EPSON
EXCEED YOUR VISION

Administrator's Guide

Contents

Contents

Copyright

Trademarks

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

❏ Epson Scan 2 software is based in part on the work of the Independent JPEG Group.

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

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

About this Manual

Marks and Symbols

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

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

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

Related Information

➡ Clicking this icon takes you to related information.

Descriptions Used in this Manual

❏ Screenshots of the scanner driver and the Epson Scan 2(scanner driver) screens are from Windows 10 or OS X El Capitan. The content displayed on the screens varies depending on the model and situation.

❏ Illustrations used in this manual are examples only. Although there may be slight differences depending on the model, the method of operation is the same.

❏ Some of the menu items on the LCD screen vary depending on the model and settings.

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

About this Manual

❏ Microsoft® Windows Server® 2016 operating system

❏ 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

Manual Component

This manual is for the device administrator who is in charge of connecting the printer or scanner to the network and it contains information on how to make settings to use the functions.

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

Preparation

Explains the administrator's tasks, how to set devices, and the software for managing.

Connection

Explains how to connect a device to the network. It also explains the network environment, such as using a port for the device, DNS and proxy server information.

Function Settings

Explains the settings for each function of the device.

Basic Security Settings

Explains the basic security settings, such as administrator password settings and protocol control.

Operation and Management Settings

Explains the operations after beginning use of devices, such as information check and maintenance.

Solving Problems

Explains settings initialization and troubleshooting of the network.

Advanced Security Settings for Enterprise

Explains the settings method to enhance the device's security, such as using CA certificate, SSL/TLS communication, and IPsec/IP Filtering.

Depending on the model, some functions in this chapter are not supported.

Definitions of Terms Used in this Guide

The following terms are used in this guide.

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.

Introduction

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.

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.

Tool

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

Push scan

A generic term for scanning from the device's control panel.

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.

SP*	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
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.

Preparation

This chapter explains the role of the administrator and preparation before making settings.

Flow of the Scanner Settings and Management

The administrator makes the network connection settings, initial setup and maintenance for the scanner so they can be available to users.

1. Preparing
   ❏ Collecting the connection setting information
   ❏ Decision on the connection method

2. Connecting
   ❏ Network connection from the scanner's control panel

3. Setting up the functions
   ❏ Scanner driver settings
   ❏ Other advanced settings

4. Security settings
   ❏ Administrator settings
   ❏ SSL/TLS
   ❏ Protocol control
   ❏ Advanced security settings (Option)

5. Operating and managing
   ❏ Checking the device status
   ❏ Handling for events emergence
   ❏ Backup the device settings

Related Information

Example of Network Environment
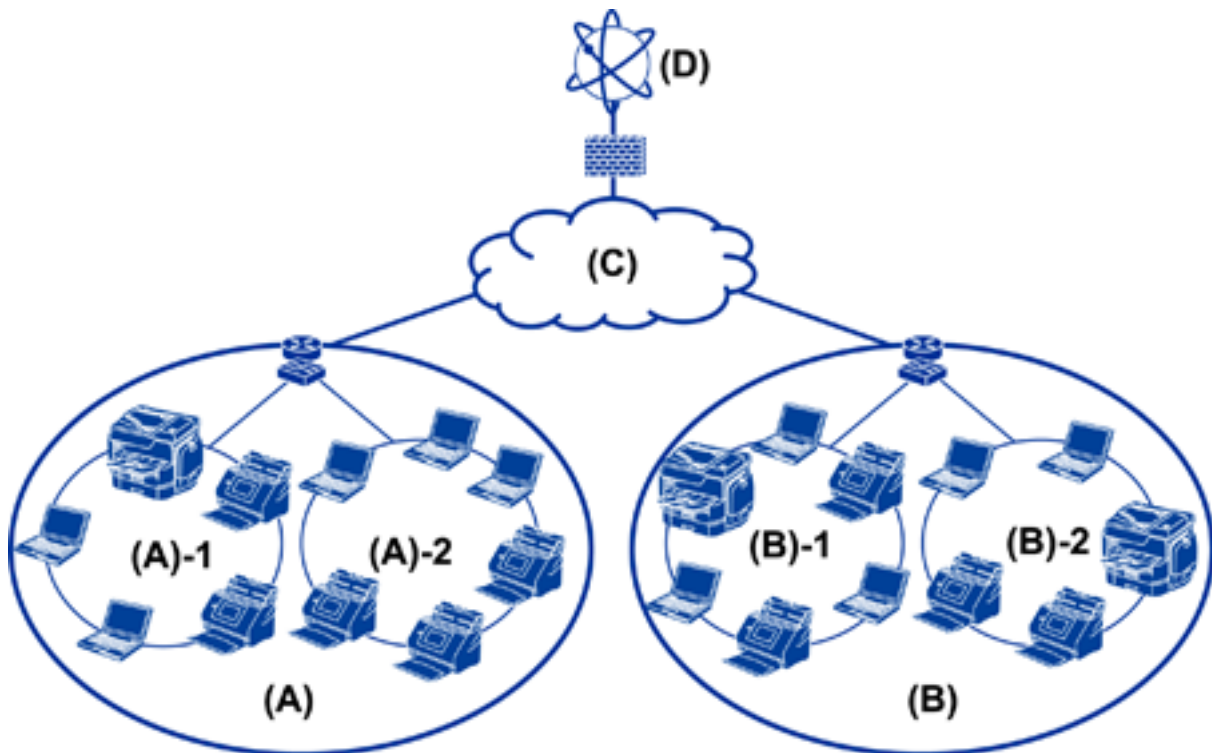
(A) : Office 1

