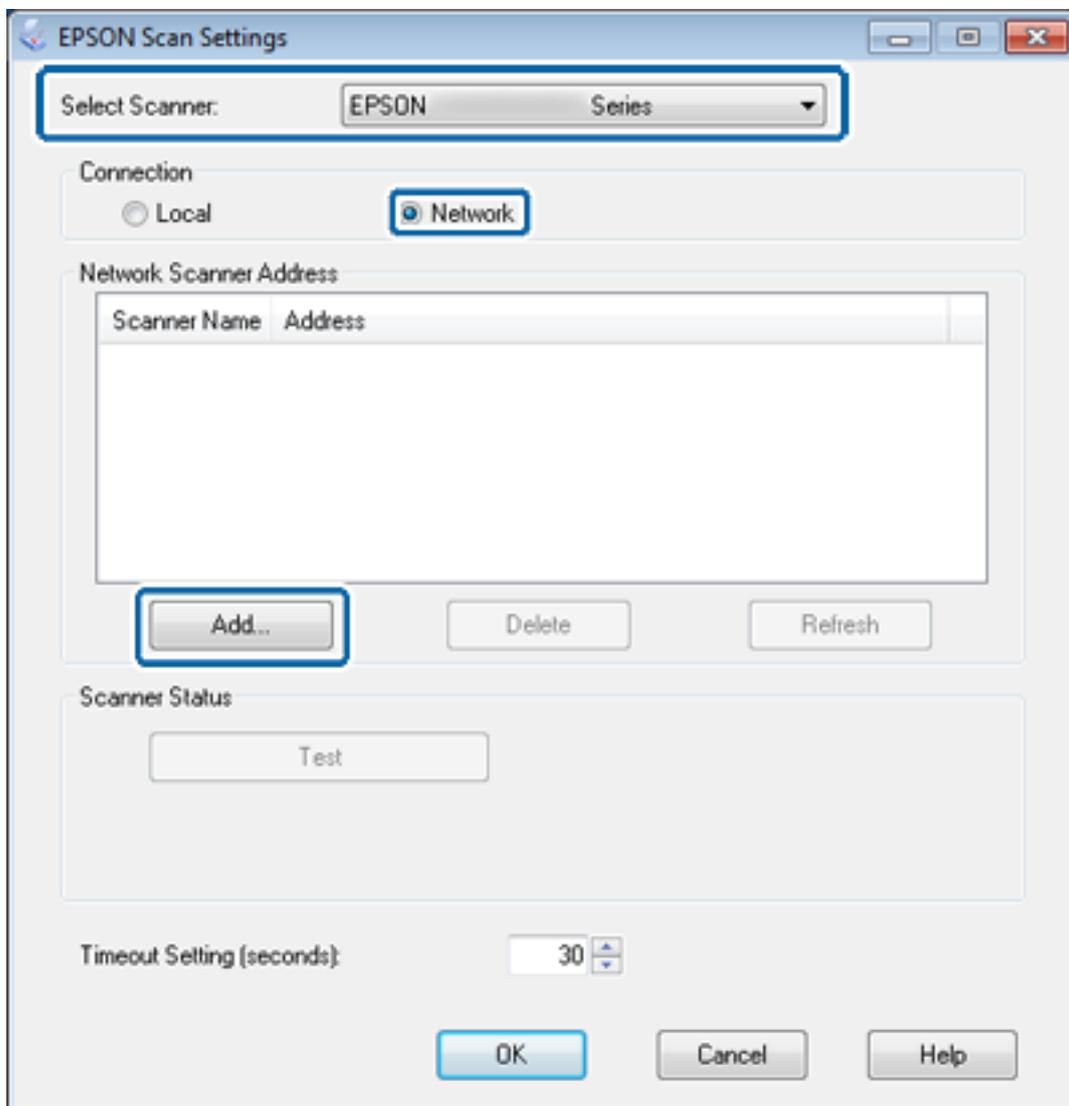
The **Add** screen is displayed and scanner(s) connected to the network are listed.

