EPSON
EXCEED YOUR VISION

Administrator's Guide

Contents

Copyright

Trademarks

About this Manual

Introduction

Printer Settings and Management

Network Connection

Function Settings

Product Security Settings

Operation and Management Settings

Contents

Copyright

Trademarks

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

❏ Google Cloud Print, Chrome, Chrome OS, and Android are trademarks of Google Inc.

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

❏ Apple, Macintosh, macOS, OS X, Bonjour, Safari, AirPrint, the AirPrint Logo, iPad, iPhone, iPod touch, and iTunes 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.

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.

Descriptions Used in this Manual

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

❑ Screen shots are from Windows Server 2012 R2. 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 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Vista", "Windows XP", Windows Server 2016, "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" is used to refer to all versions.

❑ Microsoft® Windows® 10 operating system

❑ 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® 2016 operating system

About this Manual

❏ Microsoft® Windows Server® 2012 R2 operating system

❏ Microsoft® Windows Server® 2012 operating system

❏ Microsoft® Windows Server® 2008 R2 operating system

❏ Microsoft® Windows Server® 2008 operating system

❏ Microsoft® Windows Server® 2003 R2 operating system

❏ Microsoft® Windows Server® 2003 operating system

Mac OS

In this manual, "Mac OS" is used to refer to macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x, and Mac OS X v10.6.8.

Introduction

This is a common manual for the administrator to use and manage the printer.

There are unavailable functions and unshown menus because this is a common manual. Therefore, information is given near setting items or menus.

See the *User's Guide* for function usage information.

Manual Component

Printer Settings and Managing

Explains the flow from network connection, to setting each function, to managing the printer.

Connection

Explains how to connect a device to the network. Also explains the using port of the printer, DNS server, and proxy server.

Function Settings

Explains the settings to use each function of the printer.

Product Security Settings

Explains the basic security settings, such as administrator password setting.

Operation and Management Settings

Explains the operations and management after beginning use of the printer, such as checking the printer's information and the notification settings when an event is occurring.

Solving Problems

Explains settings initialization and troubleshooting of the network.

Advanced Security Settings for Enterprise

Explains the advanced security settings used on the network, such as SSL/TLS communication and IPsec / IP filtering.

Terms Used in this Guide

Terms

The following terms are used in this guide.

Introduction

Administrator

The person in charge of installing and setting the device or the network at an office or organization. For small organizations, this person may be in charge of both device and network administration. For large organizations, administrators have authority over the network or devices on the group unit of a department or division, and network administrators are in charge of the communication settings for beyond the organization, such as the Internet.

Network administrator

The person in charge of controlling network communication. The person who set up the router, proxy server, DNS server and mail server to control communication through the Internet or network.

User

The person who uses devices such as printers or scanners.

Server / client connection (printer sharing using the Windows server)

The connection that indicates the printer is connected to the Windows server through the network or by USB cable, and the print queue set on the server can be shared. Communication between the printer and the computer goes through the server, and the printer is controlled on the server.

Peer to peer connection (direct printing)

The connection that indicates the printer and the computer are connected to the network through the hub or access point, and the print job can be executed directly from the computer.

Web Config(device's web page)

The web server that is built into the device. It is called Web Config. You can check and change the device's status on it using the browser.

Print queue

For Windows, the icon for each port displayed on **Device and Printer** such as a printer. Two or more icons are created even for a single device if the device is connected to the network by two or more ports, such as standard TCP/IP and WSD network.

Tool

A generic term for Epson software to set up or manage a device, such as Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, etc.

ASCII (American Standard Code for Information Interchange)

One of the standard character codes. 128 characters are defined, including such characters as the alphabet (a-z, A-Z), Arabic numbers (0-9), symbols, blank characters, and control characters. When "ASCII" is described in this guide, it indicates the 0x20 - 0x7E (hex number) listed below, and does not involve control characters.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
20	SP*	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
30	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
40	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
50	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
60	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
70	p	q	r	s	t	u	v	w	x	y	z	{			}	~	

*   Space character.

Unicode (UTF-8)

An international standard code, covering the major global languages. When "UTF-8" is described in this guide, it indicates coding characters in UTF-8 format.

Example of Network Environment

This is an example of the network environment connection products. Functions and services that are not available in your product may be included.

Example of Medium to Large Office Network Environment
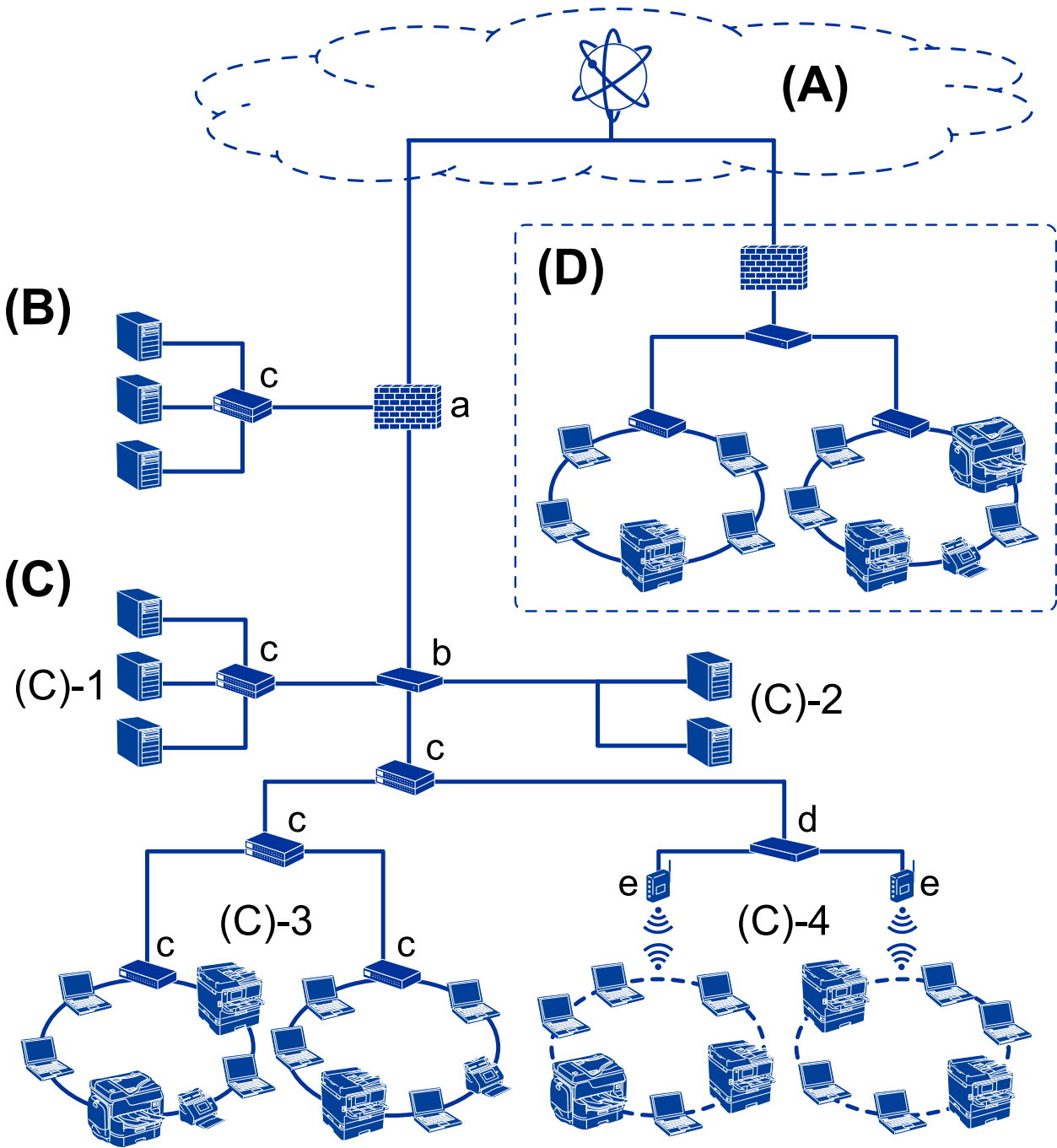
(A):Internet

The following services are available if the printer is able to connect to the Internet.

❏ Epson Connect

Email Print, Remote Print, etc.

❏ Cloud Services

Google Cloud Print, Evernote etc.

❏ Site of Epson

Downloading the driver and software and updating the printer's firmware, etc.

Introduction

(B):DMZ(demilitarized zone)

This zone is placed between the internal network (intranet) and the external network (internet), and both networks are segments isolated by the firewall. It is common to put the server that is opened for the external network. It is able to protect diffusion of an external threat to the internal network. Also, it is able to protect against unauthorized access from the internal network to the server that is opened.

❏ DNS server

❏ Proxy server

❏ Email transfer server

❏ Web server

❏ FTP server

(C): Trust Zone (Intranet)

This is a trust network that is protected by the firewall or UTM (Unified Threat Management).

❏ (C)-1: Server inside of the intranet

This server applies each service to the organization's computers.

❏ DNS server

❏ DHCP server

❏ Email server

❏ Active Directory server / LDAP server

❏ File server

❏ (C)-2: Application server

This server applies the function of the server application as follows.

❏ Epson Print Admin

❏ Document Capture Pro Server

❏ (C)-3: Wired LAN (Ethernet), (C)-4: Wireless LAN (Wi-Fi)

Connect printers, scanners, computers, etc. to the LAN by using a LAN cable or radio wave.

(D): Other branch

This is the other branch network. It is connected by the Internet, leased line, etc.

Network devices

❏ a: Firewall, UTM

❏ b: Router

❏ c: LAN switch

❏ d: Wireless LAN controller

❏ e: Access point

Example of Small Office Network
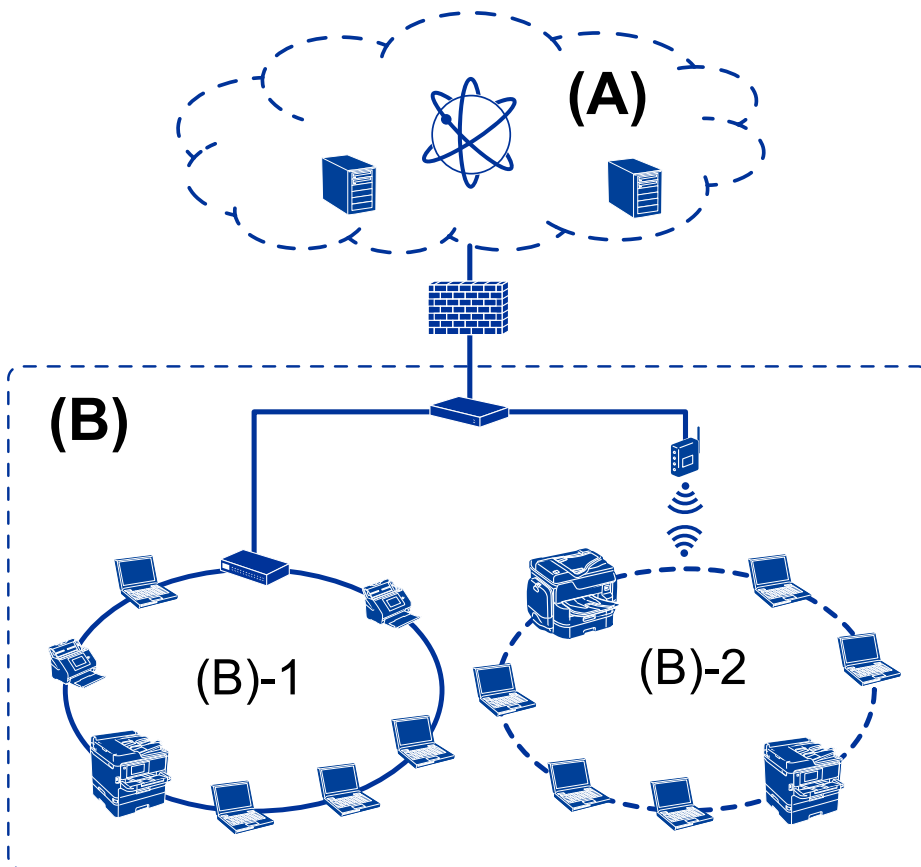
(A): Internet

❏ Epson Connect

❏ Cloud services

❏ Email server, FTP server

(B): Trust Zone (Intranet)

❏ (B)-1: Wired LAN (Ethernet)

❏ (B)-2: Wireless LAN (Wi-Fi)

Printer Connection Types

The following two methods are available for the printer's network connection.

❏ Server / client connection (printer sharing using the Windows server)

❏ Peer to peer connection (direct printing)

Server / Client Connection Settings

This is the connection that the server computer shares with the printer. To prohibit the connection without going through the server computer, you can enhance the security.

Introduction

When using USB, the printer without the network function can be also shared.

Connection method:

Connect the printer to the network via LAN switch or access point.

You can also connect the printer to the server directly by USB cable.

Printer driver:

Install the printer driver on the Windows server depending on the OS of the client computers.

By accessing the Windows server and linking the printer, the printer driver is installed on the client computer and can be used.

Features:

❏ Manage the printer and the printer driver in batch.

❏ Depending on the server spec, it may take time to start the print job because all print jobs go through the print server.

❏ You cannot print when the Windows server is turned off.

Related Information

➡ "Terms" on page 8

Peer to Peer Connection Settings

This is the connection to connect the printer on the network and the computer directly. Only a network-capable model can be connected.

Connection method:

Connect the printer to the network directly via hub or access point.

Printer driver:

Install the printer driver on each client computer.

When using EpsonNet SetupManager, you can provide the driver's package that includes the printer settings.

Features:

❏ The print job starts immediately because the print job is sent to the printer directly.

❏ You can print as long as the printer runs.

Related Information

➡ "Terms" on page 8

Printer Settings and Management

Flow of the Printer Settings and Management
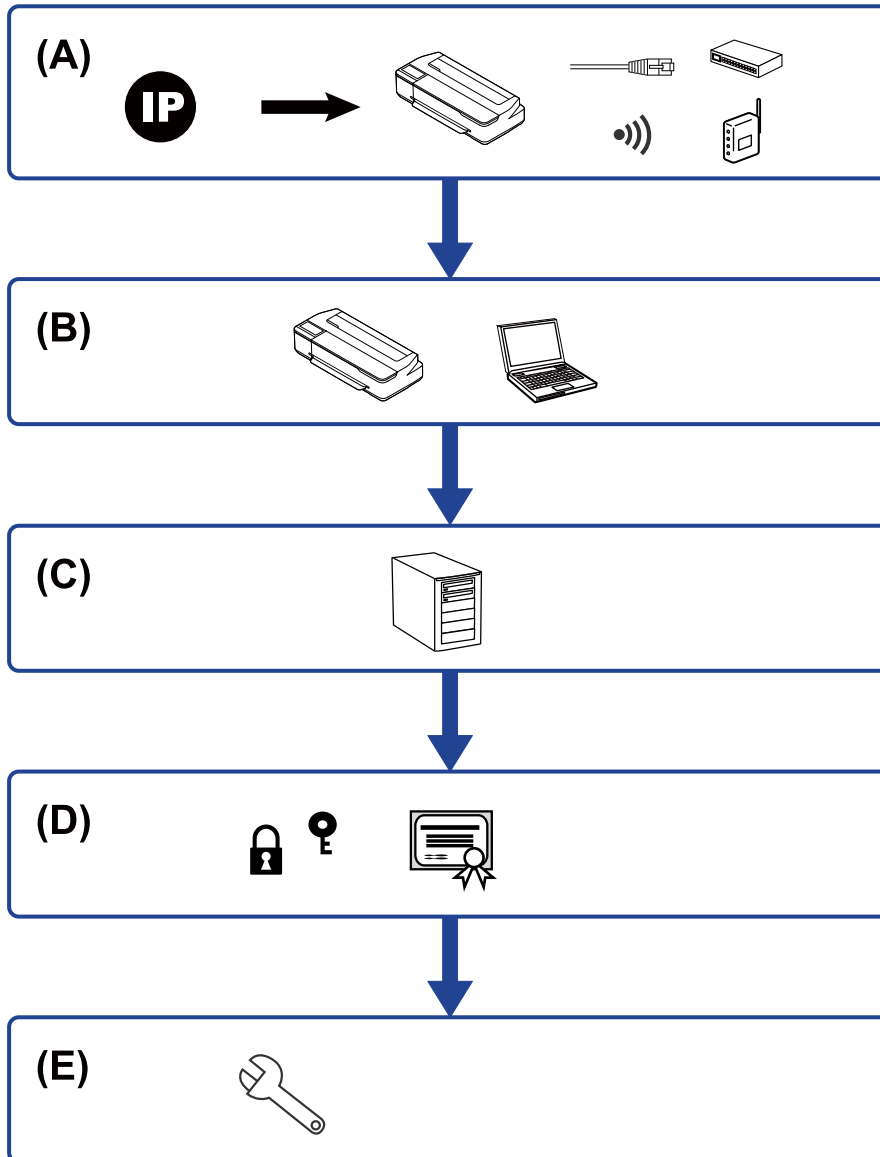
A	Network Connection for the Printer	B	Print function Setting
C	Server Setting	D	Security Settings
E	Operation and Management Settings		

Network Connection for the Printer

Set the IP address to the printer and connect it to the network.

Printer Settings and Management

❏ IP address setting

❏ Connecting to the network (LAN cable connection / Wi-Fi settings)

Related Information

➡

Print Function Setting

Make setting to enable print function.

❏ Print settings for Server / Client Connection

❏ Print settings for Peer to Peer Connection

Related Information

➡

Mail Server Setting

Make the mail server setting for email forwarding or email notification.

❏ SMTP Server

❏ POP3 Server

Related Information

➡

Security Settings

❏ Administrator password setting

❏ Controlling using Protocols

❏ Advanced Security setting

Related Information

➡

➡

Operation and Management Setting

❏ Checking the device status

❏ Responding to the event occurrence

❏ Backing up the device settings

Printer Settings and Management

Related Information

➡

Network Connection

This chapter explains the procedure to connect the printer to the network.

Before Making Network Connection

To connect to the network, check the connection method and setting information for connection in advance.

Gathering Information on the Connection Setting

Prepare the necessary setting information to connect. Check the following information in advance.

Divisions	Items	Note
Device connection method	❏ Ethernet ❏ Wi-Fi	Decide how to connect the printer to the network. For Wired LAN, connects to the LAN switch. For Wi-Fi, connects to the network (SSID) of the access point.
LAN connection information	❏ IP address ❏ Subnet mask ❏ Default gateway	Decide the IP address to assign to the printer. When you assign the IP address statically, all values are required. When you assign the IP address dynamically using the DHCP function, this information is not required because it is set automatically.
Wi-Fi connection information	❏ SSID ❏ Password	These are the SSID (network name) and the password of the access point that the printer connects to. If MAC address filtering has been set, register the MAC address of the printer in advance to register the printer. For the supported standards, see the User's Guide.
DNS server information	❏ IP address for primary DNS ❏ IP address for secondary DNS	These are required when assigning a static IP address to the printer. The secondary DNS is set when the system has a redundant configuration and there is a secondary DNS server. If you are in a small organization and do not set the DNS server, set the IP address of the router.
Proxy server information	❏ Proxy server name	Set this when your network environment uses the proxy server to access the internet from the intranet, and you use the function that the printer directly accesses to the internet. The printer directly connects to the Internet for the following function. ❏ Firmware updating
Port number information	❏ Port number to release	Check the port number used by the printer and computer, then release the port that is blocked by a firewall, if necessary. For the port number used by the printer, see the Appendix.

IP Address Assignment

These are the following types of IP address assignment.

Static IP address:

Assign the predetermined IP address to the printer (host) manually.

The information to connect to the network (subnet mask, default gateway, DNS server and so on) need to be set manually.

The IP address does not change even when the device is turned off, so this is useful when you want to manage devices with an environment where you cannot change the IP address or you want to manage devices using the IP address. We recommend settings to the printer, server, etc. that many computers access. Also, when using security features such as IPsec / IP filtering, assign a fixed IP address so that the IP address does not change.

Automatic assignment by using DHCP function (dynamic IP address):

Assign the IP address automatically to the printer (host) by using the DHCP function of the DHCP server or router.

The information to connect to the network (subnet mask, default gateway, DNS server and so on) is set automatically, so you can easily connect the device to the network.

If the device or the router is turned off, or depending on the DHCP server settings, IP address may change when re-connecting.

We recommend managing devices other than the IP address and communicating with protocols that can follow the IP address.

Note:
When you use the IP address reservation function of the DHCP, you can assign the same IP address to the devices at any time.

DNS Server and Proxy Server

The DNS server has a host name, domain name of the email address, etc. in association with the IP address information.

Communication is impossible if the other party is described by host name, domain name, etc. when the computer or the printer performs IP communication.

Queries the DNS server for that information and gets the IP address of the other party. This process is called name resolution.

Therefore, the devices such as computers and printers can communicate using the IP address.

Name resolution is necessary for the printer to communicate using the email function or Internet connection function.

When you use those functions, make the DNS server settings.

When you assign the printer's IP address by using the DHCP function of the DHCP server or router, it is automatically set.

The proxy server is placed at the gateway between the network and the Internet, and it communicates to the computer, printer, and Internet (opposite server) on behalf of each of them. The opposite server communicates only to the proxy server. Therefore, printer information such as the IP address and port number cannot be read and increased security is expected.

When you connect to the Internet via a proxy server, configure the proxy server on the printer.

Connecting to the Network from the Control Panel

Connect the printer to the network by using the printer's control panel.

For the printer's control panel, see the *User's Guide* for more details.

Assigning the IP Address

Set up the basic items such as Host Address, Subnet Mask, Default Gateway.

This section explains the procedure for setting a static IP address.

1. Turn on the printer.

2. Select **Settings** on the home screen on the printer's control panel.
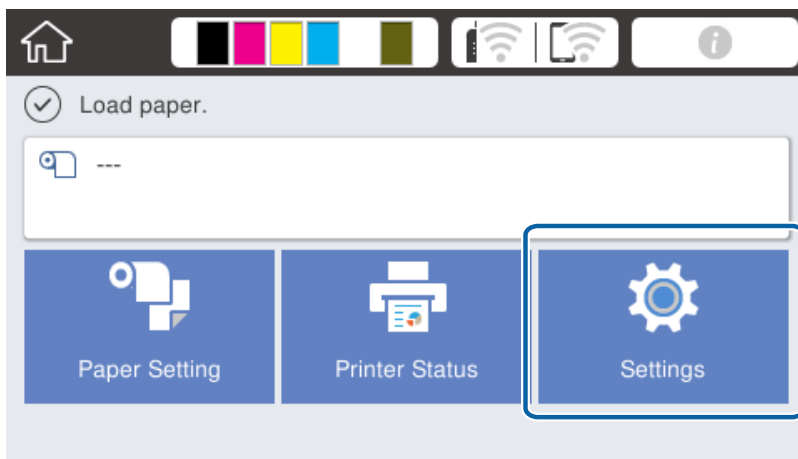
3. Select **General Settings** > **Network Settings** > **Advanced**.