❏ (A) - 1 : LAN 1

❏ (A) - 2 : LAN 2

(B) : Office 2

❏ (B) - 1 : LAN 1

❏ (B) - 2 : LAN 2

(C) : WAN

(D) : Internet

Introduction of scanner connection setting example

There are mainly two connection types depending on how to use the scanner. Both connect the scanner to the network with the computer via the hub.

❏ Server / client connection (scanner using Windows server, job management)

❏ Peer to peer connection (direct connection by client computer)

Related Information

➡ "Server / Client Connection" on page 12
➡ "Peer to Peer Connection" on page 12

Server / Client Connection

Centralize scanner and job management with Document Capture Pro Server installed on the server. It is most suitable for work that uses multiple scanners to scan a large number of documents in a certain format.

Related Information

➡ "Definitions of Terms Used in this Guide" on page 8

Peer to Peer Connection

Use an individual scanner with a scanner driver such as Epson Scan 2 installed on the client computer. Installing Document Capture Pro (Document Capture) on the client computer allows you to run jobs on the scanner's individual client computers.

Related Information

➡ "Definitions of Terms Used in this Guide" on page 8

Preparing Connection to a Network

Gathering Information on the Connection Setting

You need to have an IP address, gateway address, etc. for network connection. Check the following in advance.

Divisions	Items	Note
Device connection method	❏ Ethernet	Use a category 5e or higher STP (Shielded Twisted Pair) cable for Ethernet connection.
LAN connection information	❏ IP address ❏ Subnet mask ❏ Default gateway	If you automatically set the IP address using the DHCP function of the router, it is not required.
DNS server information	❏ IP address for primary DNS ❏ IP address for secondary DNS	If you use a static IP address as the IP address, configure the DNS server. Configure when assigning automatically using the DHCP function and when the DNS server cannot be assigned automatically.
Proxy server information	❏ Proxy server name ❏ Port number	Configure when using a proxy server for Internet connection and when using the Epson Connect service or the firmware's automatic update function.

Scanner Specifications

The specification that the Scanner supports standard or connection mode, see the *User's Guide*.

Using Port Number

See "Appendix" for the port number that the scanner uses.

Related Information

➡

Type of IP Address Assignment

There are two types for assigning an IP address to the scanner.

Static IP address:

Assign the predetermined unique IP address to the scanner.

The IP address is not changed even when turning the scanner or router off, so you can manage the device by IP address.

This type is suitable for a network where many scanners are managed, such as a large office or school.

Automatic assignment by DHCP function:

The correct IP address is automatically assigned when the communication between the scanner and router that supports the DHCP function succeeds.

If it is inconvenient to change the IP address for a particular device, reserve the IP address in advance and then assign it.

DNS Server and Proxy Server

If you use an Internet connection service, configure the DNS server. If you do not configure it, you need to specify the IP address for accessing because you may fail the name resolution.

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

You can prohibit access to a specific URL by using the filtering function, as the proxy server is able to check the contents of the communication.

Method for Setting Network Connection

For connection settings for the scanner's IP address, subnet mask, and default gateway, proceed as follows.

Using the Control Panel:

Configure the settings using the scanner's control panel for each scanner. Connect to the network after configuring the scanner's connection settings.

Preparation

Using the Installer:

If the installer is used, the scanner's network and client computer are set automatically. The setting is available by following the installer's instructions, even if you do not have deep knowledge of the network.