4. Select the IP address of the scanner that you want to use, and then click **OK**.

   Note:
   Only scanners in the local network can be used.

5. Select the IP address, and then click **Test**.

   If the completion message is displayed, connection of the scanner and computer is successfully complete.

6. Click **OK**.

Related Information

➡ "Restricting Available Features and Configuring the Administrator Password" on page 48

Mapping an External Storage as a Network Drive

Mapping an External Storage as a Network Drive - Windows

1. Check the name and IP address for the printer with an external storage device that you want to share.

   You can check them using Web Config, EpsonNet Config and the printer's control panel.

2. Select **Run**.

3. Enter the printer name in **Open:** in the following format, and then click **OK**.

   \\printername or \\xxx.xxx.xxx.xxx (the printer's IP address)

4. Right-click the **memorycard** icon or **usbstorage** icon, and then click **Map Network Drive**.

5. Select the **Drive** that you want to map.

   Note:
   If you want to use a network drive every time you start up a computer, select **Reconnect at logon**.

6. Click **Finish**.

   The mapped network drive is displayed on **My computer** or **Computer** as a hard disk.

Mapping an External Storage as a Network Drive - Mac OS X

1. Select **Go** > **Connect to Server**.

2. Enter the printer name or the printer's IP address in the **Server Address** field in the following format.

   cifs://printername or

   smb://printername

3. Click **Connect**.

   Note:
   Before you remove the storage device, always drag the removable disk icon on your desktop into the trash otherwise contents may not be displayed correctly when you insert another device.

Appendix

Configuring to Share the Printer - Windows

Sharing the Printer

If you want to use a computer connected to the printer as a print server, share the printer with the computer you want use a server connected to it.

1. Select **Control Panel** > **View devices and printers**.

2. Right-click the printer icon, click **Printer Properties** > **Sharing** tab.

3. Select **Share this printer**, and then enter to **Share name**.

   For Windows Server 2012, click **Change Sharing Options** and then configure the settings.

Related Information

➡

Installing Additional Drivers

If the Windows versions of a print server and clients are different, you should install additional drivers to the print server so that users do not have to find a printer driver when they connect to the shared printer.

1. Select **Control Panel** > **View devices and printers**.

2. Right-click the printer icon that you want to share with the clients, and then click **Printer Properties** > **Sharing** tab.

3. Click **Additional Drivers**.

   Note:
   *For Windows Server 2012, click **Change Sharing Options** and then configure the settings.*

4. Select versions of Windows for clients, and then click **OK**.

Related Information

➡

Using the Shared Printer

Using the Shared Printer – Windows

The administrator needs to inform the clients of the computer name assigned to the print server and how to add it to their computers.

If additional driver(s) have already been configured on the print server, follow these steps:

1. Select the name assigned to the print server in **Windows Explorer**.

Appendix

2.   Double-click the printer that you want to use.

Note:
*If the additional driver(s) have not been configured yet, inform the clients how to use **Devices and Printers** to add the shared printer.*

Related Information

➡
➡

Using the Shared Printer – Mac OS X

Add the printer and install the printer driver via the Internet. Make sure the computer has an Internet connection.

If the printer supports the PostScript and you want to install the Epson PostScript printer driver, see the printer's documentation.

1.   Turn on the printer.

2.   Select **System Preferences** > **Print & Scan**.

3.   Select **+** > **Add Printer or Scanner**.

4.   Make sure the **Default** is selected, and then select the printer that you want to add from the list.

5.   Specify a product name for **Driver**, and then select **Add**.

The printer driver is downloaded automatically and the printer is added.

Note:
❏ *If the installation of the driver does not start, download the driver manually from the Epson support website. If you are using Mac OS X 10.5.8, the driver is not installed automatically. You must download it from the Epson support website.*

❏ *Do not specify driver names with "**AirPrint**" and "**Secure AirPrint**", or the driver will not be installed.*