4. Select **TCP/IP**.
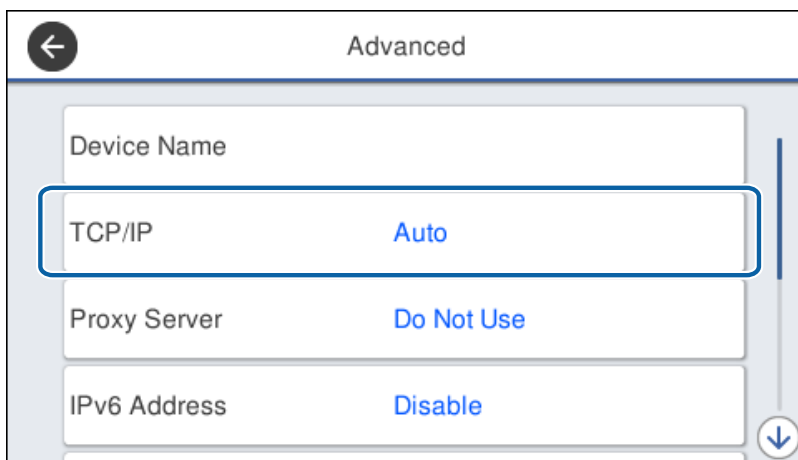
5. Select **Manual** for **Obtain IP Address**.

   When you set the IP address automatically by using the DHCP function of router, select **Auto**. In that case, the **IP Address**, **Subnet Mask**, and **Default Gateway** on step 6 to 7 are also set automatically, so go to step 8.
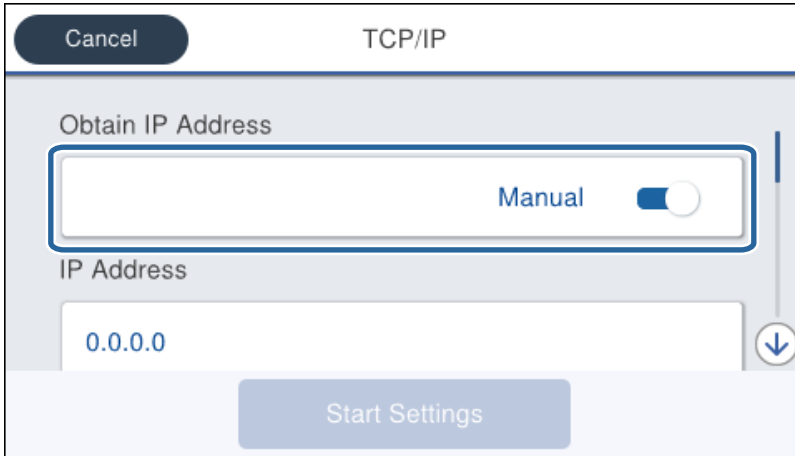
6. Enter the IP address.

   Focus moves to the forward segment or the back segment separated by a period if you select ◀ and ▶.
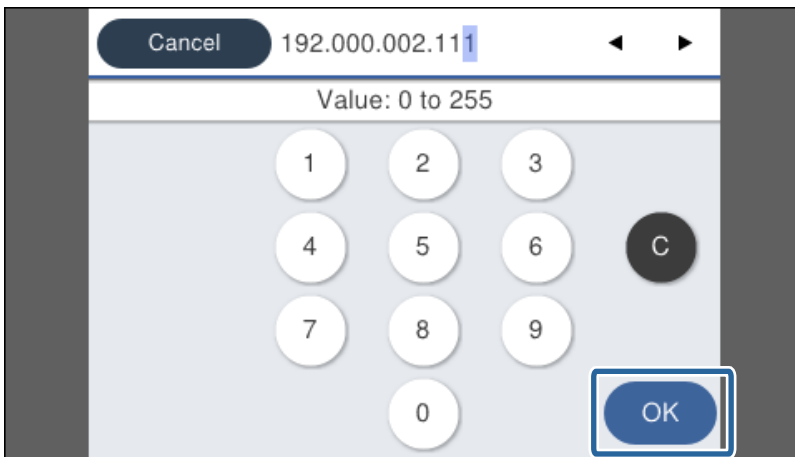
   Confirm the value reflected on the previous screen.

7. Set up the **Subnet Mask** and **Default Gateway**.

   Confirm the value reflected on the previous screen.

   > **⚠ Important:**
   >
   > *If the combination of the IP Address, Subnet Mask and Default Gateway is incorrect, **Start Setup** is inactive and cannot proceed with the settings. Confirm that there is no error in the entry.*

8. Enter the IP address for the primary DNS server.

   Confirm the value reflected on the previous screen.

Note:
When you select Auto for the IP address assignment settings, you can select the DNS server settings from Manual or Auto. If you cannot obtain the DNS server address automatically, select Manual and enter the DNS server address. Then, enter the secondary DNS server address directly. If you select Auto, go to step 10.

9. Enter the IP address for the secondary DNS server.

    Confirm the value reflected on the previous screen.

10. Tap **Start Setup**.

11. Close the confirmation screen.

Setting the Proxy Server

Set up the proxy server if both of the following are true.

❏ The proxy server is built for Internet connection.

❏ You want to update the printer firmware via the Internet from the printer's control panel or Web Config.

1. Select **Settings** on the home screen.

    When making settings after IP address setting, the **Advanced** screen is displayed. Go to step 3.
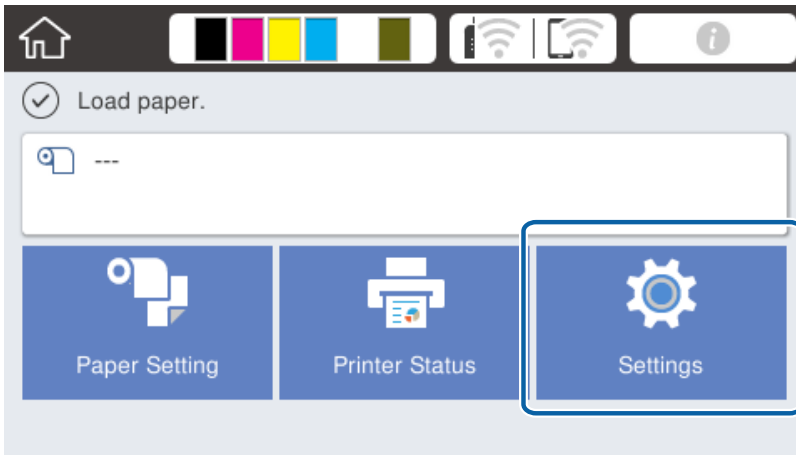
2. Select **General Settings** > **Network Settings** > **Advanced**.

3. Select **Proxy Server**.
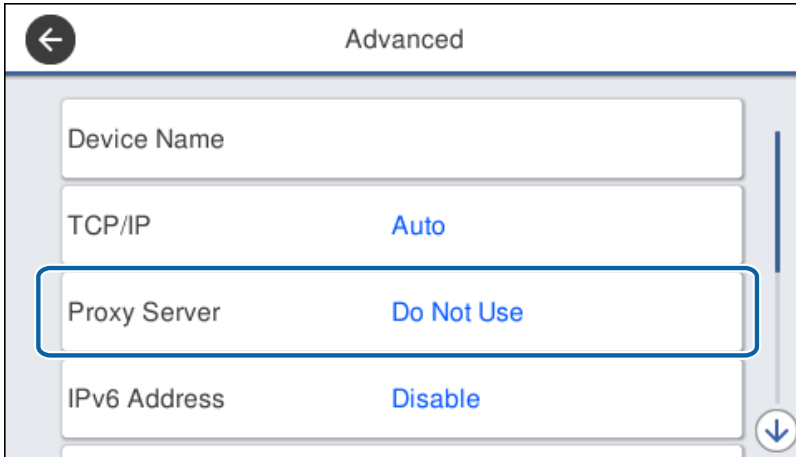
4. Select **Use** for **Proxy Server Settings**.
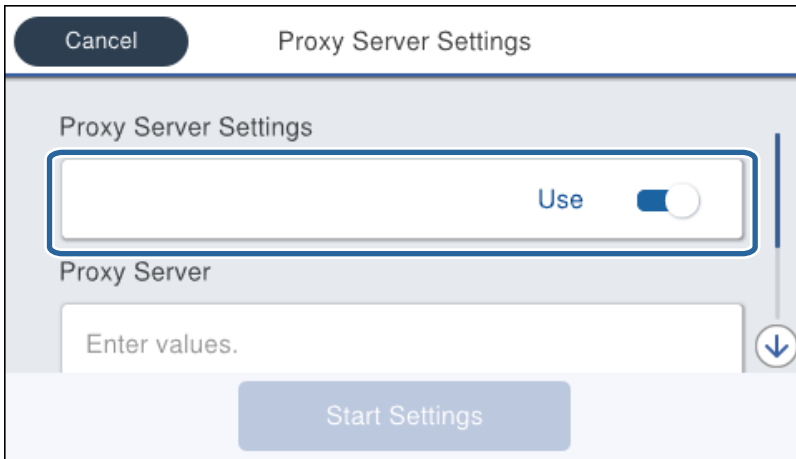
5. Enter the address for the proxy server by IPv4 or FQDN format.

Confirm the value reflected on the previous screen.

6. Enter the port number for the proxy server.

   Confirm the value reflected on the previous screen.

7. Tap **Start Setup**.

8. Close the confirmation screen.

Connecting to LAN

Connect the printer to the network by Ethernet or Wi-Fi.

Related Information

Connecting to Ethernet

Connect the printer to the network by using the Ethernet cable, and check the connection.

1. Connect the printer and hub (LAN switch) by Ethernet cable.

2. Select **Settings** on the home screen.
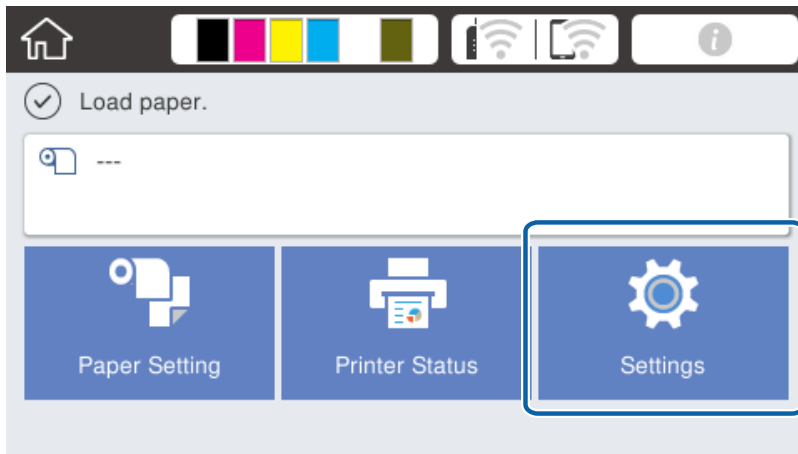
3. Select **General Settings** > **Network Settings**.

4. Select **Connection Check**.

   The connection diagnosis result is displayed. Confirm the connection is correct.

5. Tap **OK** to finish.

   When you tap **Print Check Report**, you can print the diagnosis result. Follow the on-screen instructions to print it.

Related Information

Connecting to the Wireless LAN (Wi-Fi)

You can manually set up the information necessary to connect to an access point from the printer's control panel. To set up manually, you need the SSID and password for an access point.

Note:
When the access point supports WPS, you can automatically make the Wi-Fi connection settings by using the push button or PIN code, without using the SSID and password.

1. Tap [icon] | [icon] on the home screen.

2. Select **Router**.

3. Tap **Start Setup**.

    If the network connection is already set up, the connection details are displayed. Tap **Change Settings** to change the settings.

    If the printer is already connected by Ethernet, the connection details are displayed. Tap **Change to Wi-Fi connection.**, and then tap **Yes** after confirming the message.

4. Select **Wi-Fi Setup Wizard**.

5. Select the SSID for the access point.

    If the SSID you want to connect to is not displayed on the printer's control panel, tap **Search Again** to update the list. If it is still not displayed, tap **Enter Manually**, and then enter the SSID directly.

6. Tap **Enter Password**, and then enter the password.

    Note:
    ❏ *The password is case-sensitive.*

    ❏ *If you enter the SSID directly, select **Available** for **Password**, and then enter the password.*

7. When you have finished, tap **OK**.

8. Check the settings, and then tap **Start Setup**.

9. Tap **OK** to finish.

    If you fail to connect, select **Print Check Report** to print a network connection report, and then check the printed solutions.

10. Close the network connection settings screen.

Related Information

➡ "Messages and Solutions on the Network Connection Report" on page 59
➡ "Making Wi-Fi Settings from the Control Panel (WPS)" on page 74
➡ "Changing from Wi-Fi Connection to Ethernet Connection" on page 78

Function Settings

This chapter explains the first settings to make in order to use each function of the device.

Software for Setting

In this topic, the procedure for making settings from the administrator's computer using Web Config is explained.

Web Config (Web Page for Device)

About Web Config

Web Config is a built-in web page of the printer for configuring the printer's settings. You can operate the printer connected to the network from the computer.

To access 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.
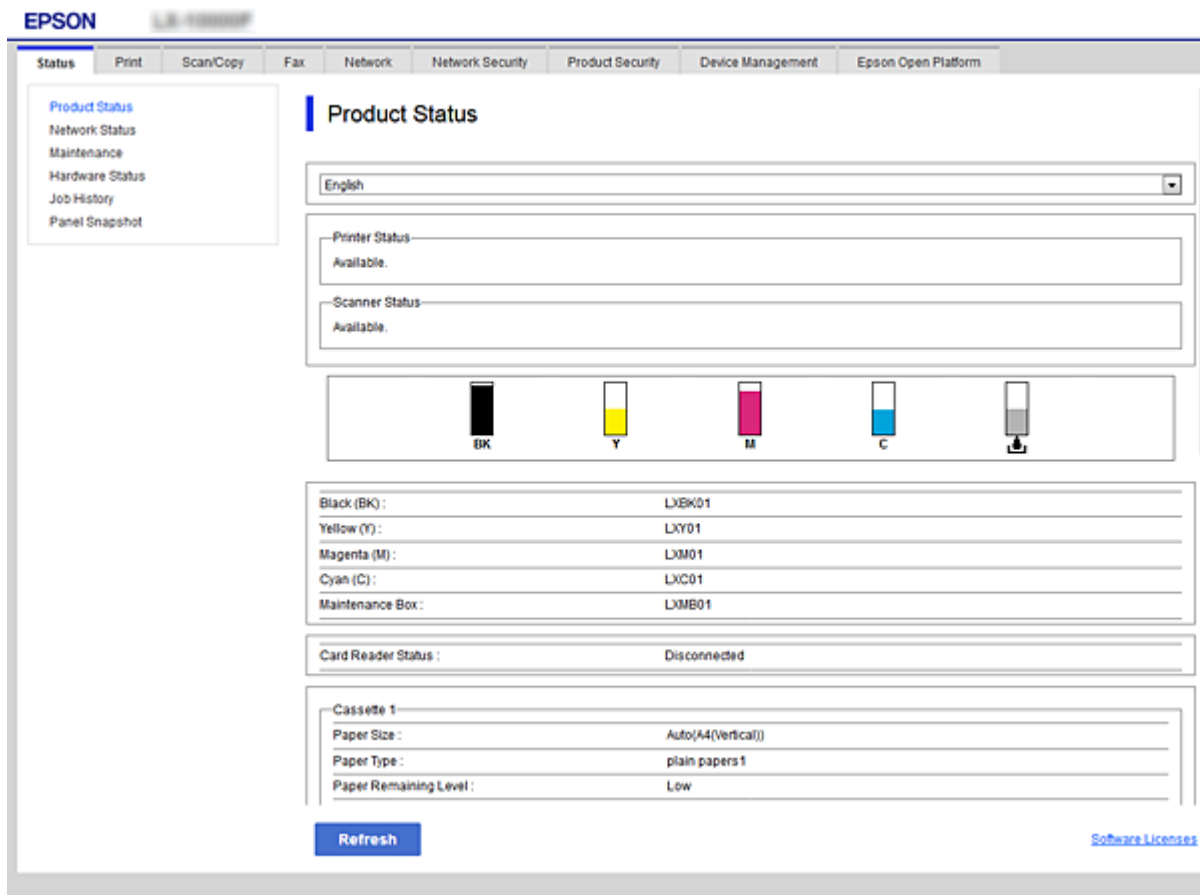
Accessing Web Config

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 HTTPS

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

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

❏ Accessing via HTTP

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

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

Examples

❏ IPv4:

https://192.0.2.111/

http://192.0.2.111/

❏ IPv6:

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

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

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

Related Information

➡ "SSL/TLS Communication with the Printer" on page 82

➡ "About Digital Certification" on page 82

Using the Print Functions

Enable to use the print function through the network.

To use the printer on the network, you need to set the port for network connection on the computer as well as the printer's network connection.

❏ Server / client connection : Set the port on the server computer

For the server / client connection, explain how to set the port manually.

❏ Peer to peer connection : Set the port on each computer

For peer to peer connection, explain how to set the port automatically using the installer available from the software disc or Epson's website.

Print Settings for Server / Client Connection

Enable to print from the printer that is connected as the server / client connection.

For the server / client connection, set up the print server first, and then share the printer on the network.

When using the USB cable to connect to the server, also set the print server first, and then share the printer on the network.

Setting Up the Network Ports

Create the print queue for network printing on the print server by using standard TCP/IP, and then set the network port.

This example is when using Windows 2012 R2.

1. Open the devices and printers screen.

   Desktop > **Settings** > **Control Panel** > **Hardware and Sound** or **Hardware** > **Devices and Printers**.

2. Add a printer.

   Click **Add printer**, and then select **The printer that I want isn't listed**.

3. Add a local printer.

   Select **Add a local printer or network printer with manual settings**, and then click **Next**.

4. Select **Create a new port**, select **Standard TCP/IP Port** as the Port Type, and then click **Next**.
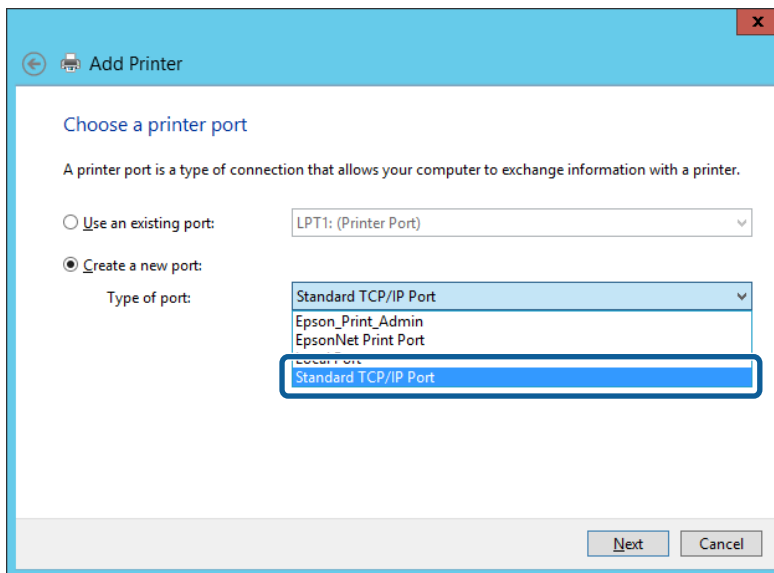
5. Enter the printer's IP address or printer name in **Host Name or IP Address** or **Printer Name or IP Address**, and then click **Next**.

   Example:

   ❏ Printer name : EPSONA1A2B3C

   ❏ IP address : 192.0.2.111

   Do not change **Port name**.

<div align="center">**Function Settings**</div>

Click **Continue** when the **User Account Control** screen is displayed.

Note:
If you specify the printer name on the network where the name resolution is available, the IP address is tracked even if printer's IP address has been changed by DHCP. You can confirm the printer name from the network status screen on the printer's control panel or network status sheet.

6. Set the printer driver.

   ❏ If the printer driver is already installed:

   Select **Manufacturer** and **Printers**. Click **Next**.

   ❏ If the printer driver is not installed:

   Click **Have Disc** and then insert the software disc supplied with the printer. Click **Browse**, and then select the folder on the disc containing the printer driver. Make sure you select the correct folder. The location of the folder may change depending on your operating system.

   32 bit version of Windows: WINX86

   64 bit version of Windows: WINX64

7. Follow the on-screen instructions.

When using the printer under the server / client connection (printer sharing using the Windows server), make the sharing settings hereafter.

Related Information

➡ "Sharing the Printer (Windows only)" on page 30

Checking the Port Configuration - Windows

Check if the correct port is set for the print queue.

1. Open the devices and printers screen.

   Desktop > **Settings** > **Control Panel** > **Hardware and Sound** or **Hardware** > **Devices and Printers**.

Function Settings

2. Open the printer properties screen.

   Right-click the printer icon, and then click **Printer properties**.

3. Click the **Ports** tab, select **Standard TCP/IP Port**, and then click **Configure Port**.

4. Check the port configuration.

   ❏ For RAW

      Check that **Raw** is selected in **Protocol**, and then click **OK**.

   ❏ For LPR

      Check that **LPR** is selected in **Protocol**. Enter "PASSTHRU" in **Queue name** from **LPR Settings**. Select **LPR Byte Counting Enabled**, and then click **OK**.

Sharing the Printer (Windows only)

When using the printer under the server / client connection (printer sharing using the Windows server), set up the printer sharing from the print server.

1. Select **Control Panel** > **View devices and printers** on the print server.

2. Right-click the printer icon (print queue) that you want to share with, and then select **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.

Installing Additional Drivers (Windows only)

If the Windows versions for a server and clients are different, it is recommended to install additional drivers to the print server.

1. Select **Control Panel** > **View devices and printers** on the print server.

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**.

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

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

5. Select the information file for the printer driver (*.inf) and then install the driver.

Related Information

➡ "Using the Shared Printer – Windows" on page 31

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

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**.

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

Related Information

➡ "Sharing the Printer (Windows only)" on page 30
➡ "Installing Additional Drivers (Windows only)" on page 30

Print Settings for Peer to Peer Connection

For peer to peer connection (direct printing), a printer and a client computer have a one-to-one relationship.

The printer driver must be installed on each client computer.

Related Information

➡ "Setting the Printer Driver - Windows" on page 31
➡ "Setting the Printer Driver - Mac OS" on page 32

Setting the Printer Driver - Windows

For small organizations, we recommend installing the printer driver on each client computer. Use the installer on Epson website or on the software disc.

Note:
When the printer is used from many client computers, by using EpsonNet SetupManager and delivering the driver as a package, install operation time can be reduced dramatically.

1. Run the installer.

    ❏ Running from the website

    Access the following website, and then enter the product name. Go to **Setup**, download the software, and then run it.

    http://epson.sn

    ❏ Running from the software disc (only for the models that come with a software disc and users with computers with disc drives.)