Using a Tool:

Use a tool from the administrator's computer. You can discover a scanner and then set the scanner, or create an SYLK file to make batch settings to scanners. You can set many scanners, but they need to be connected physically by the Ethernet cable before setting. Therefore, this is recommended if you can build an Ethernet for the setting.

Related Information

Connection

This chapter explains the environment or procedure to connect the scanner to the network.

Connecting to the Network

Connecting to the Network from the Control Panel

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

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

Assigning the IP Address

Set up the basic items such asIP Address,Subnet Mask, and Default Gateway.

1. Turn on the scanner.

2. Flick the screen to the left on the scanner's control panel, and then tap **Settings**.
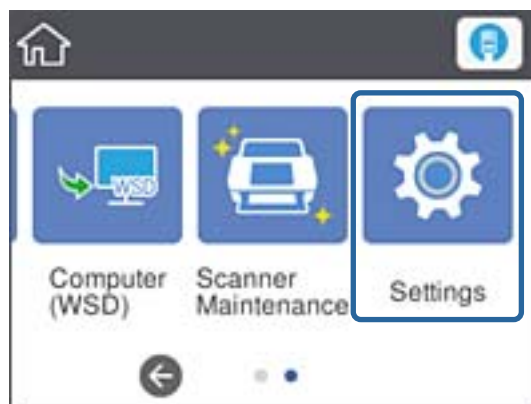
3. Tap **Network Settings** > **Change Settings**.

   If the item is not displayed, flick the screen upward to display it.

4. Tap **TCP/IP**.
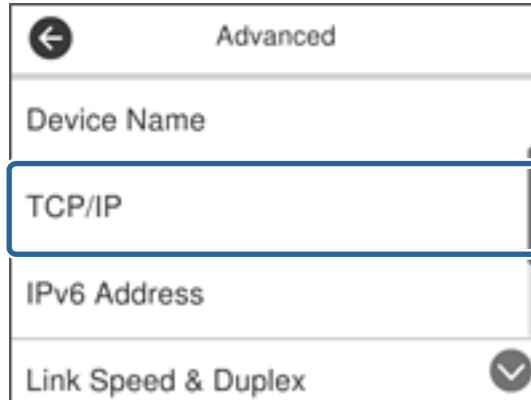
5. Select **Manual** for **Obtain IP Address**.
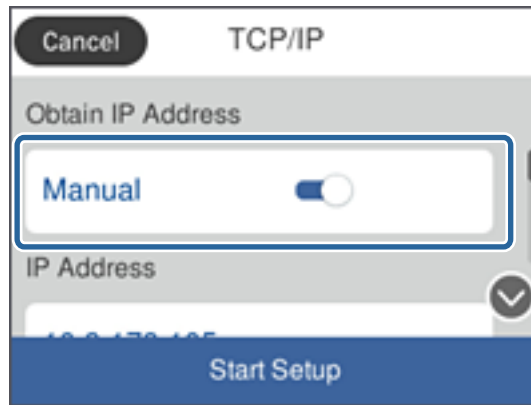
Note:
*When you set the IP address automatically by using the DHCP function of router, select **Auto**. In that case, the **IP Address**, **Subnet Mask**, and **Default Gateway** on step 6 to 7 are also set automatically, so go to step 8.*

6. Tap the **IP Address** field, enter the IP address using the keyboard displayed on the screen, and then tap **OK**.
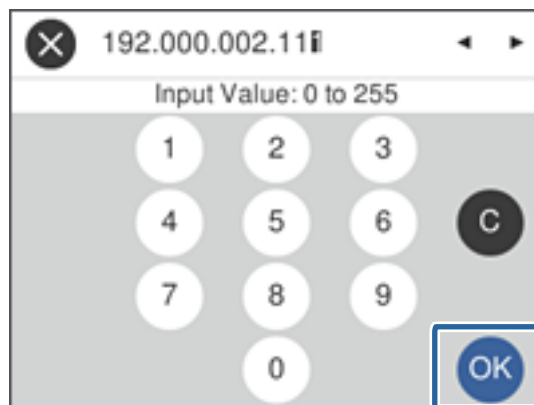
Confirm the value reflected on the previous screen.

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

Confirm the value reflected on the previous screen.

Connection

Note:
*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. Tap the **Primary DNS** field for the **DNS Server**, enter the IP address for the primary DNS server using the keyboard displayed on the screen, and then tap **OK**.

   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. Tap the **Secondary DNS** field, enter the IP address for the secondary DNS server using the keyboard displayed on the screen, and then tap **OK**.

   Confirm the value reflected on the previous screen.