    Insert the software disc into the computer.

2. Select the connection method for the printer, and then click **Next**.
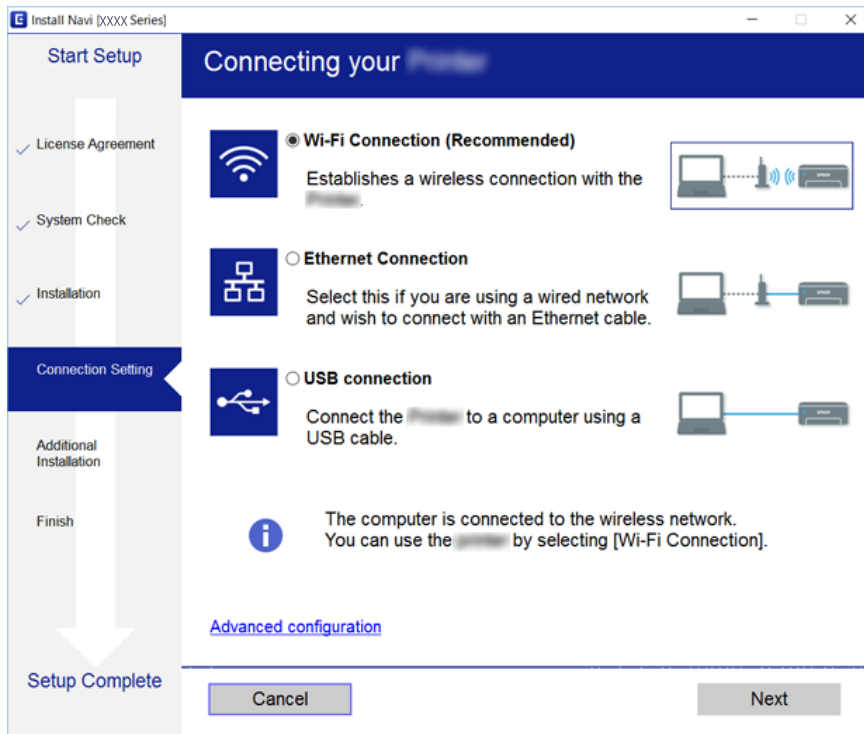
Note:
If **Select Software Installation** *is displayed, select* **Change or re-set the connection method** *and then click* **Next**.

3. Follow the on-screen instructions.

Related Information

➡ "EpsonNet SetupManager" on page 73

Setting the Printer Driver - Mac OS

Download the software from the website, and then make connection settings for adding a computer. Start the setup under the Internet available environment.

1. Access the following website from the computer you want to make settings, and then enter the product's name.

   http://epson.sn

2. Go to **Setup**, and then download the software.

3. Run the software, and then follow the on-screen instructions.

4. Select **Additional Computer** on the Connection Type screen.
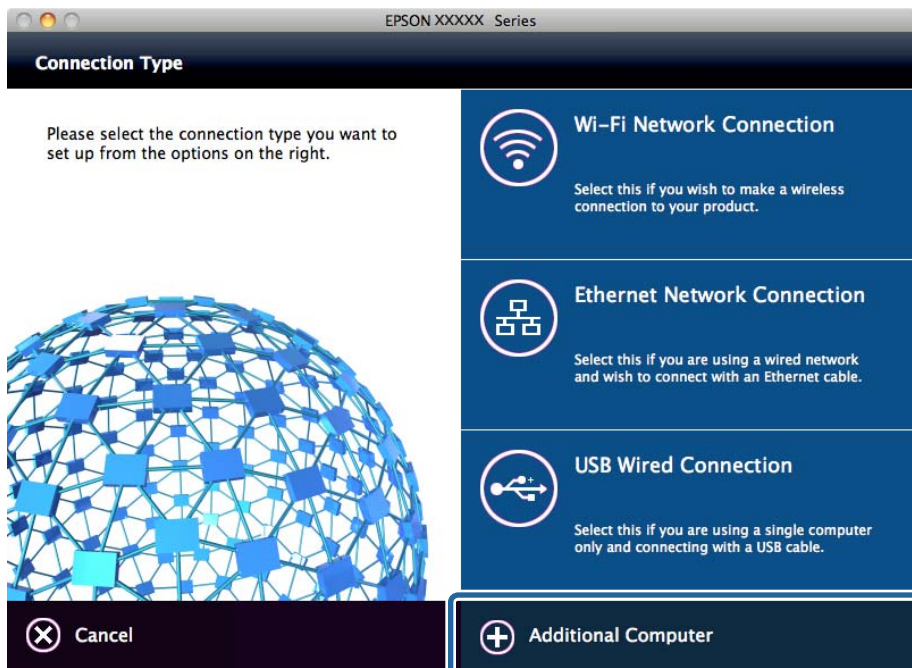
5. Follow the on-screen instructions.

Defining Custom Paper Setting

You can define paper settings such as paper size and paper type. Defined user paper settings can be used by calling from the printer's control panel.

1. Access Web Config and select the **Print** tab > **Custom Paper Setting**.

2. Click a circle beside the number you want to edit, and then click **Edit**.

3. Set each item.

   ❏ Custom Paper Name

   Enter Custom Paper Name you want to register. The name that registered here is displayed in the paper type list.

   ❏ Reference Paper

   You can select the media type that is the closest to the paper you are using.

   ❏ Platen Gap

   Select the platen gap, which is the distance between the print head and the paper.

   Since the platen gap of the selected Reference Paper is set, you don't need to change value normally. If printed images are smeared, change to a wider setting.

   ❏ Top/Bottom Margins

   Set margins of the printing area. The left and right margins will remain at 3 mm regardless of this setting. If the top of the printed image is dirty, change the top margin to a wider setting.

❑ Paper Suction

Set the appropriate amount of suction for the paper used in order to maintain the correct distance between the paper and the print head. Choosing too high a value for thin or soft paper will increase the distance between the paper and the print head, causing print quality to decline or preventing the paper feeding correctly. In such cases, you will need to lower the paper suction. The suction power is weakened when the parameter is lowered. This item is not displayed depending on the model.

❑ Back Tension

Adjust paper tension. If the paper wrinkles during printing, select **High** or **Extra High**.

❑ Drying Time per Pass

Depending on the paper type, the ink may take a while to dry. Set the time to stop the movement (pass) of the print head to assist drying of the ink. If the ink blurs on the paper, set a longer time for drying the ink. The longer the drying time, the more time required for printing.

❑ Drying Time per Page

Depending on the ink density or paper type, the ink may take a while to dry. Specify how long the printer pauses to allow the ink to dry after printing each page. If the ink blurs on the paper, set a longer time for drying the ink. The longer the drying time, the more time required for printing.

❑ Paper Size Check

When set the paper, select whether the printer automatically detects or does not detect the paper width. Try choosing **Off** if a paper setting error is displayed when the paper is correctly loaded. Note, however, that the printer may print outside the paper when **Off** is selected. The changed settings are applied after the paper is reloaded. This item is not displayed depending on the model.

❑ Auto Cut

Select whether to automatically cut roll paper as each page is printed or not. When select **On**, leading edge cutting is automatically performed when the leading edge of the set paper is not horizontal. The setting selected with the printer driver takes priority when the printer driver is used.

❑ Remove Skew

Select whether to reduce or prevent diagonal paper feed. This item is not displayed depending on the model.

4. Check the settings, and then click **OK**.

    Note:
    The custom paper settings can be exported to a file and imported from a file. You can share settings with another printer with the same function using the setting file.

Related Information

➡ "Accessing Web Config" on page 27

➡ "Accessing Web Config" on page 27

Configuring a Mail Server

Set the mail server from Web Config.

When the printer can send the email, receiving the email notification from the printer is enabled.

Check below before setting up.

❑ The printer is connected to the network that can access the mail server.

❏ Email setting information of the computer that uses the same mail server as the printer.

Note:
When you use the mail server on the Internet, confirm the setting information from the provider or website.

1. Access Web Config and select the **Network** tab > **Email Server** > **Basic**.

2. Enter a value for each item.

3. Select **OK**.

    The settings you have selected are displayed.

    When the setup completes, perform the connection check.

Related Information

➡ "Checking a Mail Server Connection" on page 37
➡ "Mail Server Setting Items" on page 35
➡ "Accessing Web Config" on page 27

Mail Server Setting Items
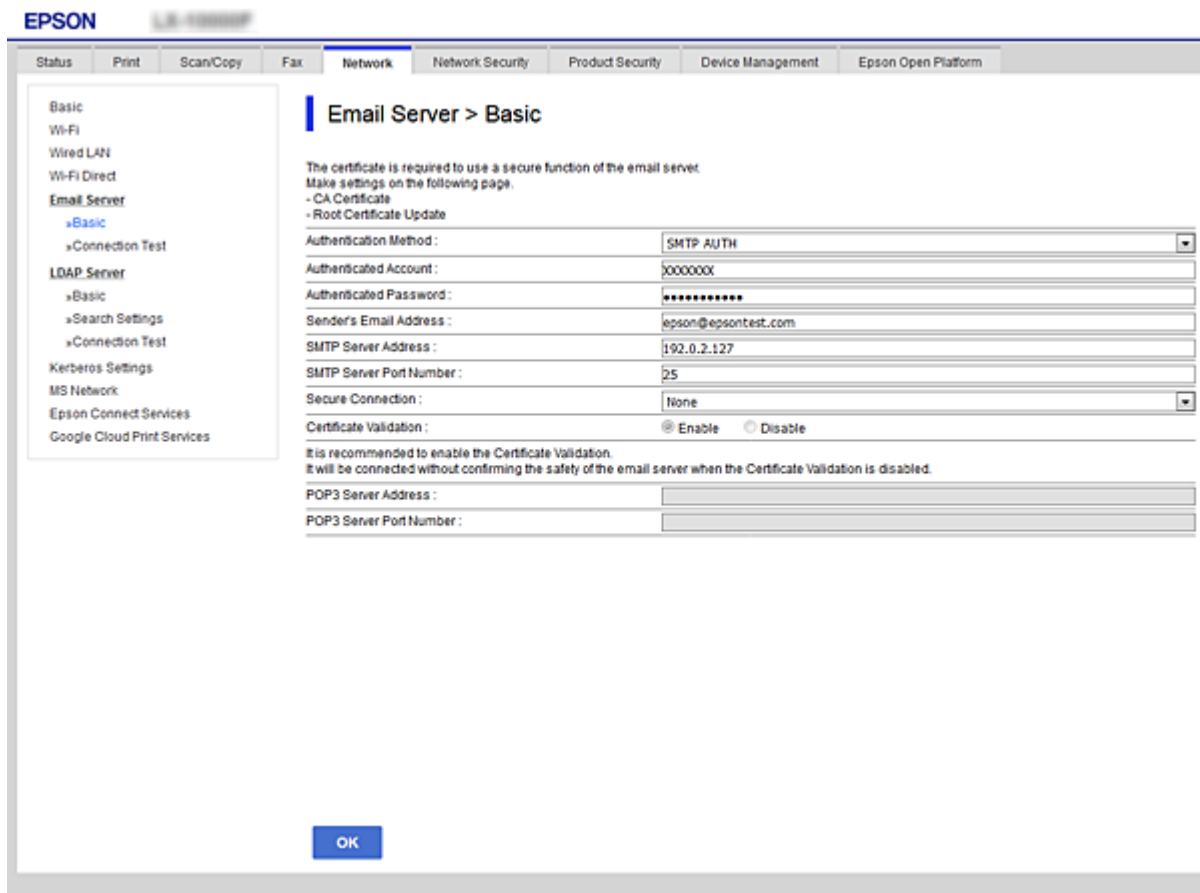
Function Settings

Items	Settings and Explanation	
Authentication Method	Specify the authentication method for the printer to access the mail server.	
	Off	Set when the mail server does not need authentication.
	SMTP AUTH	Authenticates on the SMTP server (outgoing mail server) when sending the email. The mail server needs to support SMTP authentication.
	POP before SMTP	Authenticates on the POP3 server (receiving mail server) before sending the email. When you select this item, set the POP3 server.
Authenticated Account	If you select **SMTP AUTH** or **POP before SMTP** as the **Authentication Method**, enter the authenticated account name between 0 and 255 characters in ASCII (0x20-0x7E). When you select **SMTP AUTH**, enter the SMTP server account. When you select **POP before SMTP**, enter the POP3 server account.	
Authenticated Password	If you select **SMTP AUTH** or **POP before SMTP** as the **Authentication Method**, enter the authenticated password between 0 and 20 characters in ASCII (0x20-0x7E). When you select **SMTP AUTH**, enter the authenticated account for the SMTP server. When you select **POP before SMTP**, enter the authenticated account for the POP3 server.	
Sender's Email Address	Enter the sender's email address such as the email address of the system administrator. This is used when authenticating, so enter a valid email address that is registered to the mail server. 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.	
Secure Connection	Select the encryption method of the communication to the mail server.	
	None	If you select **POP before SMTP** in **Authentication Method**, the connection is not encrypted.
	SSL/TLS	This is available when **Authentication Method** is set to **Off** or **SMTP AUTH**. Communication is encrypted from the start.
	STARTTLS	This is available when **Authentication Method** is set to **Off** or **SMTP AUTH**. Communication is not encrypted from the start, but depending on the network environment, whether the communication is encrypted or not is changed.
Certificate Validation	The certificate is validated when this is enabled. We recommend this is set to **Enable**. To set up, you need to import the CA Certificate to the printer.	
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.	

Related Information

Checking a Mail Server Connection

You can check the connection to the mail server by performing the connection check.

1. Access Web Config and select the **Network** tab > **Email Server** > **Connection Test**.

2. Select **Start**.

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

Related Information

➡
➡

Mail Server Connection Test References

Messages	Cause
Connection test was successful.	This message appears when the connection with the server is successful.
SMTP server communication error. Check the following. - Network Settings	This message appears when ❑ The printer is not connected to a network ❑ SMTP server is down ❑ Network connection is disconnected while communicating ❑ Received incomplete data
POP3 server communication error. Check the following. - Network Settings	This message appears when ❑ The printer is not connected to a network ❑ POP3 server is down ❑ Network connection is disconnected while communicating ❑ Received incomplete data
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	This message appears when ❑ Connecting to a DNS server failed ❑ Name resolution for an SMTP server failed
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	This message appears when ❑ Connecting to a DNS server failed ❑ Name resolution for an POP3 server failed
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	This message appears when SMTP server authentication failed.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	This message appears when POP3 server authentication failed.

Function Settings

Messages	Cause
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	This message appears when you try to communicate with unsupported protocols.
Connection to SMTP server failed. Change Secure Connection to None.	This message appears when an SMTP mismatch occurs between a server and a client, or when the server does not support SMTP secure connection (SSL connection).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	This message appears when an SMTP mismatch occurs between a server and a client, or when the server requests to use an SSL/TLS connection for an SMTP secure connection.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	This message appears when an SMTP mismatch occurs between a server and a client, or when the server requests to use an STARTTLS connection for an SMTP secure connection.
The connection is untrusted. Check the following. - Date and Time	This message appears when the printer's date and time setting is incorrect or the certificate has expired.
The connection is untrusted. Check the following. - CA Certificate	This message appears when the printer does not have a root certificate corresponding to the server or a CA Certificate has not been imported.
The connection is not secured.	This message appears when the obtained certificate is damaged.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	This message appears when an authentication method mismatch occurs between a server and a client. The server supports SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	This message appears when an authentication method mismatch occurs 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.	This message appears when the specified sender's Email address is wrong.
Cannot access the printer until processing is complete.	This message appears when the printer is busy.

Related Information

➡

Making System Settings

Setting the Control Panel

Setup for the printer's control panel. You can set up as follows.

1. Access Web Config and select the **Device Management** tab > **Control Panel**.

2. Set up the following items as necessary.

   ❑ Language

   Select the displayed language on the control panel.

❏ Panel Lock

If you select **ON**, the administrator password is required when you perform an operation that requires the administrator's authority. If the administrator password is not set, panel lock is disabled.

❏ Operation Timeout

If you select **ON**, when you log in as the administrator, you are automatically logged out and go to the initial screen if there is no activity for a certain period of time.

You can set between 10 seconds and 240 minutes by the second.

Note:
You can also set up from the printer's control panel.

❏ *Language :* ***Settings*** *>* ***General Settings*** *>* ***Basic Settings*** *>* ***Language***

❏ *Panel Lock :* ***Settings*** *>* ***General Settings*** *>* ***System Administration*** *>* ***Security Settings*** *>* ***Admin Settings*** *>* ***Lock Setting***

❏ *Operation Time Out :* ***Settings*** *>* ***General Settings*** *>* ***Basic Settings*** *>* ***Operation Time Out*** *(You can specify On or Off.)*

3. Click **OK**.

Related Information

➡ "Accessing Web Config" on page 27

Power Saving Settings During Inactivity

You can set up the time to shift to the power saving mode or to turn the power off when the printer's control panel is not operated for a certain period of time. Set the time depending on your usage environment.

1. Access Web Config and select the **Device Management** tab > **Power Saving**.

2. Enter the time for the **Sleep Timer** to switch to power saving mode when inactivity occurs.

You can set up to 210 minutes by the minute.

Note:
You can also set up from the printer's control panel.

Settings *>* ***General Settings*** *>* ***Basic Settings*** *>* ***Sleep Timer***

3. Select the turning off time for the **Power Off Timer**.

Note:
You can also set up from the printer's control panel.

Settings *>* ***General Settings*** *>* ***Basic Settings*** *>* ***Power Off Timer***

4. Click **OK**.

Related Information

➡ "Accessing Web Config" on page 27

Synchronizing the Date and Time with Time Server

When synchronizing with the time server (NTP server), you can synchronize the time of the printer and the computer on the network. The time server may be operated within the organization or published on the Internet.

When using the CA certificate, time-related trouble can be prevented by synchronizing with the time server.

1. Access Web Config and select the **Device Management** tab > **Date and Time** > **Time Server**.

2. Select **Use** for **Use Time Server**.

3. Enter the time server address for **Time Server Address**.

    You can use IPv4, IPv6 or FQDN format. Enter 252 characters or less. If you do not specify this, leave it blank.

4. Enter **Update Interval (min)**.

    You can set up to 10,800 minutes by the minute.

5. Click **OK**.

    Note:
    *You can confirm the connection status with the time server on **Time Server Status**.*

Related Information

➡

AirPrint Setup

Set when using AirPrint printing.

Access Web Config and select the **Network** tab > **AirPrint Setup**.

Items	Explanation
Bonjour Service Name	Enter the Bonjour service name between 1 and 41 characters in ASCII (0x20-0x7E).
Bonjour Location	Enter location information such as the printer's placement within 127 bytes or less in Unicode (UTF-8).
Geolocation Latitude and Longitude (WGS84)	Enter the printer's location information. This entry is optional. Enter values by using WGS-84 datum, which separates latitude and longitude with a comma. You can enter -90 to +90 for the latitude value, and -180 to +180 for the longitude value. You can enter less than a decimal to the sixth place, and you can omit "+".
Top Priority Protocol	Select top priority protocol from IPP and Port9100.
Wide-Area Bonjour	Set whether or not to use Wide-Area Bonjour. If you use it, the printers must be registered on the DNS server to be able to search the printer over the segment.
Enable AirPrint	IPP, Bonjour, AirPrint are enabled, and IPP is established only with secure communication.

Product Security Settings

This chapter explains the security settings of the device.

Introduction of Product Security Features

This section introduces the security function of the Epson Devices.

Feature name	Feature type	What to set	What to prevent
Setup for the administrator password	Locks the system settings, such as connection setup for network or USB.	An administrator sets a password to the device. You can set or change from both Web Config and the printer's control panel.	Prevent from illegally reading and changing the information stored in the device such as ID, password, network settings, and so on. Also, reduce a wide range of security risks such as leakage of information for the network environment or security policy.
Setup for external interface	Controls the interface that connects to the device.	Enable or disable USB connection with the computer.	Prevents unauthorized use of the device by prohibiting printing without going through the network.

Related Information

➡

➡

➡

➡

Configuring the Administrator Password

When you set the administrator password, you can prevent the users from changing system management settings. You can set and change the administrator password using either Web Config, the printer's control panel, or software (Epson Device Admin). When using the software, see the documentation for each software.

Related Information

➡

➡

➡

Configuring the Administrator Password from the Control Panel

You can set the administrator password from the printer's control panel.

1. Select **Settings** on the printer's control panel.

2. Select **General Settings** > **System Administration** > **Security Settings**.

3. Select **Admin Settings**.

4. Select **Admin Password** > **Register**.

5. Enter the new password.

6. Enter the password again.

7. Close the confirmation screen.

   The administrator settings screen is displayed.

Note:
*You can change or delete the administrator password when you select **Change** or **Reset** on the **Admin Password**screen and enter the administrator password.*

Configuring the Administrator Password Using Web Config

You can set the administrator password using Web Config.

1. Access Web Config and select the **Product Security** tab > **Change Administrator Password**.

2. Enter a password to **New Password** and **Confirm New Password**. Enter the user name, if necessary.

   If you want to change the password to new one, enter a current password.

3. Select **OK**.

   Note:
   ❏ *To set or change the locked menu items, click **Administrator Login**, and then enter the administrator password.*

   ❏ *To delete the administrator password, click **Product Security** tab > **Delete Administrator Password**, and then enter the administrator password.*

Related Information

➡

Controlling the Panel Operation

If you set the administrator password and enable the Lock Setting, you can lock the items related to the printer's system settings so that users cannot change them.

Enabling the Lock Setting

Enable the Lock Setting for the printer where the password is set.

Specify an administrator's password first.

Enabling the Lock Setting from the Control Panel

1. Select **Settings** on the printer's control panel.

2. Select **General Settings** > **System Administration** > **Security Settings**.

3. Select **Admin Settings**.

4. Select **On** on **Lock Setting**.

5. Select **Yes** on the confirmation screen.

6. Select **Settings** > **General Settings** > **Network Settings**, and then check that the password is required.

Enabling the Lock Setting from Web Config

1. Access Web Config and click the **Administrator Login**.

2. Enter the user name and password, and then click **OK**.

3. Select the **Device Management** tab > **Control Panel**.

4. On the **Panel Lock**, select **ON**.

5. Click **OK**.

6. Select **Settings** > **General Settings** > **Network Settings** on the printer's control panel, and then check that the password is required.

Lock Setting Items for General Settings Menu

This is a list of the Lock Setting items in **Settings** > **General Settings** on the control panel.

Some functions can be set enabled or disabled individually.