10. Tap **Start Setup**.

11. Tap **Close** on the confirmation screen.

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

Connecting to Ethernet

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

1. Connect the scanner and hub (L2 switch) by Ethernet cable.

   The icon on the home screen changes to ⊕ .

2. Tap ⊕ on the home screen.
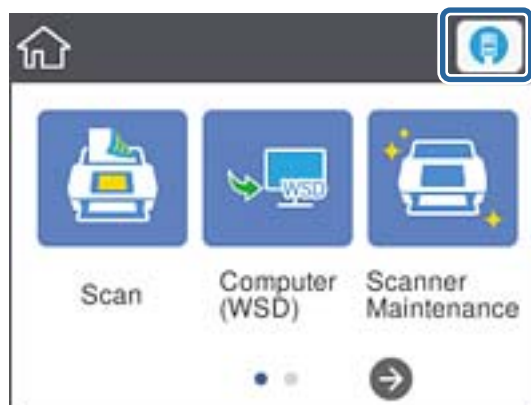
3. Flick the screen upward, and then make sure the connection status and IP address are correct.
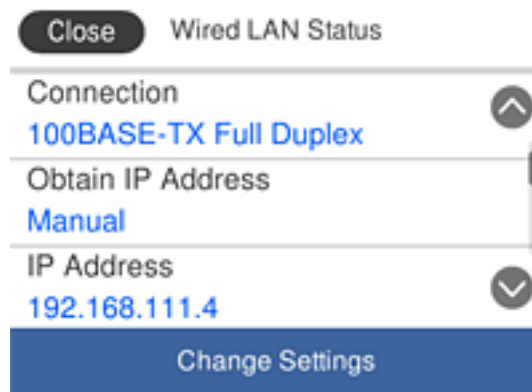
Setting the Proxy Server

The proxy server can not be set on the panel. Configure using Web Config.

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

2. Select **Use** in **Proxy Server Setting**.

3. Specify the proxy server in IPv4 address or FQDN format in **Proxy Server**, and then enter the port number in **Proxy Server Port Number**.

   For proxy servers that require authentication, enter the Proxy server authentication user name and Proxy server authentication password.

4.   Click the **Next** button.
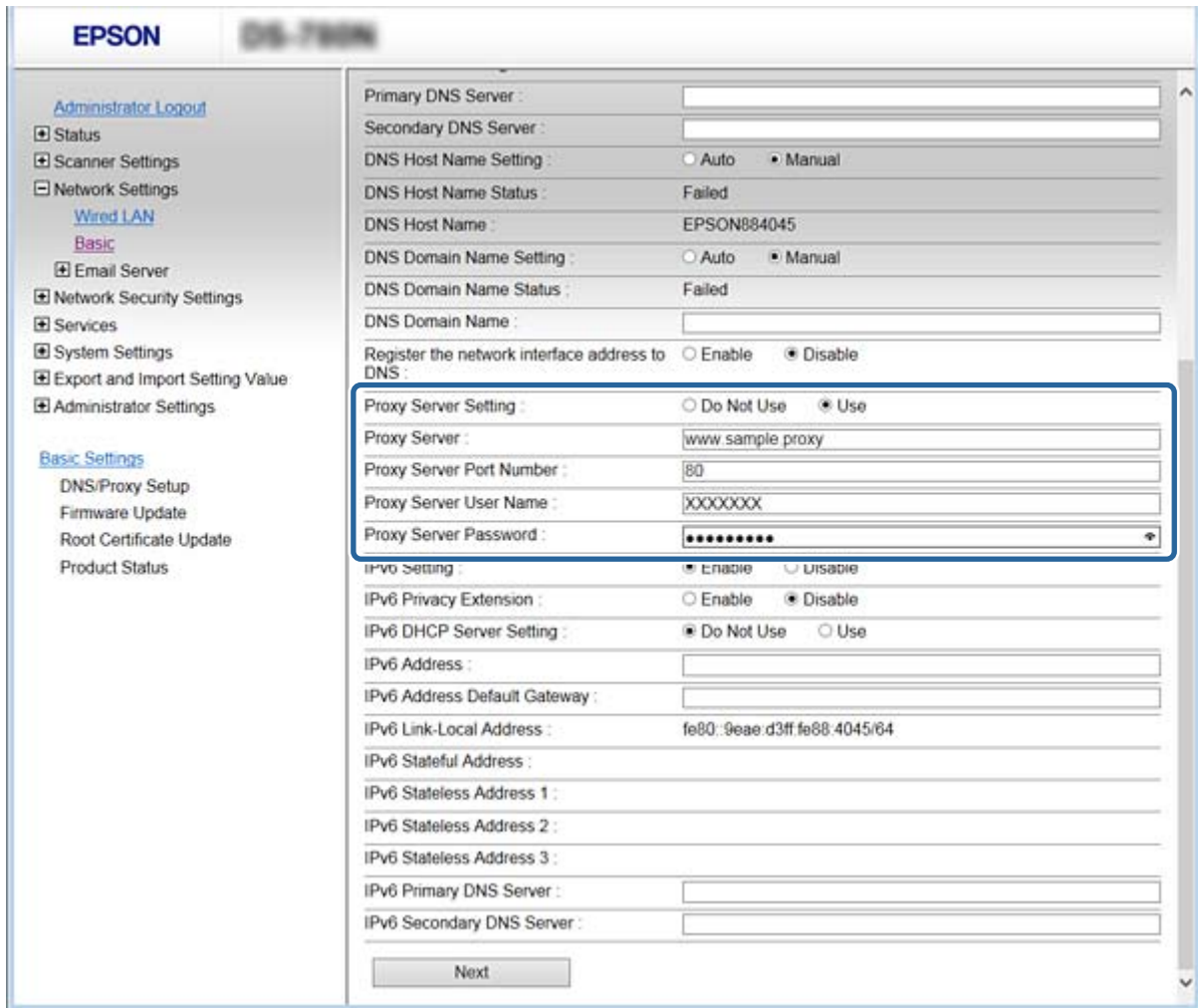
5.   Confirm the settings, and then click **Settings**.