General Settings menu	Panel Lock
Basic Settings	-

Product Security Settings

General Settings menu		Panel Lock
	LCD Brightness	-
	Sound	-
	Sleep Timer	✓
	Power Off Timer	✓
	Circuit Breaker Interlock Startup	✓
	Date/Time Settings	✓
	Language	-
	Operation Time Out	✓
	Keyboard	-
	Length Unit	-
Printer Settings		-
	Paper Source Settings	-
	Custom Paper Setting	-
	Printing Language	✓
	Universal Print Settings	✓
	HP-GL/2 Unique Settings	-
	Memory Device Interface[*3]	✓
	Thick Paper	-
	Self Check and Cleaning[*3]	✓
	Bidirectional	-
	PC Connection via USB	✓
	USB I/F Timeout Setting	✓
Network Settings		✓

Product Security Settings

General Settings menu			Panel Lock
	Wi-Fi Setup		✓
	Wired LAN Setup		✓
	Network Status		✓
		Wired LAN/Wi-Fi Status	✓*1
		Wi-Fi Direct Status	✓*1
		Print Status Sheet	✓*1
	Connection Check		✓*2
	Advanced		✓
		Device Name	✓
		TCP/IP	✓
		Proxy Server	✓
		IPv6 Address	✓
		Link Speed & Duplex	✓
		Redirect HTTP to HTTPS	✓
		Disable IPsec/IP Filtering	✓
		Disable IEEE802.1X	✓
System Administration			✓
	Security Settings		✓
		Admin Settings	✓
		Admin Password	✓
		Lock Setting	✓
	Restore Default Settings		✓
	Firmware Update		✓
Maintenance			-

General Settings menu		Panel Lock
	Print Quality Adjustment	-
	Print Head Nozzle Check	-
	Print Head Cleaning	-
	Paper Guide Cleaning*3	-
	Ink Cartridge(s) Replacement	-
	Replace Maintenance Box	-
	Replace Cutter	-
	Powerful Cleaning	✓
	Discharging/Charging Ink	✓

✓ = To be locked.

- = Not to be locked.

*1   : Even though items on the upper level can be locked by administrator lock, you can still access them from the same name menu of **Settings** > **Printer Status/Print**.

*2   : Even though items on the upper level can be locked by administrator lock, you can still access them from Home > 📶 | 📶 > **Description** > **When you cannot connect to the network**.

*3   : This item is not displayed depending on the model.

Disabling the External Interface

You can restrict the USB connection from the computer. Make the restriction settings to restrict printing other than via network.

Note:
You can also make the restriction settings on the printer's control panel.

Settings > *General Settings* > *Printer Settings* > *PC Connection via USB*

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

2. Select **Disable** on PC Connection via USB.

    Select **Enable** when you want to cancel controlling.

3. Click **OK**.

4. Check that the disabled port cannot be used.

    If the driver was installed on the computer

    Connect the printer to the computer using a USB cable, and then confirm that the printer does not print.

    If the driver was not installed on the computer

    Windows:

Product Security Settings

Open the device manager and keep it, connect the printer to the computer using a USB cable, and then confirm that the device manager's display contents stays unchanged.

Mac OS:

Connect the printer to the computer using a USB cable, and then confirm that the printer is not listed if you want to add the printer from **Printers & Scanners**.

Related Information

➡ "Accessing Web Config" on page 27

Operation and Management Settings

This chapter explains the items related to the daily operations and management of the device.

Logging on to the Printer as an Administrator

If the administrator password is set to the printer, you need to log on as an administrator to operate the locked menu items on Web Config.

Enter the password to operate the locked menu items on the control panel.

Logging on to the Printer Using Web Config

When you log in to Web Config as an administrator, you can operate items that are set in the Lock Setting.

1. Enter the printer's IP address into a browser to run Web Config.

2. Click **Administrator Login**.

3. Enter the user name and administrator password in **User Name** and **Current password**.

4. Click **OK**.

   The locked items and **Administrator Logout** are displayed when being authenticated.

   Click **Administrator Logout** to log off.

Note:
*When you select **ON** for the **Device Management** tab > **Control Panel** > **Operation Timeout**, you log off automatically after a specific length of time if there is no activity on the control panel.*

Confirm Information of the Printer

Checking the Information from the Control Panel

You can check and print the following information from the control panel.

❏ Number of printed pages

   Settings > **Print Counter**

   You can check the total number of printed pages and the number of pages of color / monochrome printing.

❏ Supply

   Settings > **Supply Status**

   You can check the information for the ink and maintenance box.

❏ Status sheet for the product

   Settings > **Printer Status/Print** > **Print Status Sheet**

   You can print a status sheet, such as printer information and consumables information.

❏ Network information

Settings > **General Settings** > **Network Settings** > **Network Status**

Settings > **Printer Status/Print** > **Network**

You can check the network-related information such as network connection status, mail server settings, etc. and print the network status sheet.

❏ Network connection report

Settings > **General Settings** > **Network Settings** > **Connection Check**

Home > 📶 | 📶 > **Description** > **When you cannot connect to the network**

You can diagnose the network connection status of the printer and print the report.

❏ Network connection status

Home > 📶 | 📶 > **Router**

You can check the connection status for Wired / Wireless LAN.

Checking the Information from Web Config

You can check the following information of the operating printer from **Status** by using Web Config.

❏ Product Status

Check the language, status, product number, MAC address, etc.

❏ Network Status

Check the information of the network connection status, IP address, DNS server, etc.

❏ Hardware Status

Check the status of each Wi-Fi.

❏ Panel Snapshot

Display a screen image snapshot that is displayed on the control panel of the device.

Receiving Email Notifications When Events Occur

About Email Notifications

This is the notification function that, when events such as printing stop and printer error occur, send the email to the specified address.

You can register up to five destinations and set the notification settings for each destination.

To use this function, you need to set up the mail server before setting up notifications.

Related Information

➡ "Configuring a Mail Server" on page 34

Configuring Email Notification

Configure email notification by using Web Config.

1. Access Web Config and select the **Device Management** tab > **Email Notification**.

2. Set the subject of email notification.

   Select the contents displayed on the subject from the two pull-down menus.

   ❏ The selected contents are displayed next to **Subject**.

   ❏ The same contents cannot be set on left and right.

   ❏ When the number of characters in **Location** exceeds 32 bytes, characters exceeding 32 bytes are omitted.

3. Enter the email address for sending the notification email.

   Use A-Z a-z 0-9 ! # $ % & ' * + - . /= ? ^ _ { | } ~ @, and enter between 1 and 255 characters.

4. Select the language for the email notifications.

5. Select the check box on the event for which you want to receive a notification.

   The number of **Notification Settings** is linked to the destination number of **Email Address Settings**.

   Example :

   If you want a notification sent to the email address set for number 1 in **Email Address Settings** when the printer is out of paper, select the check box column **1** in line **Paper out**.
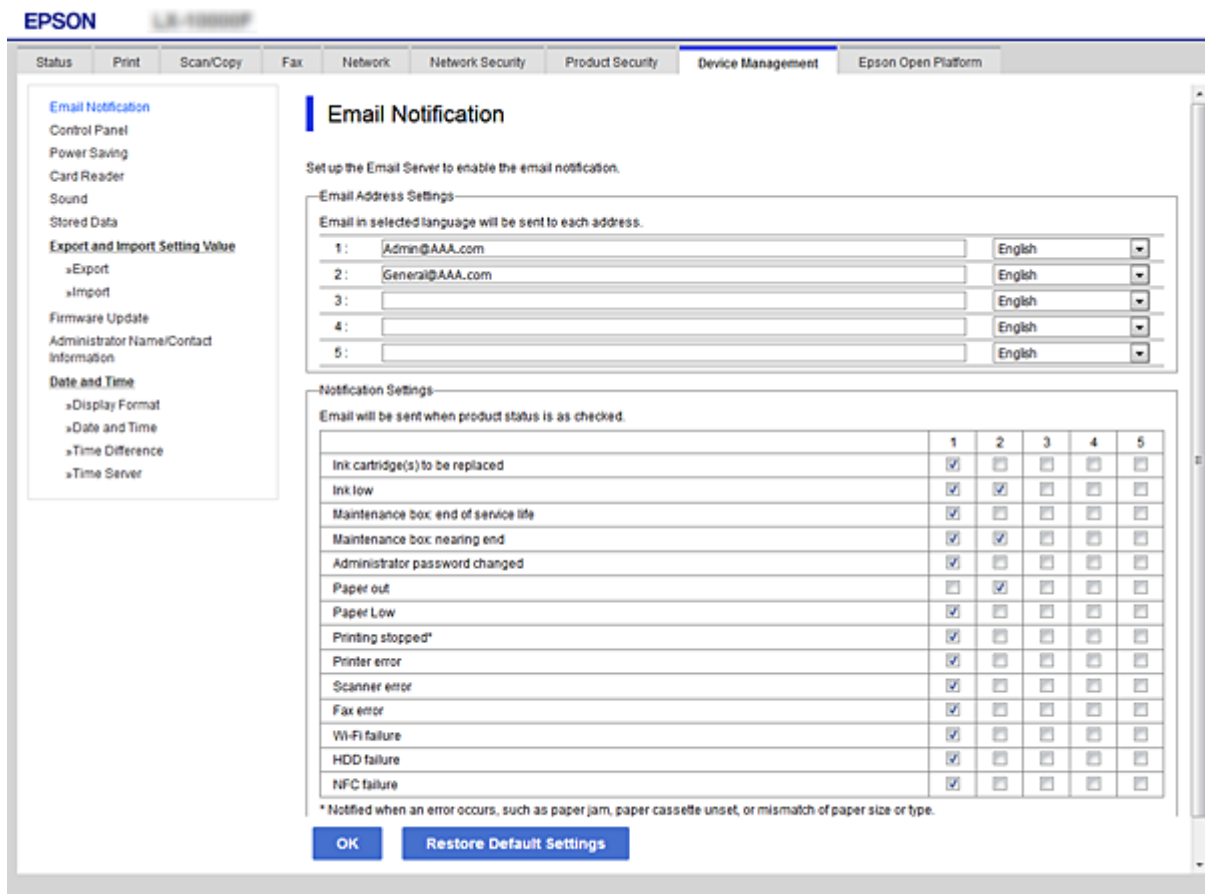
Operation and Management Settings

6. Click **OK**.

   Confirm that an email notification will be sent by causing an event.

   Example : Print by specifying the Paper Source where paper is not set.

Related Information

➡
➡

Items for Email Notification

Items	Settings and Explanation
Ink supply unit(s) to be replaced	Notice when the ink is expended.
Ink low	Notice when the ink is nearing expended.
Maintenance box: end of service life	Notice when the maintenance box is full.
Maintenance box: nearing end	Notice when the maintenance box is nearing full.
Administrator password changed	Notice when administrator password has been changed.
Paper out	Notice when the paper-out error has occurred in the specified paper source..
Printing stopped*	Notice when the printing is stopped due to paper jam or paper cassette not set.
Printer error	Notice when the printer error has occurred.
Wi-Fi failure	Notice when the error of the wireless LAN interface has occurred.
Print Job Completion *2	The printer sends an e-mail each time the number of print jobs set in the pulldown menu is completed.

Updating Firmware

When new firmware is available, updating the firmware of the printer improves the function or resolves the problem.

Updating the Printer's Firmware using the Control Panel

If the printer can be connected to the Internet, you can update the printer's firmware using the control panel. You can also set the printer to regularly check for firmware updates and notify you if any are available.

1. Select **Settings** on the home screen.

2. Select **General Settings** > **System Administration** > **Firmware Update** > **Update**.

   Note:
   *Select **Notification** > **On** to set the printer to regularly check for available firmware updates.*

3. Select **Start Checking**.

    The printer starts searching for available updates.

4. If a message is displayed on the LCD screen informing you that a firmware update is available, follow the on-screen instructions to start the update.

> ❗ *Important:*
> ❏ *Do not turn off or unplug the printer until the update is complete; otherwise, the printer may malfunction.*
> ❏ *If the firmware update is not completed or is unsuccessful, the printer does not start up normally and "Recovery Mode" is displayed on the LCD screen the next time the printer is turned on. In this situation, you need to update the firmware again using a computer. Connect the printer to the computer with a USB cable. While "Recovery Mode" is displayed on the printer, you cannot update the firmware over a network connection. On the computer, access your local Epson website, and then download the latest printer firmware. See the instructions on the website for the next steps.*

Updating Firmware Using Web Config

When the printer can connect to the Internet, you can update the firmware from Web Config.

1. Access Web Config and select the **Device Management** tab > **Firmware Update**.

2. Click **Start**.

    The firmware confirmation starts, and the firmware information is displayed if the updated firmware exists.

3. Click **Start**, and follow the on-screen instructions.

Note:
You can also update the firmware using Epson Device Admin. You can visually confirm the firmware information on the device list. It is useful when you want to update multiple devices' firmware. See the Epson Device Admin guide or help for more details.

Related Information

➡ "Accessing Web Config" on page 27
➡ "Epson Device Admin" on page 72

Updating Firmware without Connecting to the Internet

You can download the device's firmware from Epson website on the computer, and then connect the device and the computer by USB cable to update the firmware. If you cannot update over the network, try this method.

1. Access Epson website and download the firmware.

2. Connect the computer that contains the downloaded firmware to the printer by USB cable.

3. Double-click the downloaded .exe file.

    Epson Firmware Updater starts.

4. Follow the on-screen instructions.

Backing Up the Settings

You can export the setting value set from Web Config to the file. You can use it for backing up the setting values, replacing the printer, etc.

The exported file cannot be edited because it is exported as a binary file.

Export the settings

Export the setting for the printer.

1. Access Web Config, and then select the **Device Management** tab > **Export and Import Setting Value** > **Export**.

2. Select the settings that you want to export.

    Select the settings you want to export. If you select the parent category, subcategories are also selected. However, subcategories that cause errors by duplicating within the same network (such as IP addresses and so on) cannot be selected.

3. Enter a password to encrypt the exported file.

    You need the password to import the file. Leave this blank if you do not want to encrypt the file.

4. Click **Export**.

    > **!** *Important:*
    >
    > *If you want to export the printer's network settings such as the device name and IPv6 address, select **Enable to select the individual settings of device** and select more items. Only use the selected values for the replacement printer.*

Related Information

➡ "Accessing Web Config" on page 27

Import the settings

Import the exported Web Config file to the printer.

> **!** *Important:*
>
> *When importing values that include individual information such as a printer name or IP address, make sure the same IP address does not exist on the same network. If the IP address overlaps, the printer does not reflect the value.*

1. Access Web Config, and then select the **Device Management** tab > **Export and Import Setting Value** > **Import**.

2. Select the exported file, and then enter the encrypted password.

3. Click **Next**.

4. Select the settings that you want to import, and then click **Next**.

Operation and Management Settings

5.   Click **OK**.

The settings are applied to the printer.

Solving Problems

Hints to Solving Problems

❏ Checking the error message

When trouble has occurred, first check whether there are any messages on the printer's control panel or driver screen. If you have the notification email set when the events occur, you can promptly learn the status.

❏ Network connection report

Diagnose the network and the printer status, and then print the result.

You can find the diagnosed error from the printer side.

❏ Checking the communication status

Check the communication status of server computer or client computer by using the command such as ping and ipconfig.

❏ Connection test

For checking the connection between the printer to the mail server, perform the connection test from the printer. Also, check the connection from the client computer to the server to check the communication status.

❏ Initializing the settings

If the settings and communication status show no problem, the problems may be solved by disabling or initializing the network settings of the printer, and then setting up again.

Checking the Status of the Printer

To identify the cause of trouble, check the status of the printer and network.

Checking the Error Message

Checking the Error Message from Email Notification

When setting the email notification, check that the error message is sent from the printer.

If instructions for handling the problem are in the email notification, please follow them.

Related Information

➡ "Receiving Email Notifications When Events Occur" on page 50

Checking Messages on the LCD Screen

If an error message is displayed on the LCD screen, follow the on-screen instructions or the solutions below to solve the problem.

Solving Problems

Error Messages	Causes and Solutions
Printer error. Turn the power off and on again. If the problem persists, contact Epson Support.	❏ **Causes :** There is a foreign substance inside the printer or a printer error occurred. ❏ **Solutions :** Remove any paper or protective material in the printer. If the error message is still displayed, contact Epson support.
You need to replace Ink Cartridge(s).	❏ **Causes :** The ink is expended. ❏ **Solutions :** To ensure you receive premium print quality and to help protect your print head, a variable ink safety reserve remains in the cartridge when your printer indicates it is time to replace the cartridge. Replace the cartridge when you are prompted to do so.
The maintenance box is not recognized. Install it correctly.	❏ **Causes :** The Maintenance Box is not installed correctly. ❏ **Solutions :** Check the maintenance box's installing status, and then install it correctly.
The Maintenance Box is at the end of its service life. You need to replace it.	❏ **Causes :** The Maintenance Box is at the end of its service life. ❏ **Solutions :** Replace the Maintenance Box according to the guidance.
There is not enough space in maintenance box to perform head cleaning. You can continue printing until replacement is required.	❏ **Causes :** The Maintenance Box does not have enough capacity for the head cleaning. ❏ **Solutions :** Turn the power of the printer off, and then replace the Maintenance Box. You can use the replaced Maintenance Box again after the head cleaning.
Remove and reinstall the Maintenance Box.	❏ **Causes :** The Maintenance Box is not recognized correctly. ❏ **Solutions :** Remove the Maintenance Box once, and then install it again. If it is not recognized after all that, replace it to a new Maintenance Box.
The combination of the IP address and the subnet mask is invalid. See your documentation for more details.	❏ **Causes :** The combination of the IP address you set is invalid. ❏ **Solutions :** Enter the correct IP address or default gateway.
To use cloud services, update the root certificate from the Epson Web Config utility.	❏ **Causes :** The root certificate used for cloud services is expired. ❏ **Solutions :** Run Web Config, and then update the root certificate. **Network Security** - **Root Certificate Update**

Solving Problems

Error Messages	Causes and Solutions
Recovery Mode	❏ **Causes :** Failed to update firmware and cannot return to the normal mode. ❏ **Solutions :** The printer has started in recovery mode because the firmware update failed. Follow the steps below to try to update the firmware again. 1. Connect the computer and the printer with a USB cable. (During recovery mode, you cannot update the firmware over a network connection.) 2. Visit your local Epson website for further instructions.

Checking the Panel Display of the Remote Printer

You can check the panel display of the remote printer by using Web Config.

1. Run Web Config of the printer that you want to check.

   When you receive the email notification, you can run Web Config from the URL on the email.

2. Select **Status** tab > **Panel Snapshot**.

   The current panel of the printer is displayed on Web Config.

   To update, click **Refresh**.

Printing a Network Connection Report

You can print a network connection report to check the status between the printer and the access point.

1. Load papers.

2. Select **Settings** on the home screen.

3. Select **General Settings** > **Network Settings** > **Connection Check**.

   The connection check starts.

4. Select **Print Check Report**.

5. Print the network connection report.

   If an error has occurred, check the network connection report, and then follow the printed solutions.

6. Close the screen.

Related Information

➡ "Messages and Solutions on the Network Connection Report" on page 59

Messages and Solutions on the Network Connection Report

Check the messages and error codes on the network connection report, and then follow the solutions.
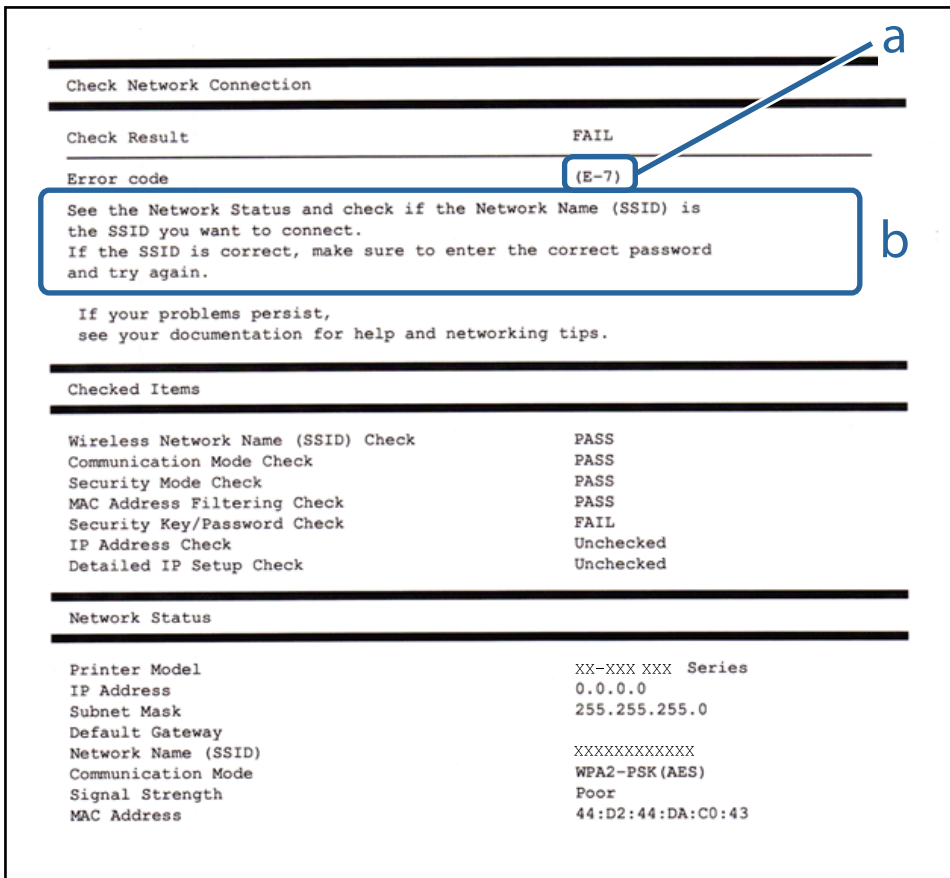
a. Error code

b. Messages on the Network Environment

E-1

Message:

Confirm that the network cable is connected and network devices such as hub, router, or access point are turned on.

Solutions:

❏ Make sure the Ethernet cable is securely connected to your printer and to your hub or other network device.

❏ Make sure your hub or other network device is turned on.

❏ If you want to connect the printer by Wi-Fi, make Wi-Fi settings for the printer again because it is disabled.

Solving Problems

E-2, E-3, E-7

Message:

No wireless network names (SSID) found. Confirm that the router/access point is turned on and the wireless network (SSID) is set up correctly. Contact your network administrator for assistance.

No wireless network names (SSID) found. Confirm that the wireless network name (SSID) of the PC you wish to connect is set up correctly. Contact your network administrator for assistance.

Entered security key/password does not match the one set for your router/access point. Confirm security key/password. Contact your network administrator for assistance.

Solutions:

❏ Make sure your access point is turned on.

❏ Confirm that your computer or device is connected correctly to the access point.

❏ Turn off the access point. Wait for about 10 seconds, and then turn it on.

❏ Place the printer closer to your access point and remove any obstacles between them.

❏ If you have entered the SSID manually, check if it is correct. Check the SSID from the **Network Status** part on the network connection report.

❏ If an access point has multiple SSIDs, select the SSID that is displayed. When the SSID is using a non-compliant frequency, the printer does not display them.

❏ If you are using push button setup to establish a network connection, make sure your access point supports WPS. You cannot use push button setup if your access point does not support WPS.

❏ Makes sure your SSID uses only ASCII characters (alphanumeric characters and symbols). The printer cannot display an SSID that contains non-ASCII characters.

❏ Makes sure you know your SSID and password before connecting to the access point. If you are using an access point with its default settings, the SSID and password are located on a label on the access point. If you do not know your SSID and password, contact the person who set up the access point, or see the documentation provided with the access point.

❏ If you are connecting to an SSID generated from a tethering smart device, check for the SSID and password in the documentation provided with the smart device.

❏ If your Wi-Fi connection suddenly disconnects, check for the conditions below. If any of these conditions are applicable, reset your network settings by downloading and running the software from the following website.

http://epson.sn > **Setup**

 ❏ Another smart device was added to the network using push button setup.

 ❏ The Wi-Fi network was set up using any method other than push button setup.

E-5

Message:

Security mode (e.g. WEP, WPA) does not match the current setting of the printer. Confirm security mode. Contact your network administrator for assistance.

Solutions:

Make sure the access point's security type is set to one of the following. If it is not, change the security type on the access point, and then reset the printer's network settings.

❏ WEP-64 bit (40 bit)

❏ WEP-128 bit (104 bit)

❏ WPA PSK (TKIP/AES)*

❏ WPA2 PSK (TKIP/AES)*

❏ WPA (TKIP/AES)

❏ WPA2 (TKIP/AES)

* WPA PSK is also known as WPA Personal. WPA2 PSK is also known as WPA2 Personal.

E-6

Message:

MAC address of your printer may be filtered. Check whether your router/access point has restrictions such as MAC address filtering. See the documentation of the router/access point or contact your network administrator for assistance.

Solutions:

❏ Check if MAC address filtering is disabled. If it is enabled, register the printer's MAC address so that it is not filtered. See the documentation provided with the access point for details. You can check the printer's MAC address from the **Network Status** part on the network connection report.

❏ If your access point is using shared authentication with WEP security, make sure the authentication key and index are correct.

❏ If the number of connectable devices on the access point is less than the number of network devices that you want to connect, make settings on the access point to increase the number of connectable devices. See the documentation provided with the access point to make settings.

E-8

Message:

Incorrect IP address is assigned to the printer. Confirm IP address setup of the network device (hub, router, or access point). Contact your network administrator for assistance.

Solutions:

❏ Enable DHCP on the access point if the printer's Obtain IP Address setting is set to **Auto**.

❏ If the printer's Obtain IP Address setting is set to Manual, the IP address you manually set is invalid due to out of range (for example: 0.0.0.0). Set a valid IP address from the printer's control panel or by using Web Config.

Solving Problems

E-9

Message:

Confirm the connection and network setup of the PC or other device. Connection using the EpsonNet Setup is available. Contact your network administrator for assistance.

Solutions:

Check the following.

❏ Devices are turned on.

❏ You can access the Internet and other computers or network devices on the same network from the devices you want to connect to the printer.

If still does not connect your printer and network devices after confirming the above, turn off the access point. Wait for about 10 seconds, and then turn it on. Then reset your network settings by downloading and running the installer from the following website.

http://epson.sn > **Setup**

E-10

Message:

Confirm IP address, subnet mask, and default gateway setup. Connection using the EpsonNet Setup is available. Contact your network administrator for assistance.

Solutions:

Check the following.

❏ Other devices on the network are turned on.

❏ Network addresses (IP address, subnet mask, and default gateway) are correct if you have set the printer's Obtain IP Address to Manual.

Reset the network address if they are incorrect. You can check the IP address, subnet mask, and default gateway from the **Network Status** part on the network connection report.

If DHCP is enabled, change the printer's Obtain IP Address setting to **Auto**. If you want to set the IP address manually, check the printer's IP address from the **Network Status** part on the network connection report, and then select Manual on the network settings screen. Set the subnet mask to [255.255.255.0].

If still does not connect your printer and network devices, turn off the access point. Wait for about 10 seconds, and then turn it on.

E-11

Message:

Setup is incomplete. Confirm default gateway setup. Connection using the EpsonNet Setup is available. Contact your network administrator for assistance.

Solutions:

Check the following.

❑ The default gateway address is correct if you set the printer's TCP/IP Setup setting to Manual.

❑ The device that is set as the default gateway is turned on.

Set the correct default gateway address. You can check the default gateway address from the **Network Status** part on the network connection report.

E-12

Message:

Confirm the following: -Entered security key/password is correct -Index of the security key/password is set to the first number -IP address, subnet mask, or default gateway setup is correct Contact your network administrator for assistance.

Solutions:

Check the following.

❑ Other devices on the network are turned on.

❑ The network addresses (IP address, subnet mask, and default gateway) are correct if you are entering them manually.

❑ The network addresses for other devices (subnet mask and default gateway) are the same.

❑ The IP address does not conflict with other devices.

If still does not connect your printer and network devices after confirming the above, try the following.

❑ Turn off the access point. Wait for about 10 seconds, and then turn it on.

❑ Make network settings again using the installer. You can run it from the following website.

http://epson.sn > **Setup**

❑ You can register several passwords on an access point that uses WEP security type. If several passwords are registered, check if the first registered password is set on the printer.

E-13

Message:

Confirm the following: -Entered security key/password is correct -Index of the security key/password is set to the first number -Connection and network setup of the PC or other device is correct Contact your network administrator for assistance.

Solutions:

Check the following.

❑ Network devices such as an access point, hub, and router are turned on.

❑ The TCP/IP Setup for network devices has not been set up manually. (If the printer's TCP/IP Setup is set automatically while the TCP/IP Setup for other network devices is performed manually, the printer's network may differ from the network for other devices.)

If it still does not work after checking the above, try the following.

❏ Turn off the access point. Wait for about 10 seconds, and then turn it on.

❏ Make network settings on the computer that is on the same network as the printer using the installer. You can run it from the following website.

   http://epson.sn > **Setup**

❏ You can register several passwords on an access point that uses the WEP security type. If several passwords are registered, check if the first registered password is set on the printer.

Message on the Network Environment

Message	Solution
*Multiple network names (SSID) that match your entered network name (SSID) have been detected. Confirm network name (SSID).	The same SSID may be set on several access points. Check the settings on the access points, and change the SSID.
The Wi-Fi environment needs to be improved. Turn the wireless router off and then turn it on. If the connection does not improve, see the documentation for the wireless router.	After moving the printer closer to the access point and removing any obstacles between them, turn off the access point. Wait for about 10 seconds, and then turn it on. If it still does not connect, see the documentation supplied with the access point.
*No more devices can be connected. Disconnect one of the connected devices if you want to add another one.	Computer and smart devices that can be connected simultaneously are connected in full in the Wi-Fi Direct (Simple AP) connection. To add another computer or smart device, disconnect one of the connected devices first. You can confirm the number of wireless devices which can be connected simultaneously and the number of connected devices by checking the network status sheet or the printer's control panel.

Checking the Communication Status

Check whether the communication between the printer and the computer is correct, and lead to solve the problems.

Checking Log for Server and Network Device

In case of trouble with network connection, it may be possible to identify the cause by confirming the log of the mail server, etc., checking the status using the network log of system equipment logs and commands, such as routers.

Printing a Network Status Sheet

You can check the detailed network information by printing it.

1. Load papers.

2. Select **Settings** on the home screen.

3. Select **General Settings** > **Network Settings** > **Network Status**.

Solving Problems

4. Select **Print Status Sheet**.

5. Check the message, and then print the network status sheet.

6. Close the screen.

   The screen automatically closes after a specific length of time.

Checking the Communication between Devices and Computers

Checking the Communication Using a Ping Command - Windows

You can use a Ping command to make sure the computer is connected to the printer. Follow the steps below to check the communication using a Ping command.

1. Check the printer's IP address for the communication that you want to check.

   You can check this from the Network Status screen on the printer's control panel, a connection report, or the **IP Address** column of a network status sheet.

2. Display the computer's command prompt screen.

   Display the application screen, and then select **Command Prompt**.

3. Enter 'ping xxx.xxx.xxx.xxx', and then press the Enter key.

   Enter the printer's IP address for xxx.xxx.xxx.xxx.

4. Check the communication status.

   If the printer and the computer are communicating, the following message is displayed.

   If the printer and the computer are not communicating, the following message is displayed.
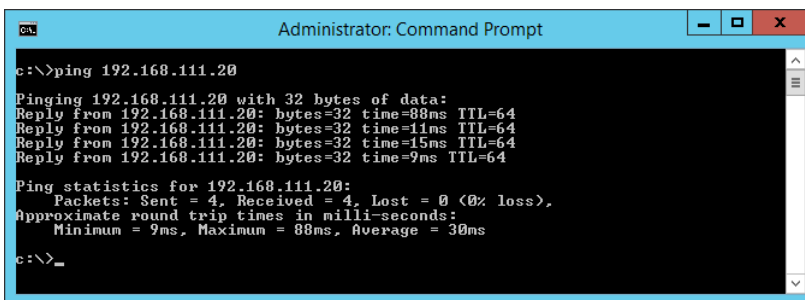
Solving Problems

Checking the Communication Using a Ping Command - Mac OS

You can use a Ping command to make sure the computer is connected to the printer. Follow the steps below to check the communication using a Ping command.

1. Check the printer's IP address for the communication that you want to check.

   You can check this from the Network Status screen on the printer's control panel, a connection report, or the **IP Address** column of a network status sheet.

2. Run Network Utility.

   Enter "Network Utility" in **Spotlight**.

3. Click the **Ping** tab, enter the IP address that you checked in step 1, and then click **Ping**.

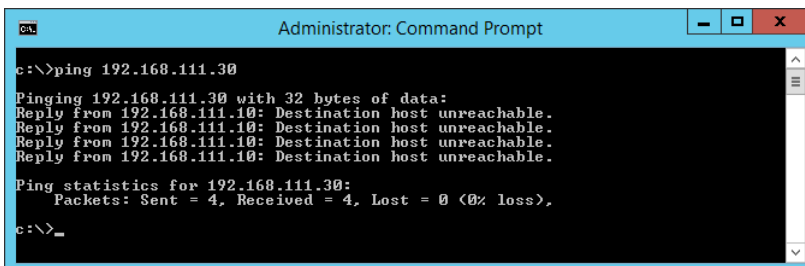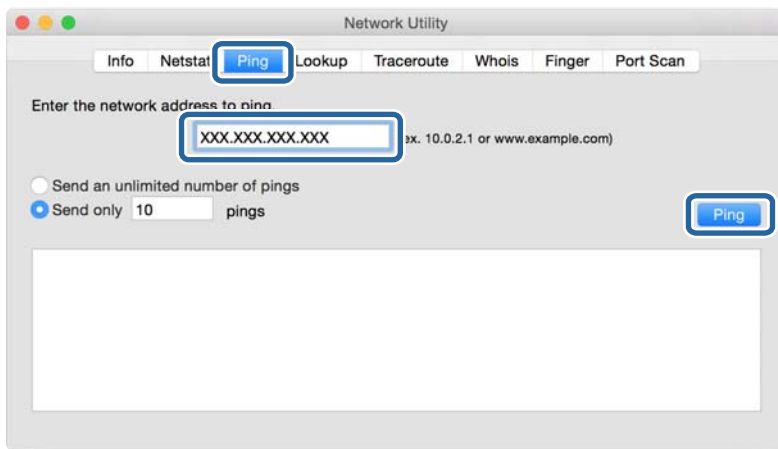

4. Check the communication status.

   If the printer and the computer are communicating, the following message is displayed.
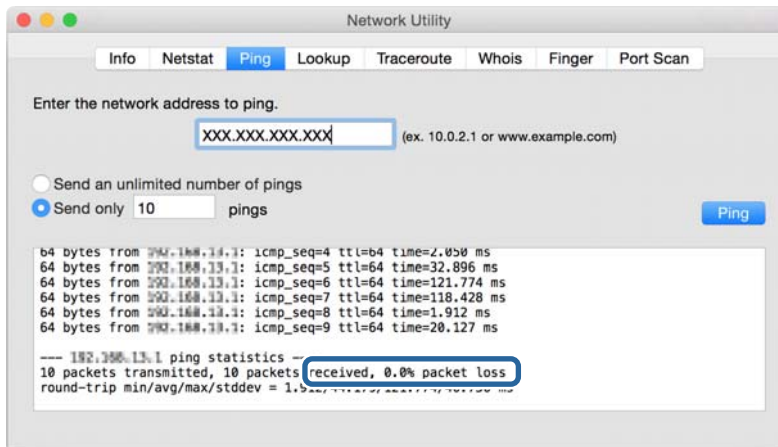
Solving Problems

If the printer and the computer are not communicating, the following message is displayed.
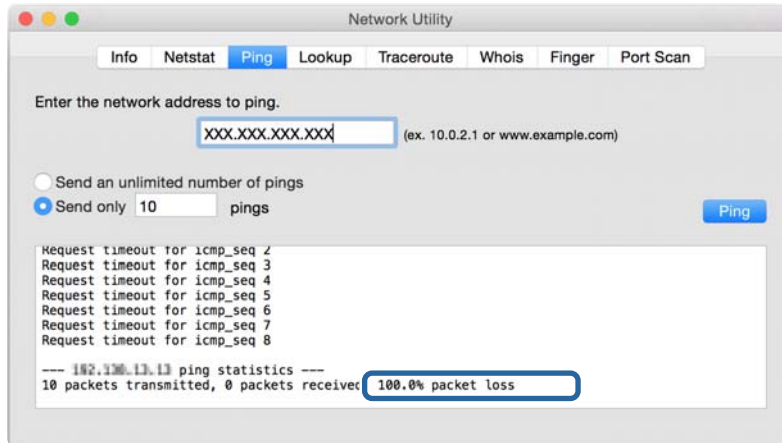
Checking the Network of the Computer - Windows

By using the command prompt, check the connection status of the computer and the connection path to the printer. This will lead you to solve the problems.

❏ ipconfig command

Display the connection status of the network interface that is currently used by the computer.

By comparing the setting information with actual communication, you can check whether the connection is correct. In case there are multiple DHCP servers on the same network, you can find out the actual address assigned to the computer, the referred DNS server, etc.

❏ Format : ipconfig /all

❏ Examples :
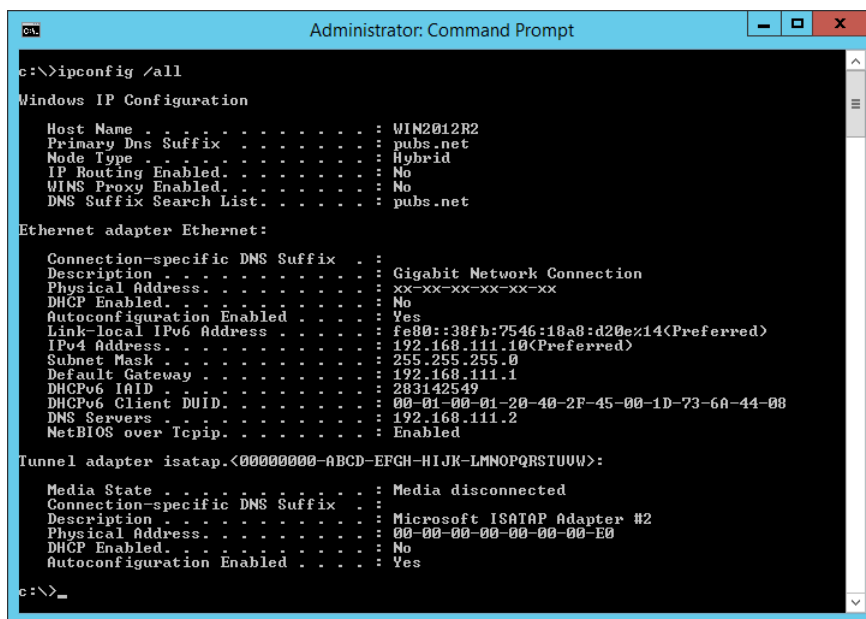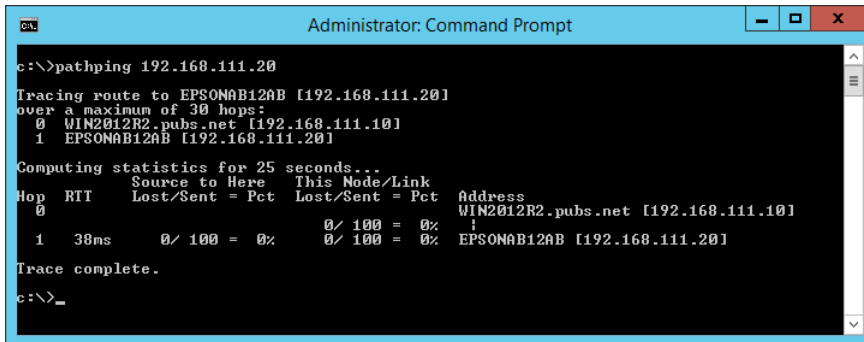
Solving Problems

❏ pathping command

You can confirm the list of routers passing through the destination host and the routing of communication.

❏ Format : pathping xxx.xxx.xxx.xxx

❏ Examples : pathping 192.0.2.222

Performing the Connection Test

From the printer or the computer connected to the same segment as the printer, check whether the connection with the server and folder is correct. This will lead you to solve the problems.

Mail Server

Check the connection between the printer and the mail server by using the connection test function of the printer.

Related Information

➡

DNS Server

Check the DNS server that is referred by the computer. Confirm the status of the network adapter of the computer on the same network segment as the printer, and confirm whether it is the same as the DNS setting of the printer.

You can check the DNS setting of the computer as follows.

❏ Windows : **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Change adapter settings**

When there are multiple network interfaces, you can check by entering "ipconfig/all" on the command prompt.

❏ Mac OS : **System Preference** > **Network** > **Advanced...** > **DNS**

Initializing the Network Settings

Disabling Wi-Fi from Web Config

Disable Wi-Fi from Web Config. If you disable Wi-Fi while some devices are connected by Wi-Fi, they are disconnected.

Solving Problems

1. Access Web Config and select the **Network** tab > **Wi-Fi**, and then select **Disable Wi-Fi**.

2. Check the message, and then select **OK**.

Disconnecting Wi-Fi Direct (Simple AP) from Web Config

Disconnect Wi-Fi Direct (simple AP) from Web Config.

1. Access Web Config and select the **Network** tab > **Wi-Fi Direct**.

2. Select **Disable** for **Wi-Fi Direct**.

3. Click **Next**

4. Check the message, and then select **OK**.

Disabling Wi-Fi from the Control Panel

When Wi-Fi is disabled, the Wi-Fi connection is disconnected.

1. Tap [icon] | [icon] on the home screen.

2. Select **Router**.

   The network status is displayed.

3. Tap **Change Settings**.

4. Select **Others** > **Disable Wi-Fi**.

5. Check the message, and then start setup.

6. When a completion message is displayed, close the screen.

   The screen automatically closes after a specific length of time.

7. Close the Network Connection Settings screen.

8. Press the [home icon] button.

Disconnecting Wi-Fi Direct (Simple AP) Connection from the Control Panel

Note:
When Wi-Fi Direct (Simple AP) connection disabled, all computers and smart devices connected to the printer in Wi-Fi Direct (Simple AP) connection are disconnected. If you want to disconnect a specific device, disconnect from the device instead of the printer.

1. Tap [icon] | [icon] on the home screen.

2. Select **Wi-Fi Direct**.

   The Wi-Fi Direct information is displayed.

Solving Problems

3. Tap **Change Settings**.

4. Select **Disable Wi-Fi Direct**.

5. Tap the **Disable the settings**.

6. When a completion message is displayed, close the screen.

   The screen automatically closes after a specific length of time.

Restoring the Network Settings from the Control Panel

You can restore all network settings to their defaults.

1. Select **Settings** on the home screen.

2. Select **General Settings** >**System Administration** >**Restore Default Settings** > **Network Settings**.

3. Check the message, and then select **Yes**.

4. When a completion message is displayed, close the screen.

   The screen automatically closes after a specific length of time.

Trouble Case

Cannot Access Web Config

The IP address is not assigned to the printer.

A valid IP address may not be assigned to the printer. Configure the IP address using the printer's control panel. You can confirm the current setting information with a network status sheet or from the printer's control panel.

Web browser does not support the Encryption Strength for SSL/TLS.

SSL/TLS has the Encryption Strength. Web Config can be opened by the web browser that supports the bulk encryptions as follows. Check your browser's encryption support.

❑ 80bit: AES256/AES128/3DES

❑ 112bit: AES256/AES128/3DES

❑ 128bit: AES256/AES128

❑ 192bit: AES256

❑ 256bit: AES256

CA-signed Certificate is expired.

If there is a problem with the expiration date of the certificate, "The certificate has expired" is displayed when connecting to Web Config with SSL/TLS communication (https). If the message appears before its expiration date, make sure that the printer's date is configured correctly.

Solving Problems

The common name of the certificate and the printer do not match.

If the common name of the certificate and the printer do not match, the message "The name of the security certificate does not match⋯" is displayed when accessing Web Config using SSL/TLS communication (https). This happens because the following IP addresses do not match.

❏ The printer's IP address entered to common name for creating a Self-signed Certificate or CSR

❏ IP address entered to web browser when running Web Config

For Self-signed Certificate, change the printer name. The certificate is updated and the printer can be connected.

For CA-signed Certificate, take the certificate again for the printer.

The proxy server setting of local address is not set to web browser.

When the printer is set to use a proxy server, configure the web browser not to connect to the local address via the proxy server.

❏ Windows:

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

❏ Mac OS:

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

➡ "Accessing Web Config" on page 27

➡ "Assigning the IP Address" on page 20

Appendix

Introduction of Network Software

The following describes the software that configures and manages devices.

Epson Device Admin

Epson Device Admin is a multifunctional application software that manages the device on the network.

The following functions are available.

❏ Monitor or manage up to 2,000 printers or scanners over the segment

❏ Make a detailed report, such as for the consumable or product status

❏ Update the firmware of the product

❏ Introduce the device to the network

❏ Apply the unified settings to multiple devices.

You can download Epson Device Admin from Epson support website. For more information, see the documentation or help of Epson Device Admin.

Running Epson Device Admin (Windows only)

Select **All Programs** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Note:
If the firewall alert appears, allow access for Epson Device Admin.

EpsonNet Config

EpsonNet Config is an application software that can make settings to the device on the network. When the devices are connected to the network via Ethernet, you can make settings, such as setting the IP address, changing the connection method and so on even for devices not assigned to the IP address. This also can be used to make network settings to the devices without the control panel.

Appendix

For more information, see the documentation or help of EpsonNet Config.

Running EpsonNet Config - Windows

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

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

Running EpsonNet Config - Mac OS

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

EpsonNet Print (Windows Only)

EpsonNet Print is a software to print on the TCP/IP network. This is installed from the installer together with the printer driver. To perform network printing, create an EpsonNet Print port. There are features and restrictions listed below.

❏ 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 various protocols.

❏ IPv6 address is not supported.

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.

Appendix

Making Wi-Fi Settings from the Control Panel (WPS)

You can connect to Wi-Fi from the printer's control panel using the WPS function.

Related Information

Making Wi-Fi Settings by Push Button Setup (WPS)

You can automatically set up a Wi-Fi network by pressing a button on the access point. If the following conditions are met, you can set up by using this method.

❏ The access point is compatible with WPS (Wi-Fi Protected Setup).

❏ The current Wi-Fi connection was established by pressing a button on the access point.

Note:
If you cannot find the button or you are setting up using the software, see the documentation provided with the access point.

1. Tap 📶 | 📶 on the home screen.

2. Select **Router**.

3. Tap **Start Setup**.

   If the network connection is already set up, the connection details are displayed. Tap **Change to Wi-Fi connection.** or **Change Settings** to change the settings.

4. Select **Push Button Setup(WPS)**.

5. Hold down the [WPS] button on the access point until the security light flashes.
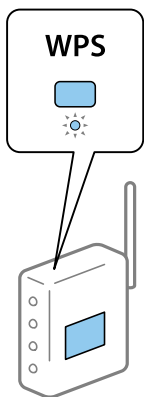
   If you do not know where the [WPS] button is, or there are no buttons on the access point, see the documentation provided with your access point for details.

6. Tap **Start Setup**.

7. Close the screen.

   The screen automatically closes after a specific length of time.

   Note:
   If connection fails, restart the access point, move it closer to the printer, and try again. If it still does not work, print a network connection report and check the solution.

8. Close the network connection settings screen.

Making Wi-Fi Settings by PIN Code Setup (WPS)

You can automatically connect to an access point by using a PIN code. You can use this method to set up if an access point is capable of WPS (Wi-Fi Protected Setup). Use a computer to enter a PIN code into the access point.

1. Tap 　 | 　 on the home screen.

2. Select **Router**.

3. Tap **Start Setup**.

   If the network connection is already set up, the connection details are displayed. Tap **Change to Wi-Fi connection.** or **Change Settings** to change the settings.

4. Select **Others** > **PIN Code Setup(WPS)**

5. Use your computer to enter the PIN code (an eight digit number) displayed on the printer's control panel into the access point within two minutes.

   Note:
   See the documentation provided with your access point for details on entering a PIN code.

6. Tap **Start Setup**.

7. Close the screen.

   The screen automatically closes after a specific length of time if you do not select **Close**.

   Note:
   If connection fails, restart the access point, move it closer to the printer, and try again. If it still does not work, print a connection report and check the solution.

8. Close the network connection settings screen.

Using Wi-Fi Direct (Simple AP) Connection

Wi-Fi Direct (simple AP) connection connects the printer and devices directly.

Because the printer can be connected directly without going through the connected network, it can be used as temporary connection of the device to the printer that is connected to the network without access authority.

Appendix

Enabling Wi-Fi Direct (Simple AP) from the Control Panel

1. Select [icon] | [icon] on the printer's control panel.

2. Select **Wi-Fi Direct**.

   When the Wi-Fi Direct (simple AP) connection is enabled, Wi-Fi connection information is displayed.

3. Select **Start Setup**.

4. Select **Start Setup**.

   When Wi-Fi Direct (simple AP) connection is enabled, network (SSID) and password is displayed.

5. Close the screen.

   Note:
   From smart devices, connect to the printer using the network (SSID) and password displayed on the printer's control panel.

Changing the Wi-Fi Direct (Simple AP) Settings

When Wi-Fi Direct (simple AP) connection is enabled, you can change the settings from [icon] | [icon] > **Wi-Fi Direct** > **Change Settings**, and then the following menu items are displayed.

Changing password

Change the Wi-Fi Direct (simple AP) password for connecting to the printer to your arbitrary value. You can set the password in ASCII characters that is displayed on the software keyboard on the control panel.

When changing the password, all connected devices are disconnected. Use the new password if you want to re-connect the device.

Disabling Wi-Fi Direct (simple AP)

Disable Wi-Fi Direct (simple AP) settings of the printer. When disabling it, all devices connected to the printer in Wi-Fi Direct (Simple AP) connection are disconnected.

Deleting the information of the smart device

Delete the (registered) information of the smart device saved to the printer when connecting by Wi-Fi Direct (simple AP).

If you have an Android device that supports Wi-Fi Direct function, you can connect it to the printer by using that function. The printer keeps the device information if you register the device as a permitted device or a rejected device when connecting by Wi-Fi Direct function. Registered device is permitted or rejected when connecting by Wi-Fi Direct function next time depending on the registered information of the printer.

Note:
To enable/disable Wi-Fi Direct (simple AP) or delete the information of the registered device, you can also set up from
Network tab > Wi-Fi Direct on Web Config.

Appendix

Changing the Connection Method

Change the connection method. Make this setting on the network enabling condition.

If the IP address assignment setting is manual, confirm with the network administrator whether the same IP address can be used on the new network.

Note:
When the Wi-Fi connection is enabled, the Ethernet connection is disabled.

Related Information

➡
➡

Changing from Ethernet Connection to Wi-Fi Connection

Changing to Wi-Fi Connection from the Control Panel

Change the Ethernet connection to Wi-Fi connection from the printer's control panel. The changing connection method is basically the same as the Wi-Fi connection settings. See the topic in this guide on Wi-Fi connection settings from the printer's control panel.

Related Information

➡

Changing to Wi-Fi Connection by Using Web Config

Change the Ethernet connection to Wi-Fi connection by using Web Config.

1. Access Web Config and select the **Network** tab > **Wi-Fi**.

   When the administrator password has been set, log in as an administrator by entering the user name and password.

2. Click **Setup**.

3. Select the SSID for the access point and enter the password.

   If the SSID you want to connect to is not displayed, select **Enter SSID** and enter the SSID.

4. Click **Next**.

5. Confirm the displayed message and click **OK**.

6. Disconnect the Ethernet cable from the printer.

Note:
You can also change the connection method by using Epson Device Admin. For details, see the manual or help for Epson Device Admin.

Appendix

Related Information

➡

➡

Changing from Wi-Fi Connection to Ethernet Connection

Changing the Network Connection to Ethernet from the Control Panel

Follow the steps below to change the network connection to Ethernet from Wi-Fi using the control panel.

1. Select **Settings** on the home screen.

2. Select **General Settings** > **Network Settings** > **Wired LAN Setup**.

3. Tap **Start Setup**.

4. Check the message, and then close the screen.

   The screen automatically closes after a specific length of time.

5. Connect the printer to a router using an Ethernet cable.

Related Information

➡

Changing to Ethernet Connection Using Web Config

Change the Wi-Fi connection to Ethernet connection by using Web Config.

1. Access Web Config and select the **Network** tab > **Wi-Fi**.

   When the administrator password has been set, log in as an administrator by entering the user name and password.

2. Click **Disable Wi-Fi**.

3. Check the message, and then select **OK**.

4. Connect the printer and hub (LAN switch) by Ethernet cable.

Note:
You can also change the connection method by using Epson Device Admin. For details, see the guide or help for Epson Device Admin.

Related Information

➡

➡

Using Port for the Printer

The printer uses the following port. These ports should be allowed to become available by the network administrator as necessary.

Sender (Client)	Use	Destination (Server)	Protocol	Port Number
Printer	Control WSD	Client computer	WSD (TCP)	5357
Client computer	Discover the printer from an application such as EpsonNet Config and printer driver.	Printer	ENPC (UDP)	3289
	Collect and set up the MIB information from an application such as EpsonNet Config and printer driver.	Printer	SNMP (UDP)	161
	Forwarding LPR data	Printer	LPR (TCP)	515
	Forwarding RAW data	Printer	RAW (Port9100) (TCP)	9100
	Forwarding AirPrint (IPP/IPPS printing) data	Printer	IPP/IPPS (TCP)	631
	Searching WSD printer	Printer	WS-Discovery (UDP)	3702

Advanced Security Settings for Enterprise

In this chapter, we describe advanced security features.

Security Settings and Prevention of Danger

When a printer is connected to a network, you can access it from a remote location. In addition, many people can share the printer, which is helpful in improving operational efficiency and convenience. However, risks such as illegal access, illegal use, and tampering with data are increased. If you use the printer in an environment where you can access the Internet, the risks are even higher.

For printers that do not have access protection from the outside, it will be possible to read the print job logs that are stored in the printer from the Internet.

In order to avoid this risk, Epson printers have a variety of security technologies.

Set the printer as necessary according to the environmental conditions that have been built with the customer's environment information.

Name	Feature type	What to set	What to prevent
SSL/TLS communications	The communication content is encrypted with SSL/TLS communications when accessing the Epson server from the printer, such as communicating to the computer via web browser or updating firmware.	Obtain a CA-signed certificate, and then import it to the printer.	Clearing an identification of the printer by the CA-signed certification prevents impersonation and unauthorized access. In addition, communication contents of SSL/TLS are protected, and it prevents the leakage of contents for printing data and setup information.
Control of protocol	Controls the protocols and services to be used for communication between printers and computers, and it enables and disables features.	A protocol or service that is applied to features allowed or prohibited separately.	Reducing security risks that may occur through unintended use by preventing users from using unnecessary functions.
IPsec/IP filtering	You can set to allow severing and cutting off of data that is from a certain client or is a particular type. Since IPsec protects the data by IP packet unit (encryption and authentication), you can safely communicate unsecured protocol.	Create a basic policy and individual policy to set the client or type of data that can access the printer.	Protect unauthorized access, and tampering and interception of communication data to the printer.
IEEE802.1X	Allows only a user who is authenticated to Wi-Fi and Ethernet to connect. Allows only a permitted user to use the printer.	Authentication setting to the RADIUS server (authentication sever).	Protect unauthorized access and use to the printer.

Related Information

Security Feature Settings

When setting IPsec/IP filtering or IEEE802.1X, it is recommended that you access Web Config using SSL/TLS to communicate settings information in order to reduce security risks such as tampering or interception.

Also, you can use Web Config by connecting the printer directly to the computer using an Ethernet cable, and then entering the IP address into a web browser. The printer can be connected in a secure environment after the security settings have been completed.

SSL/TLS Communication with the Printer

When the server certificate is set using SSL/TLS (Secure Sockets Layer/Transport Layer Security) communication to the printer, you can encrypt the communication path between computers. Do this if you want to prevent remote and unauthorized access.

About Digital Certification

❏ CA-signed Certificate

This is a certificate signed by the CA (Certificate Authority.) You can obtain it to apply to the Certificate Authority. This certificate certifies the existence of the printer is and used for SSL/TLS communication so that you can ensure the safety of data communication.

When it is used for SSL/TLS communication, it is used as a server certificate.

When it is set to IPsec/IP Filtering or IEEE802.1x communication, it is used as a client certificate.

❏ CA Certificate

This is a certificate that is in chain of the CA-signed Certificate, also called the intermediate CA certificate. It is used by the web browser to validate the path of the printer's certificate when accessing the server of the other party or Web Config.

For the CA Certificate, set when to validate the path of server certificate accessing from the printer. For the printer, set to certify the path of the CA-signed Certificate for SSL/TLS connection.

You can obtain the CA certificate of the printer from the Certification Authority where the CA certificate is issued.

Also, you can obtain the CA certificate used to validate the server of the other party from the Certification Authority that issued the CA-signed Certificate of the other server.

❏ Self-signed Certificate

This is a certificate that the printer signs and issues itself. It is also called the root certificate. Because the issuer certifies itself, it is not reliable and cannot prevent impersonation.

Use it when making the security setting and performing simple SSL/TLS communication without the CA-signed Certificate.

If you use this certificate for an SSL/TLS communication, a security alert may be displayed on a web browser because the certificate is not registered on a web browser. You can use the Self-signed Certificate only for an SSL/TLS communication.

Related Information

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 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 Web Config, and then select the **Network Security** tab. Next, select **SSL/TLS** > **Certificate** or **IPsec/IP Filtering** > **Client Certificate** or **IEEE802.1X** > **Client Certificate**.

   Whatever you choose, you can obtain the same certificate and use it in common.

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 the **Network Security** tab. Next, select **SSL/TLS** > **Certificate**, or **IPsec/IP Filtering** > **Client Certificate** or **IEEE802.1X** > **Client 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.

Advanced Security Settings for Enterprise

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. You can enter 1 to 5 IPv4 addresses, IPv6 addresses, host names, FQDNs by separating them with commas. The first element is stored to the common name, and other elements are stored to the alias field of the certificate subject. Example: Printer's IP address : 192.0.2.123, Printer name : EPSONA1B2C3 Common Name : EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organization/ Organizational Unit/ Locality/ State/Province	You can enter between 0 and 64 characters (Organizational Unit cannot exceed 55 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

Import the obtained CA-signed Certificate to the printer.

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

1. Access Web Config and then select the **Network Security** tab. Next, select **SSL/TLS** > **Certificate**, or **IPsec/IP Filtering** > **Client Certificate** or **IEEE802.1X** > **Client Certificate**.

2. Click **Import**

   A certificate importing page is opened.

3. Enter a value for each item. Set **CA Certificate 1** and **CA Certificate 2** when verifying the path of the certificate on the web browser that accesses the printer.

   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 27
➡ "CA-signed Certificate Importing Setting Items" on page 86

Advanced Security Settings for Enterprise

CA-signed Certificate Importing Setting Items
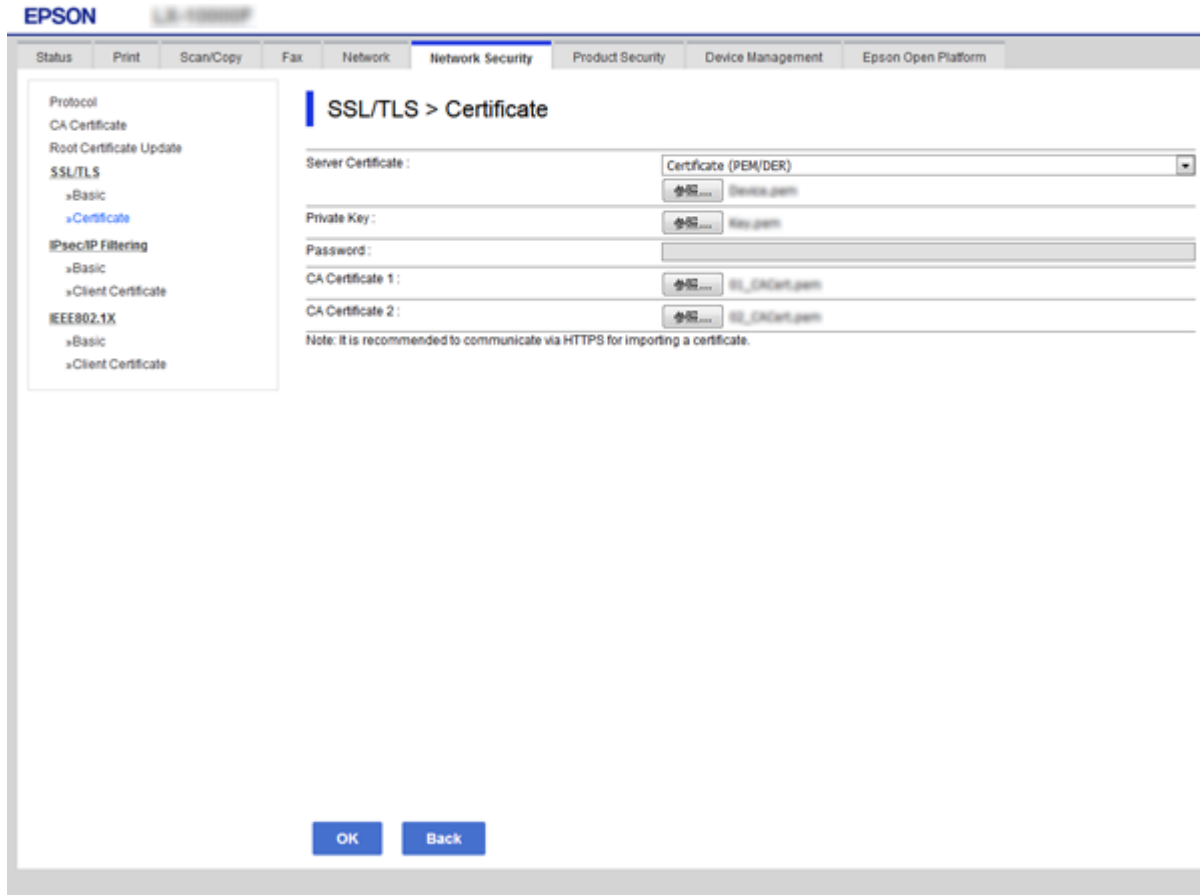
Items	Settings and Explanation
Server Certificate or Client Certificate	Select a certificate's format. For SSL/TLS connection, the Server Certificate is displayed. For IPsec/IP Filtering or IEEE802.1x, the Client Certificate is displayed.
Private Key	If you obtain a certificate of the PEM/DER format by using a CSR created from a computer, specify a private key file that is match a certificate.
Password	If the file format is **Certificate with Private Key (PKCS#12)**, enter the password for encrypting the private key that is set when you obtain the certificate.
CA Certificate 1	If your certificate's format is **Certificate (PEM/DER)**, import a certificate of a certificate authority that issues a CA-signed Certificate used as 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 Web Config, and then select the **Network Security** tab. Next, select **SSL/TLS** > **Certificate** or **IPsec/IP Filtering** > **Client Certificate** or **IEEE802.1X** > **Client Certificate**.

2. Click **Delete**.

3. Confirm that you want to delete the certificate in the message displayed.

Configure CA Certificate

When you set the CA Certificate, you can validate the path to the CA certificate of the server that the printer accesses. This can prevent impersonation.

You can obtain the CA Certificate from the Certification Authority where the CA-signed Certificate is issued.

Related Information

➡ "Accessing Web Config" on page 27

➡ "CSR Setting Items" on page 84

➡ "Importing a CA-signed Certificate" on page 85

Importing a CA Certificate

Import the CA Certificate to the printer.

1. Access Web Config and then select the **Network Security** tab > **CA Certificate**.

2. Click **Import**.

3. Specify the CA Certificate you want to import.
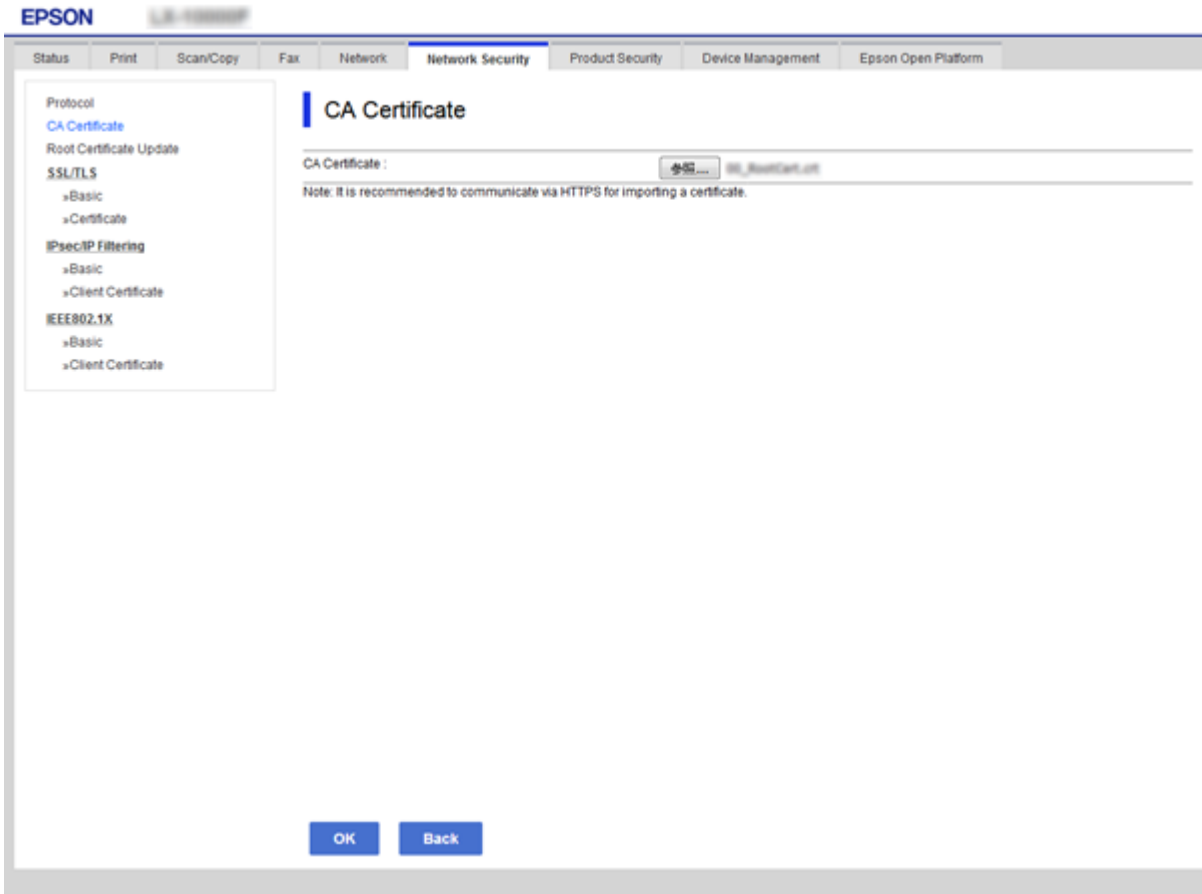
4. Click **OK**.

When importing is complete, you are returned to the **CA Certificate** screen, and the imported CA Certificate is displayed.

Deleting a CA Certificate

You can delete the imported CA Certificate.

1. Access Web Config and then select the **Network Security** tab > **CA Certificate**.

Advanced Security Settings for Enterprise

2. Click **Delete** next to the CA Certificate that you want to delete.
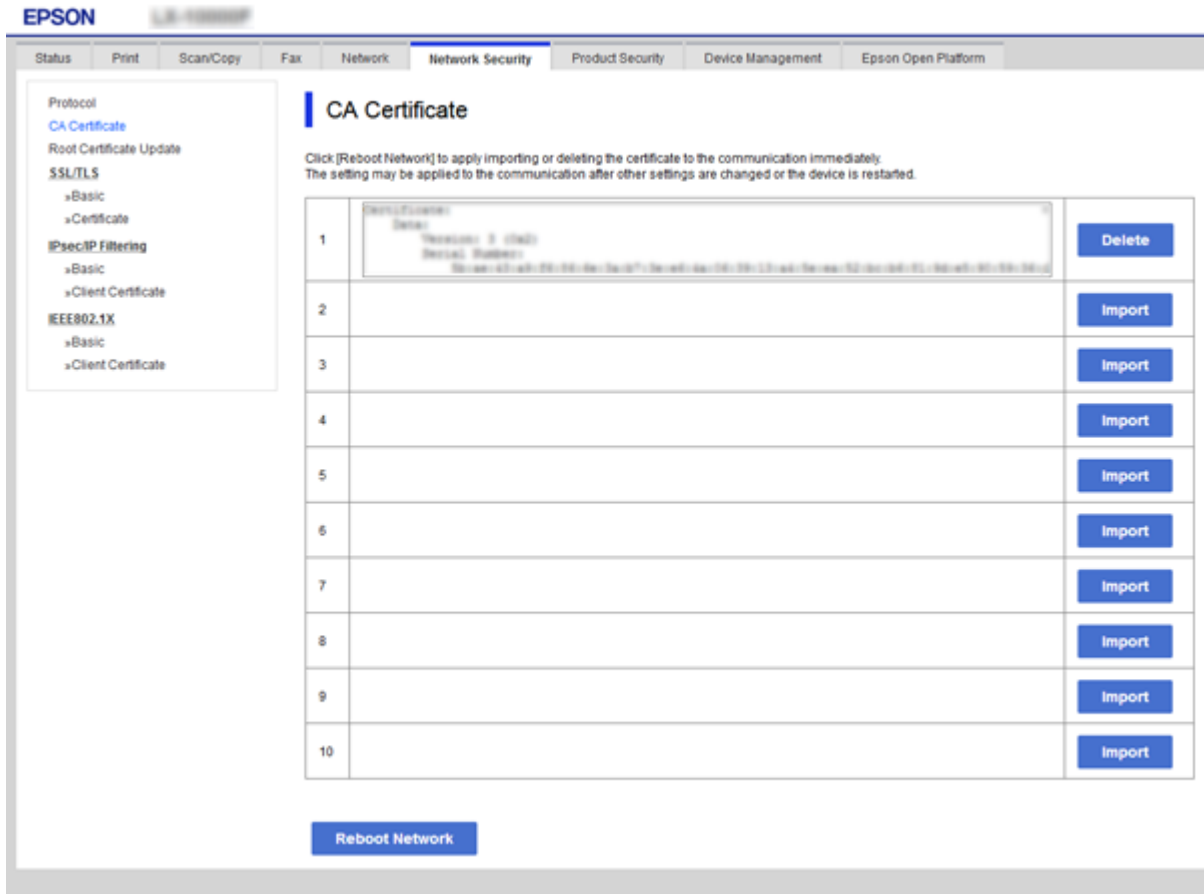
3. Confirm that you want to delete the certificate in the message displayed.

4. Click **Reboot Network**, and then check that the deleted CA Certificate is not listed on the updated screen.

Related Information

➡ "Accessing Web Config" on page 27

Updating a Self-signed Certificate

Because the Self-signed Certificate is issued by the printer, you can update it when it has expired or when the content described changes.

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

2. Click **Update**.

3. Enter **Common Name**.

    You can enter up to 5 IPv4 addresses, IPv6 addresses, host names, FQDNs between 1 to 128 characters and separating them with commas. The first parameter is stored to the common name, and the others are stored to the alias field for the subject of the certificate.

    Example:

Advanced Security Settings for Enterprise

Printer's IP address : 192.0.2.123, Printer name : EPSONA1B2C3

Common name : EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

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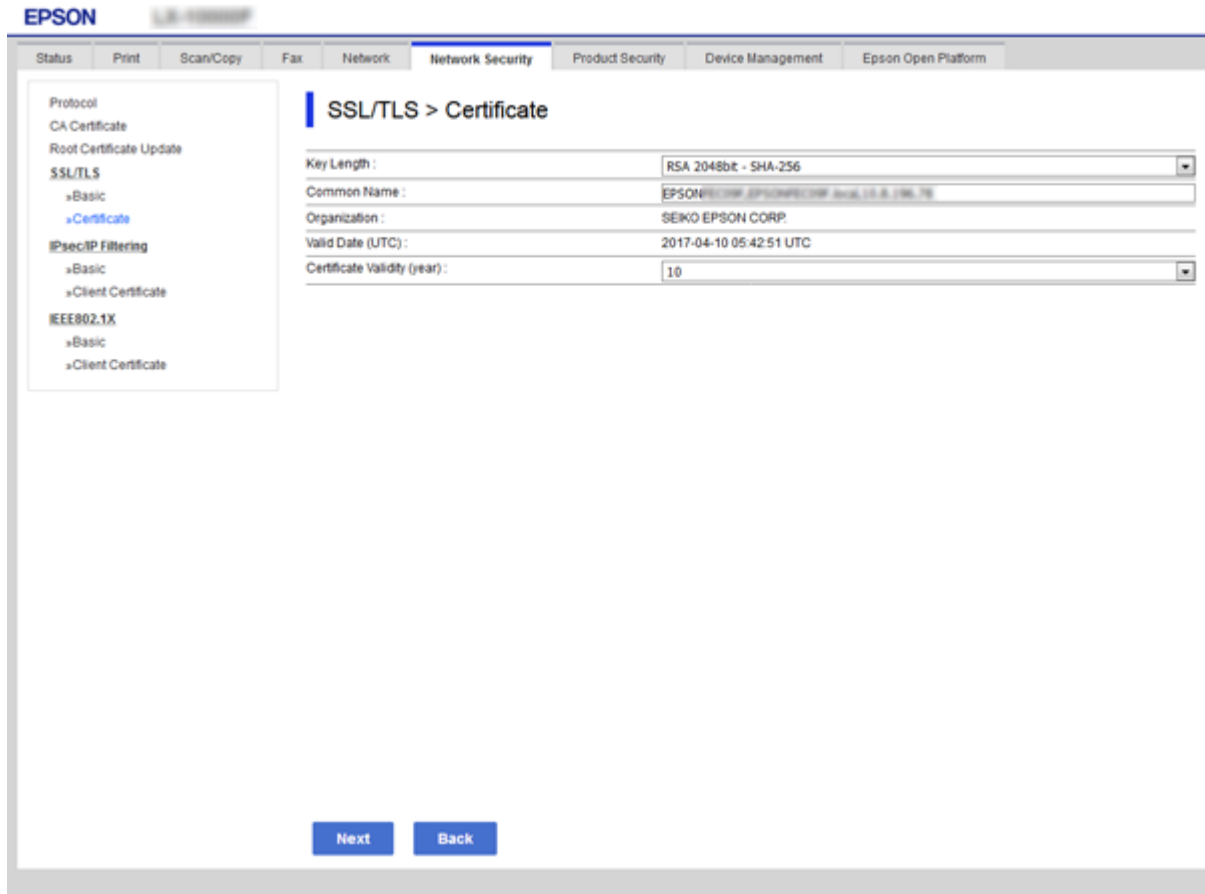
5. Click **Next**.

A confirmation message is displayed.

6. Click **OK**.

The printer is updated.

Note:
You can check the certificate information from **Network Security Settings** *tab >* **SSL/TLS** *>* **Certificate** *>* **Self-signed** **Certificate** *and click* **Confirm**.

Related Information

➡ "Accessing Web Config" on page 27

Controlling Using Protocols

You can print using a variety of pathways and protocols.

Advanced Security Settings for Enterprise

You can lower unintended security risks by restricting printing from specific pathways or by controlling the available functions.

Controlling protocols

Configure the protocol settings.

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

2. Configure each item.

3. Click **Next**.

4. Click **OK**.

   The settings are applied to the printer.

Protocols you can Enable or Disable

Protocol	Description
Bonjour Settings	You can specify whether to use Bonjour. Bonjour is used to search for devices, print, and so on.
SLP Settings	You can enable or disable the SLP function. SLP is used for network searching.
WSD Settings	You can enable or disable the WSD function. When this is enabled, you can add WSD devices, and print from the WSD port.
LLTD Settings	You can enable or disable the LLTD function. When this is enabled, it is displayed on the Windows network map.
LLMNR Settings	You can enable or disable the LLMNR function. When this is enabled, you can use name resolution without NetBIOS even if you cannot use DNS.
LPR Settings	You can specify whether or not to allow LPR printing. When this is enabled, you can print from the LPR port.
RAW(Port9100) Settings	You can specify whether or not to allow printing from the RAW port (Port 9100). When this is enabled, you can print from the RAW port (Port 9100).
IPP Settings	You can specify whether or not to allow printing from IPP. When this is enabled, you can print over the Internet.
FTP Settings	You can specify whether or not to allow FTP printing. When this is enabled, you can print over an FTP server.
SNMPv1/v2c Settings	You can specify whether or not to enable SNMPv1/v2c. This is used to set up devices, monitoring, and so on.
SNMPv3 Settings	You can specify whether or not to enable SNMPv3. This is used to set up encrypted devices, monitoring, etc.

Advanced Security Settings for Enterprise

Protocol Setting Items
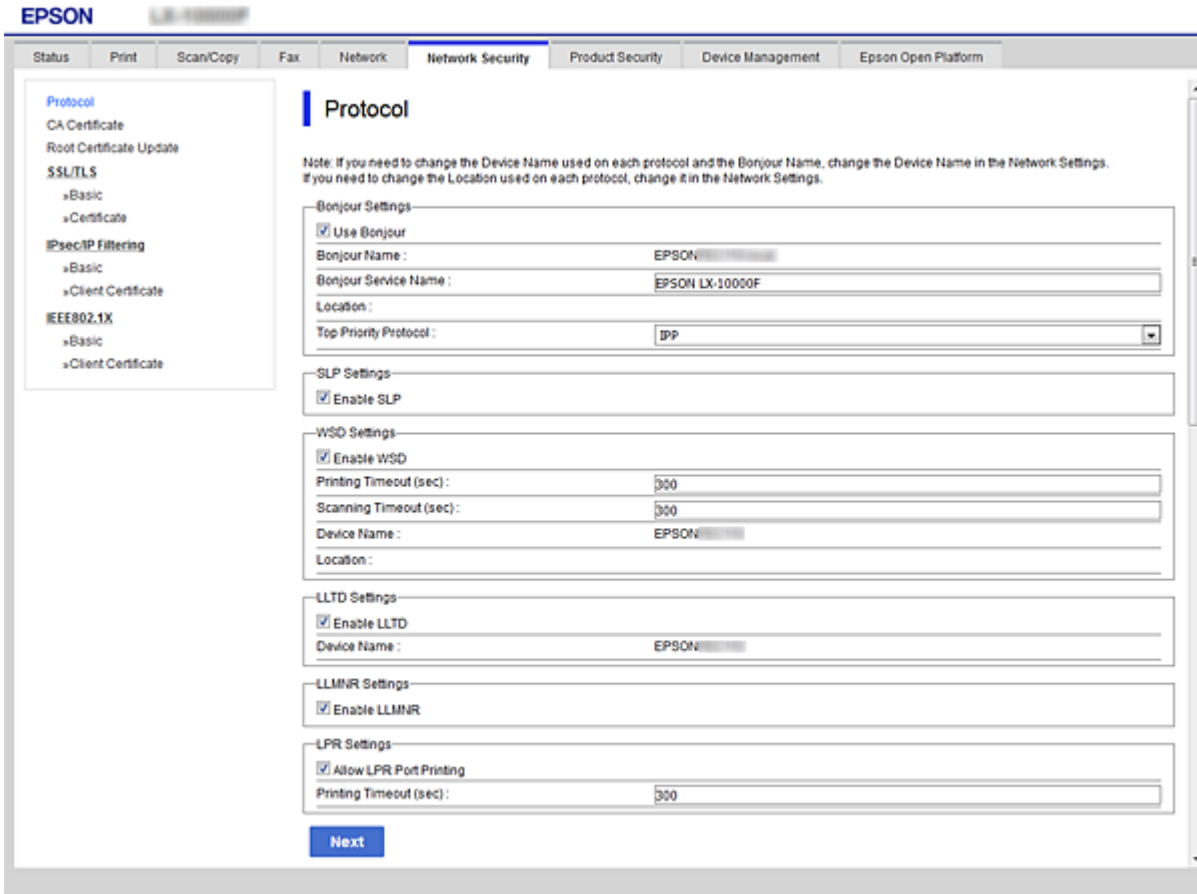
Bonjour Settings

Items	Setting value and Description
Use Bonjour	Select this to 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	Select the top priority protocol for Bonjour print.
Wide-Area Bonjour	Set whether to use Wide-Area Bonjour.

SLP Settings

Items	Setting value and Description
Enable SLP	Select this to enable the SLP function. This is used such as network searching in EpsonNet Config.

WSD Settings

Advanced Security Settings for Enterprise

Items	Setting value and Description
Enable WSD	Select this to enable adding devices using WSD, and print and scan from the WSD port.
Printing Timeout (sec)	Enter the communication timeout value for WSD printing between 3 to 3,600 seconds.
Device Name	Displays the WSD device name.
Location	Displays the WSD location name.

LLTD Settings

Items	Setting value and Description
Enable LLTD	Select this to enable LLTD. The printer is displayed in the Windows network map.
Device Name	Displays the LLTD device name.

LLMNR Settings

Items	Setting value and Description
Enable LLMNR	Select this to enable LLMNR. You can use name resolution without NetBIOS even if you cannot use DNS.

LPR Settings

Items	Setting value and Description
Allow LPR Port Printing	Select to allow printing from the LPR port.
Printing Timeout (sec)	Enter the timeout value for LPR printing between 0 to 3,600 seconds. If you do not want to timeout, enter 0.

RAW(Port9100) Settings

Items	Setting value and Description
Allow RAW(Port9100) Printing	Select to allow printing from the RAW port (Port 9100).
Printing Timeout (sec)	Enter the timeout value for RAW (Port 9100) printing between 0 to 3,600 seconds. If you do not want to timeout, enter 0.

IPP Settings

Items	Setting value and Description
Enable IPP	Select to enable IPP communication. Only printers that support IPP are displayed.
Allow Non-secure Communication	Select to allow the printer to communicate without any security measures (IPP).

Advanced Security Settings for Enterprise

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

FTP Settings

Items	Setting value and Description
Enable FTP Server	Select to enable FTP printing. Only printers that support FTP printing are displayed.
Communication Timeout (sec)	Enter the timeout value for FTP communication between 0 to 3,600 seconds. If you do not want to timeout, enter 0.

SNMPv1/v2c Settings

Items	Setting value and Description
Enable SNMPv1/v2c	Select to enable SNMPv1/v2c. Only printers that support SNMPv3 are displayed.
Access Authority	Set the access authority when SNMPv1/v2c is enabled. Select **Read Only** or **Read/Write**.
Community Name (Read Only)	Enter 0 to 32 ASCII (0x20 to 0x7E) characters.
Community Name (Read/Write)	Enter 0 to 32 ASCII (0x20 to 0x7E) characters.

SNMPv3 Settings

Items		Setting value and Description
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 for SNMPv3.
	Password	Enter the password for an authentication for SNMPv3. Enter between 8 and 32 characters in ASCII (0x20-0x7E). If you do not specify this, leave it blank.
	Confirm Password	Enter the password you configured for confirmation.

Advanced Security Settings for Enterprise

Items		Setting value and Description
Encryption Settings		
	Algorithm	Select an algorithm for an encryption for SNMPv3.
	Password	Enter the password for an encryption for SNMPv3. Enter between 8 and 32 characters in ASCII (0x20-0x7E). If you do not specify this, leave it blank.
	Confirm Password	Enter the password you configured for confirmation.
Context Name		Enter within 32 characters or less in Unicode (UTF-8). If you do not specify this, leave it blank. The number of characters that can be entered varies depending on the language.

Encrypted Communication Using IPsec/IP Filtering

About IPsec/IP Filtering

You can filter traffic based on IP addresses, services, and port by using IPsec/IP Filtering function. 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.

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

Configuring Default Policy

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.

1. Access Web Config and then select the **Network Security** tab > **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
➡ "Accessing Web Config" on page 27
➡ "Default Policy Setting Items" on page 96

Default Policy Setting Items
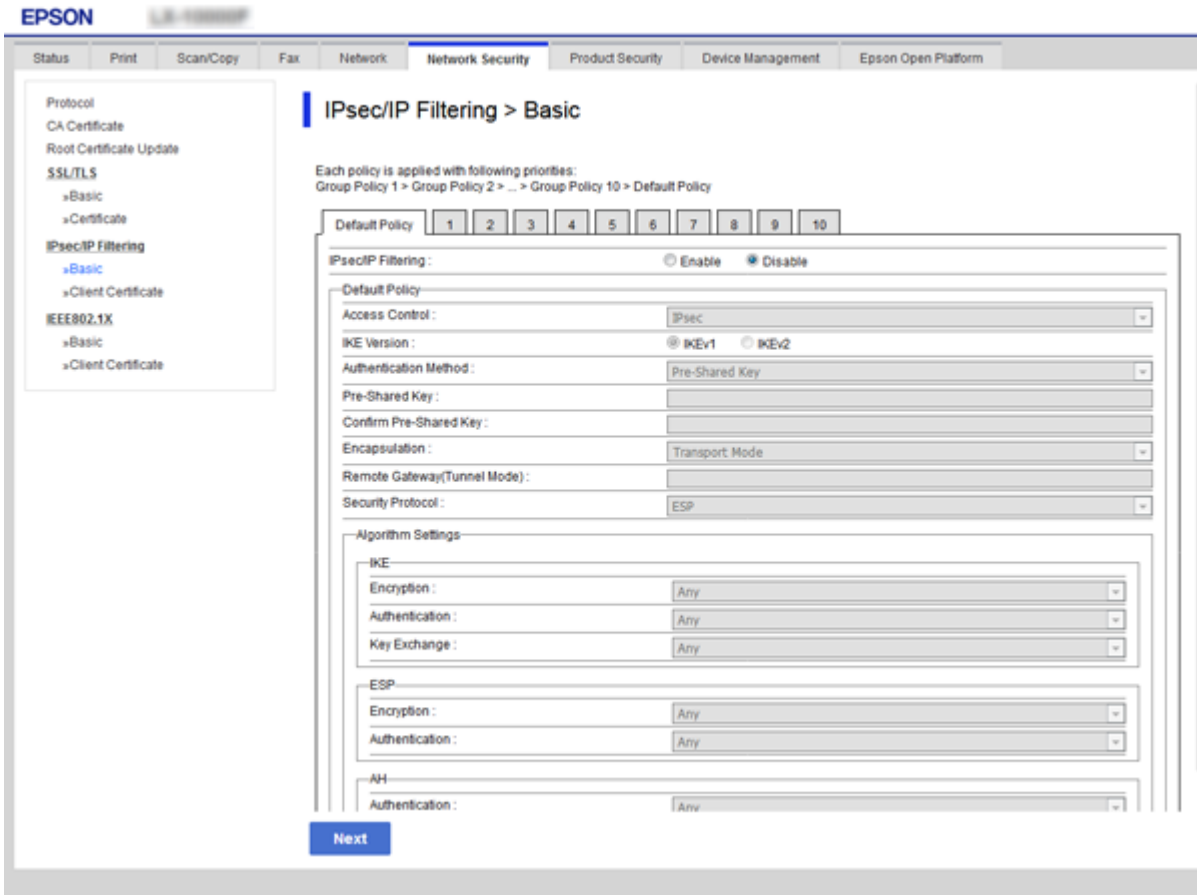
Items	Settings and Explanation
IPsec/IP Filtering	You can enable or disable an IPsec/IP Filtering feature.

Default Policy

Items	Settings and Explanation	
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.
IKE Version	Select IKEv1 or IKEv2 for IKE version.	
	Select one of them according to the device that the printer is connected to.	

Advanced Security Settings for Enterprise

Items	Settings and Explanation	
IKEv1	The following items are displayed when you select **IKEv1** for **IKE Version**.	
	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.
IKEv2	The following items are displayed when you select **IKEv2** for **IKE Version**.	

Advanced Security Settings for Enterprise

Items		Settings and Explanation	
Local	Authentication Method		To select **Certificate**, you need to obtain and import a CA-signed certificate in advance.
	ID Type		If you select **Pre-Shared Key** for **Authentication Method**, select the type of ID for the printer.
	ID		Enter the printer's ID that matches the type of ID.
			You cannot use "@", "#", and "=" for the first character.
			Distinguished Name : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. You need to include "=".
			IP Address : Enter IPv4 or IPv6 format.
			FQDN : Enter a combination of between 1 and 255 characters using A-Z, a-z, 0-9, "-", and period (.).
			Email Address : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. You need to include "@".
			Key ID : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters.
	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.
Remote	Authentication Method		To select **Certificate**, you need to obtain and import a CA-signed certificate in advance.
	ID Type		If you select **Pre-Shared Key** for **Authentication Method**, select the type of ID for the device that you want to authenticate.
	ID		Enter the printer's ID that matches to the type of ID.
			You cannot use "@", "#", and "=" for the first character.
			Distinguished Name : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. You need to include "=".
			IP Address : Enter IPv4 or IPv6 format.
			FQDN : Enter a combination of between 1 and 255 characters using A-Z, a-z, 0-9, "-", and period (.).
			Email Address : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. You need to include "@".
			Key ID : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters.
	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.

Advanced Security Settings for Enterprise

Items	Settings and Explanation		
Remote Gateway(Tunnel Mode)	If you select **Tunnel Mode** for **Encapsulation**, enter a gateway address between 1 and 39 characters.		
Security Protocol	**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.
Algorithm Settings*			
	IKE	Encryption	Select the encryption algorithm for IKE. The items vary depending on the version of IKE.
		Authentication	Select the authentication algorithm for IKE.
		Key Exchange	Select the key exchange algorithm for IKE. The items vary depending on the version of IKE.
	ESP	Encryption	Select the encryption algorithm for ESP. This is available when **ESP** is selected for **Security Protocol**.
		Authentication	Select the authentication algorithm for ESP. This is available when **ESP** is selected for **Security Protocol**.
	AH	Authentication	Select the encryption algorithm for AH. This is available when **AH** is selected for **Security Protocol**.

* For Algorithm Settings, it is recommended that you select **Any** for all settings or select an item other than **Any** for each setting. If you select **Any** for some of the settings and select an item other than **Any** for the other settings, the device may not communicate depending on the other device that you want to authenticate.

Related Information

➡

Configuring Group Policy

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.

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

Advanced Security Settings for Enterprise

5.   Click **OK**.

The printer is updated.

Related Information

➡

➡

Group Policy Setting Items
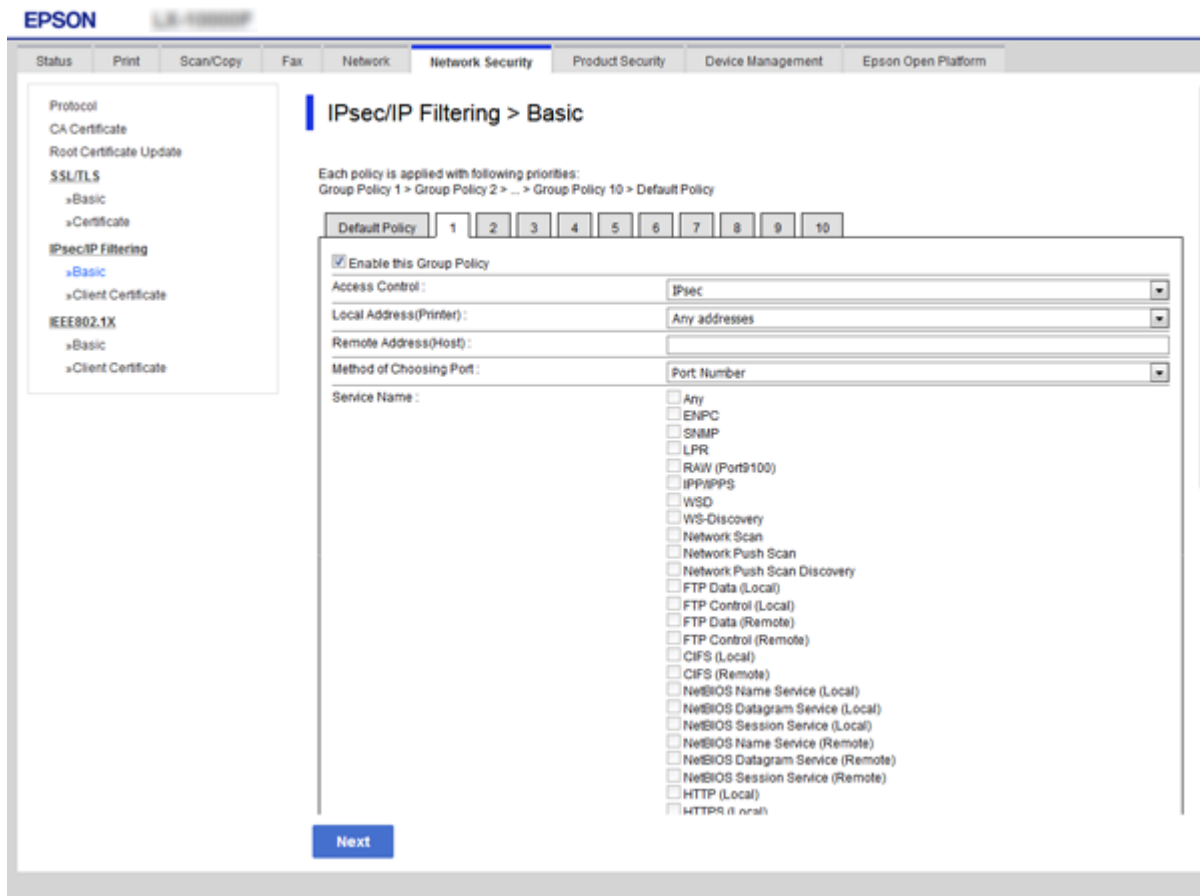
Items	Settings and Explanation	
Enable this Group Policy	You can enable or disable a group policy.	
Access Control	Configure a control method for traffic of IP packets.	
	Permit Access	Select this to permit configured IP packets to pass through.
	Refuse Access	Select this to refuse configured IP packets to pass through.
	IPsec	Select this to permit configured IPsec packets to pass through.

Advanced Security Settings for Enterprise

Items	Settings and Explanation	
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**. *Note:* *If an IPv6 address is assigned automatically, the connection may be unavailable. Configure a static IPv6 address.*	
Remote Address(Host)	Enter a device's IP address to control access. The IP address must be 43 characters or less. 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.
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.	
IKE Version	Select IKEv1 or IKEv2 for IKE version. Select one of them according to the device that the printer is connected to.	
IKEv1	The following items are displayed when you select **IKEv1** for **IKE Version**.	
	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.
IKEv2	The following items are displayed when you select **IKEv2** for **IKE Version**.	

Advanced Security Settings for Enterprise

Items		Settings and Explanation
Local	Authentication Method	If you select **IPsec** for **Access Control**, select an option. Used certificate is common with a default policy.
	ID Type	If you select **Pre-Shared Key** for **Authentication Method**, select the type of ID for the printer.
	ID	Enter the printer's ID that matches to the type of ID. You cannot use "@", "#", and "=" for the first character. **Distinguished Name** : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. You need to include "=". **IP Address** : Enter IPv4 or IPv6 format. **FQDN** : Enter a combination of between 1 and 255 characters using A-Z, a-z, 0-9, "-", and period (.). **Email Address** : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. You need to include "@". **Key ID** : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters.
	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.
Remote	Authentication Method	If you select **IPsec** for **Access Control**, select an option. Used certificate is common with a default policy.
	ID Type	If you select **Pre-Shared Key** for **Authentication Method**, select the type of ID for the device that you want to authenticate.
	ID	Enter the printer's ID that matches to the type of ID. You cannot use "@", "#", and "=" for the first character. **Distinguished Name** : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. You need to include "=". **IP Address** : Enter IPv4 or IPv6 format. **FQDN** : Enter a combination of between 1 and 255 characters using A-Z, a-z, 0-9, "-", and period (.). **Email Address** : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. You need to include "@". **Key ID** : Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters.
	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.

Advanced Security Settings for Enterprise

Items		Settings and Explanation
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.
Algorithm Settings*		
IKE	Encryption	Select the encryption algorithm for IKE. The items vary depending on the version of IKE.
	Authentication	Select the authentication algorithm for IKE.
	Key Exchange	Select the key exchange algorithm for IKE. The items vary depending on the version of IKE.
ESP	Encryption	Select the encryption algorithm for ESP. This is available when **ESP** is selected for **Security Protocol**.
	Authentication	Select the authentication algorithm for ESP. This is available when **ESP** is selected for **Security Protocol**.
AH	Authentication	Select the authentication algorithm for AH. This is available when **AH** is selected for **Security Protocol**.

* For Algorithm Settings, it is recommended that you select **Any** for all settings or select an item other than **Any** for each setting. If you select **Any** for some of the settings and select an item other than **Any** for the other settings, the device may not communicate depending on the other device that you want to authenticate.

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

Advanced Security Settings for Enterprise

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

Note:
Unavailable services are displayed but cannot be selected.

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 Epson Device Admin, and the printer driver
SNMP	UDP	161	Any port	Acquiring and configuring of MIB from applications such as Epson Device Admin, and the printer driver
LPR	TCP	515	Any port	Forwarding LPR data
RAW (Port9100)	TCP	9100	Any port	Forwarding RAW data
WSD	TCP	Any port	5357	Controlling WSD
WS-Discovery	UDP	3702	Any port	Searching for a printer from WSD
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)
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 (firmware updating and root certificate updating)
HTTPS (Remote)	TCP	Any port	443	

Configuration Examples of IPsec/IP Filtering

Receiving IPsec packets only

This example is to configure a default policy only.

Advanced Security Settings for Enterprise

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

Configure the Client Certificate for IPsec/IP Filtering. When you set it, you can use the certificate as an authentication method for IPsec/IP Filtering. If you want to configure the certification authority, go to **CA Certificate**.

1. Access Web Config and then select the **Network Security** tab > **IPsec/IP Filtering** > **Client Certificate**.

Advanced Security Settings for Enterprise

2. Import the certificate in **Client Certificate**.

   If you have already imported a certificate published by a Certification Authority in IEEE802.1X or SSL/TLS, you can copy the certificate and use it in IPsec/IP Filtering. To copy, select the certificate from **Copy From**, and then click **Copy**.
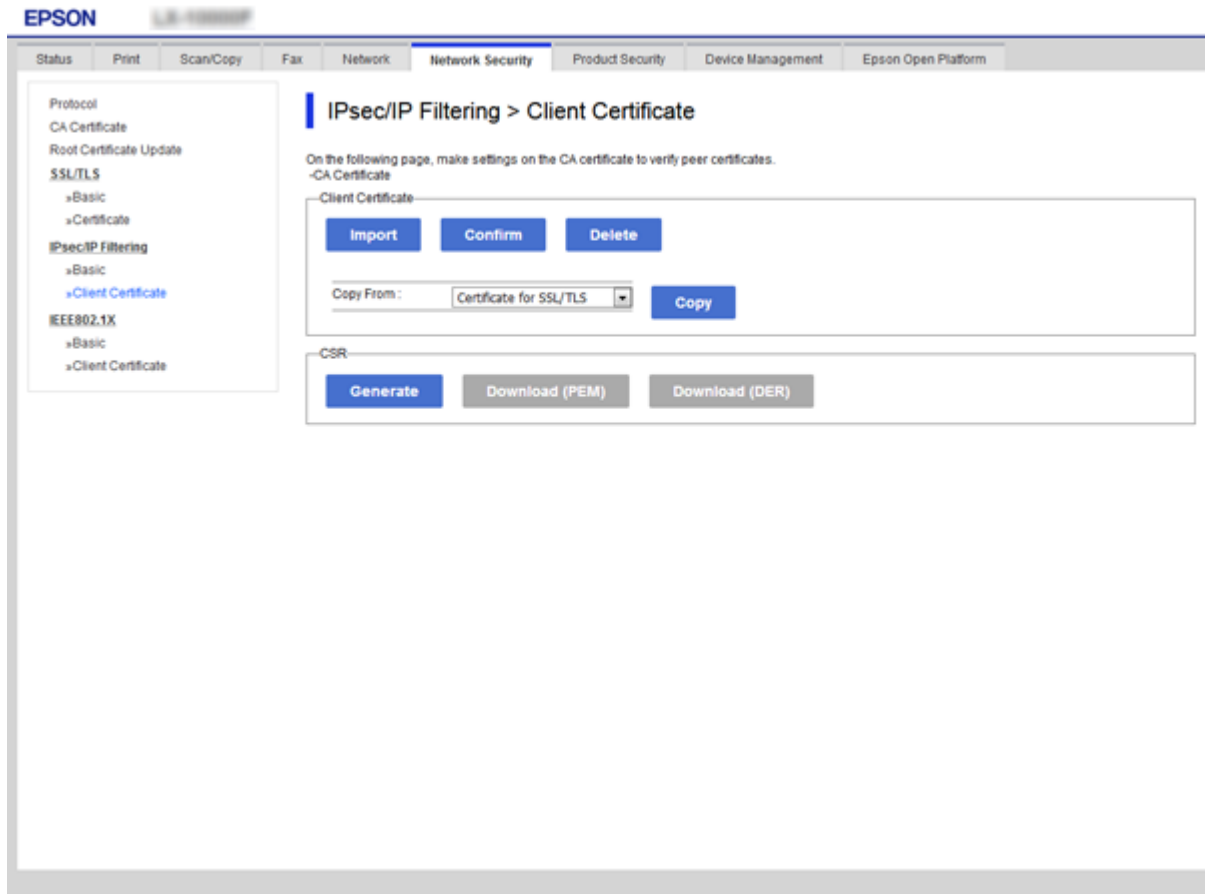
Related Information

➡
➡

Connecting the Printer to an IEEE802.1X Network

Configuring an IEEE802.1X Network

When you set IEEE802.1X to the printer, you can use it on the network connected to a RADIUS server, a LAN switch with authentication function, or an access point.

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

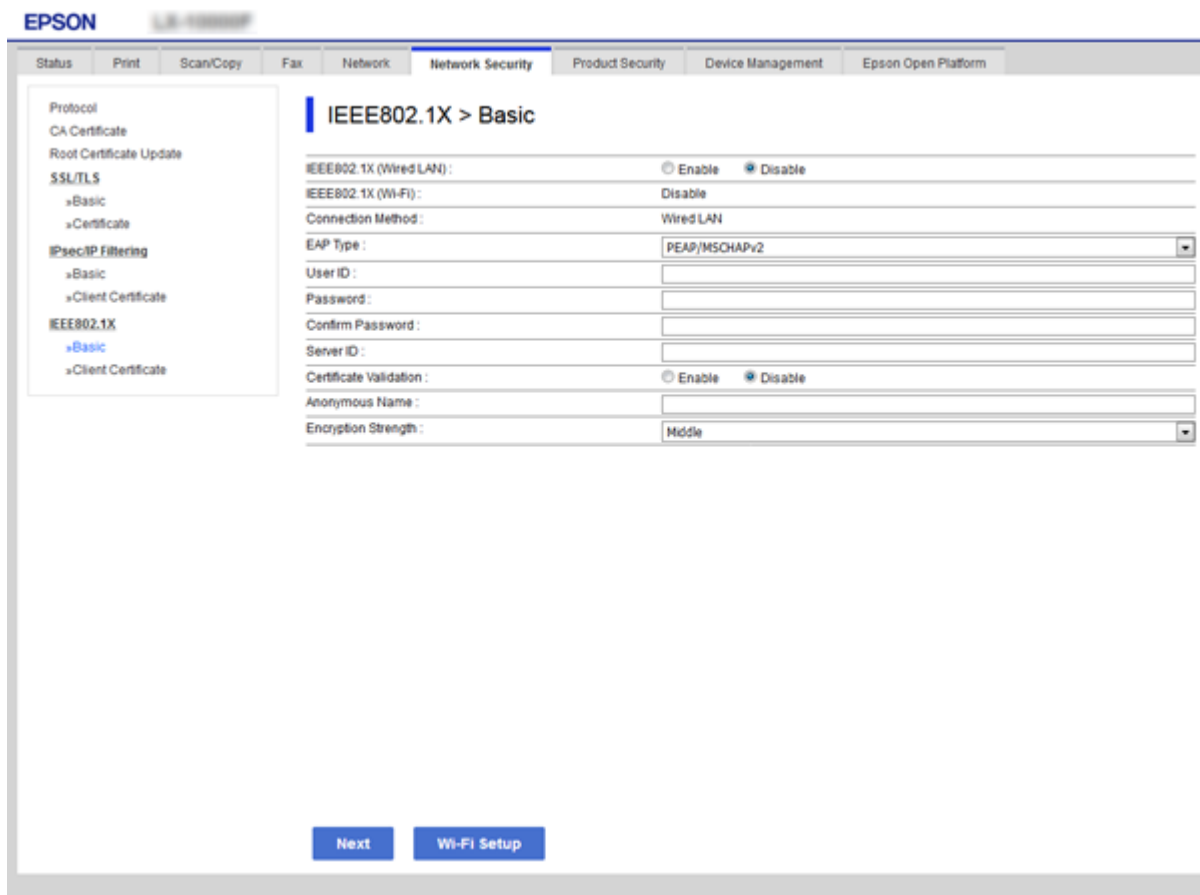**Advanced Security Settings for Enterprise**

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.

Advanced Security Settings for Enterprise

Items	Settings and Explanation	
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. Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters.	
Password	Configure a password to authenticate the printer. Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. If you are using a Windows server as a RADIUS server, you can enter up to 127 characters.	
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. Enter 0 to 128 1-byte ASCII (0x20 to 0x7E) characters.	
Certificate Validation	You can set certificate validation regardless of the authentication method. Import the certificate in **CA Certificate**.	
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. Enter 0 to 128 1-byte ASCII (0x20 to 0x7E) characters.	
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

Configure the Client Certificate for IEEE802.1X. When you set it, you can use **EAP-TLS** and **PEAP-TLS** as an authentication method of IEEE802.1x. If you want to configure the certification authority certificate, go to **CA Certificate**.

1. Access Web Config and then select the **Network Security** tab > **IEEE802.1X** > **Client Certificate**.

Advanced Security Settings for Enterprise

2.   Enter a certificate in the **Client Certificate**.

You can copy the certificate if it is published by a Certification Authority. To copy, select the certificate from **Copy From**, and then click **Copy**.
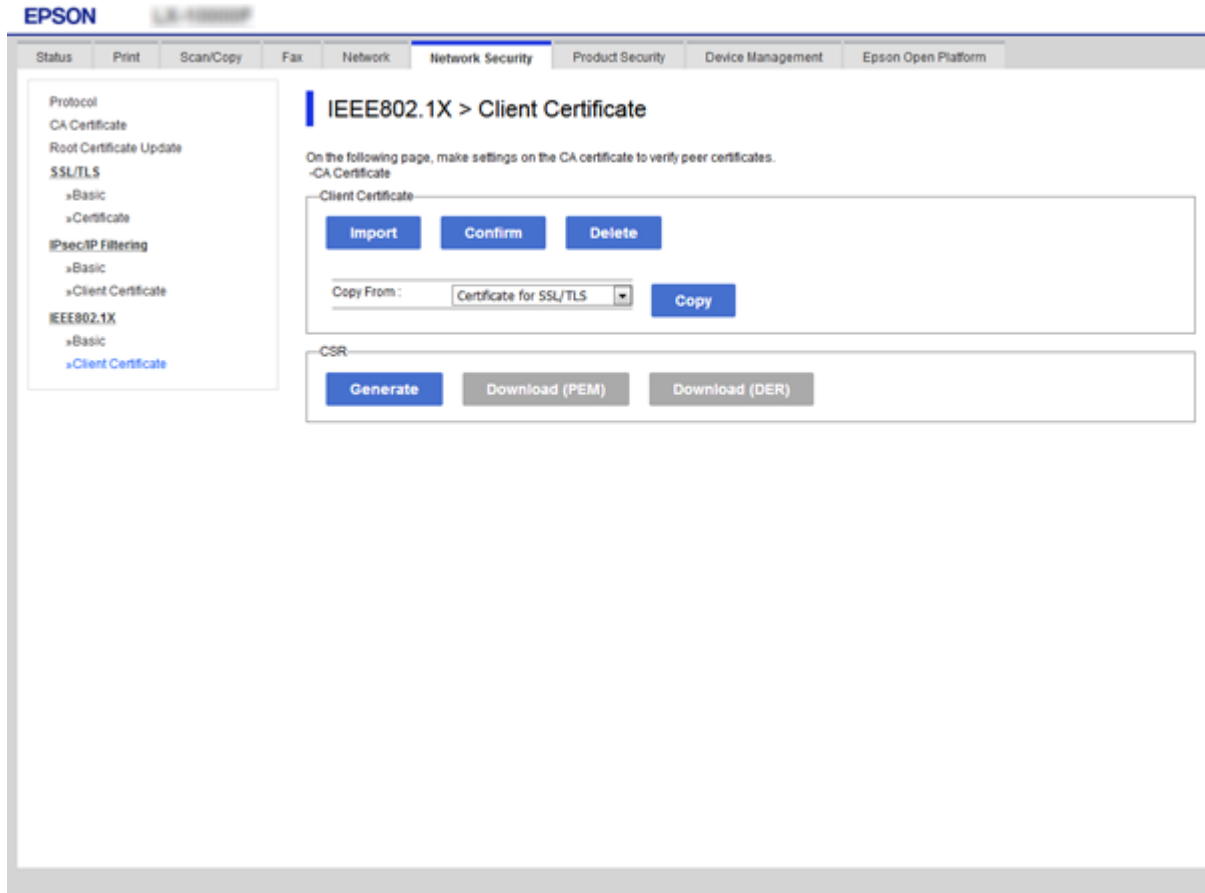
Related Information

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.

Advanced Security Settings for Enterprise

Status ID	IEEE802.1X Status
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 **EAP Type** is **EAP-TLS** or **PEAP-TLS**, client certificate is incorrect or has certain problems. ❑ If **EAP Type** is **PEAP/MSCHAPv2**, user ID or password is not correct.

Solving Problems for Advanced Security

Restoring the Security Settings

When you establish a highly secure environment such as IPsec/IP Filtering or IEEE802.1X, you may not be able to communicate with devices because of incorrect settings or trouble with the device or server. In this case, restore the security settings in order to make settings for the device again or to allow you temporary use.

Disabling the Security Function Using the Control Panel

You can disable IPsec/IP Filtering or IEEE802.1X using the printer's control panel.

1. Select **Settings** > **General Settings** > **Network Settings**.

2. Select **Advanced**.

3. Select from the following items that you want to disable.

   ❑ **Disable IPsec/IP Filtering**

   ❑ **Disable IEEE802.1X**

4. Select **Proceed** on the confirmation screen.

5. When a completion message is displayed, select **Close**.

   The screen automatically closes after a specific length of time if you do not select **Close**.

Problems Using Network Security Features

Forgot a Pre–shared Key

Re-configure a pre-shared key.

To change the key, access Web Config and select the **Network Security** tab > **IPsec/IP Filtering** > **Basic** > **Default Policy** or **Group Policy**.

When you change the pre-shared key, configure the pre-shared key for computers.

Related Information

➡ "Accessing Web Config" on page 27

Cannot Communicate with IPsec Communication

Specify the algorithm that the printer or the computer does not support.

The printer supports the following algorithms. Check the settings of the computer.

Security Methods	Algorithms
IKE encryption algorithm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE authentication algorithm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE key exchange algorithm	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
ESP encryption algorithm	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP authentication algorithm	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH authentication algorithm	SHA-1, SHA-256, SHA-384, SHA-512, MD5

*available for IKEv2 only

Related Information

➡ "Encrypted Communication Using IPsec/IP Filtering" on page 95

Cannot Communicate Suddenly

The IP address of the printer has been changed or cannot be used.

When the IP address registered to the local address on Group Policy has been changed or cannot be used, IPsec communication cannot be performed. 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** tab > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address(Printer)**) may not be found.

Use a static IP address.

The IP address of the computer has been changed or cannot be used.

When the IP address registered to the remote address on Group Policy has been changed or cannot be used, IPsec communication cannot be performed.

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** tab > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) may not be found.

Use a static IP address.

Related Information

➡
➡

Cannot Create the Secure IPP Printing Port

The correct certificate is not 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.

The CA certificate is not 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 Connect After Configuring IPsec/IP Filtering

The settings of IPsec/IP Filtering are incorrect.

Disable IPsec/IP filtering from the printer's control panel. Connect the printer and computer and make the IPsec/IP Filtering settings again.

Related Information

➡

Advanced Security Settings for Enterprise

Cannot Access the Printer or Scanner after Configuring IEEE802.1X

The settings of IEEE802.1X are 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

➡ "Configuring an IEEE802.1X Network" on page 106

Problems on Using a Digital Certificate

Cannot Import a CA-signed Certificate

CA-signed Certificate and the information on the CSR do not 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.

CA-signed Certificate is more than 5KB.

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

The password for importing the certificate is incorrect.

Enter the correct password. If you forget the password, you cannot import the certificate. Re-obtain the CA-signed Certificate.

Related Information

➡ "Importing a CA-signed Certificate" on page 85

Cannot Update a Self-Signed Certificate

The Common Name has not been entered.

Common Name must be entered.

Unsupported characters have been entered to Common Name.

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

A comma or space is 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

➡

Cannot Create a CSR

The Common Name has not been entered.

The **Common Name** must be entered.

Unsupported characters have been entered to Common Name, Organization, Organizational Unit, Locality, and State/Province.

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

A comma or space is 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

➡

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**.
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.

Advanced Security Settings for Enterprise

Messages	Cause/What to do
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.
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.

Advanced Security Settings for Enterprise

Messages	Cause/What to do
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

➡

Delete a CA-signed Certificate by Mistake

There is no backup file for the CA-signed 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

➡
➡