Related Information

➡ "Accessing Web Config" on page 23

Connecting to the Network Using the Installer

We recommend using the installer to connect the scanner to a computer. You can run the installer using one of the following methods.

❏ Setting up from the website

Access the following website, and then enter the product name. Go to **Setup**, and then start setting up.

http://epson.sn

❏ Setting up using 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, and then follow the on-screen instructions.

Selecting the Connection Methods

Follow the on-screen instructions until the following screen is displayed and then select the connection method of the scanner to the computer.

❏ Windows

Select the connection type and then click **Next**.
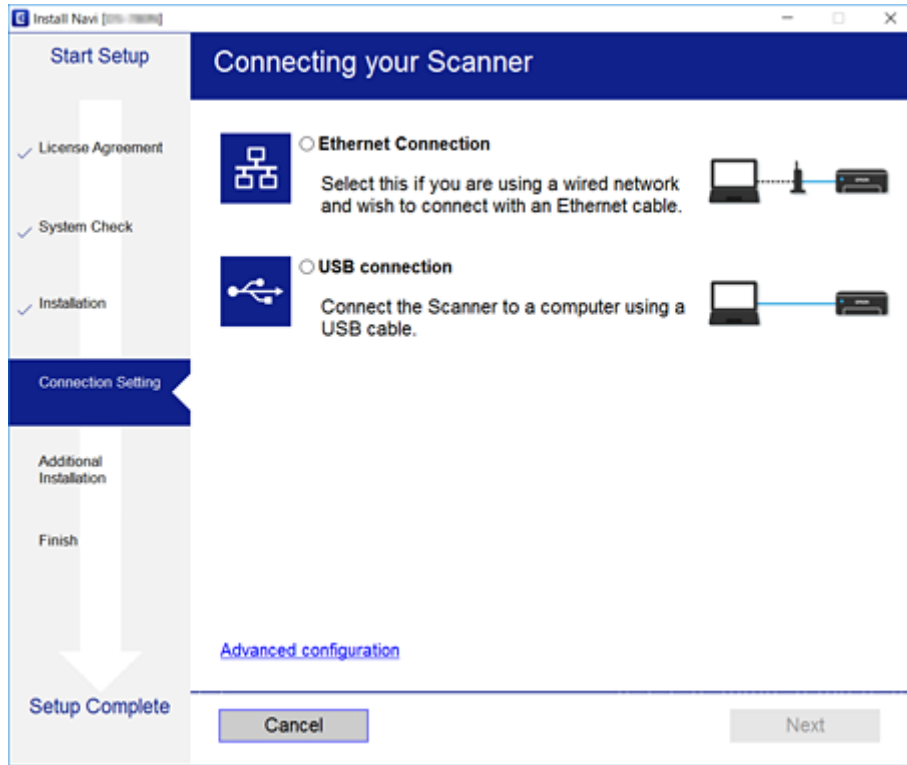
❏ Mac OS

Select the connection type.
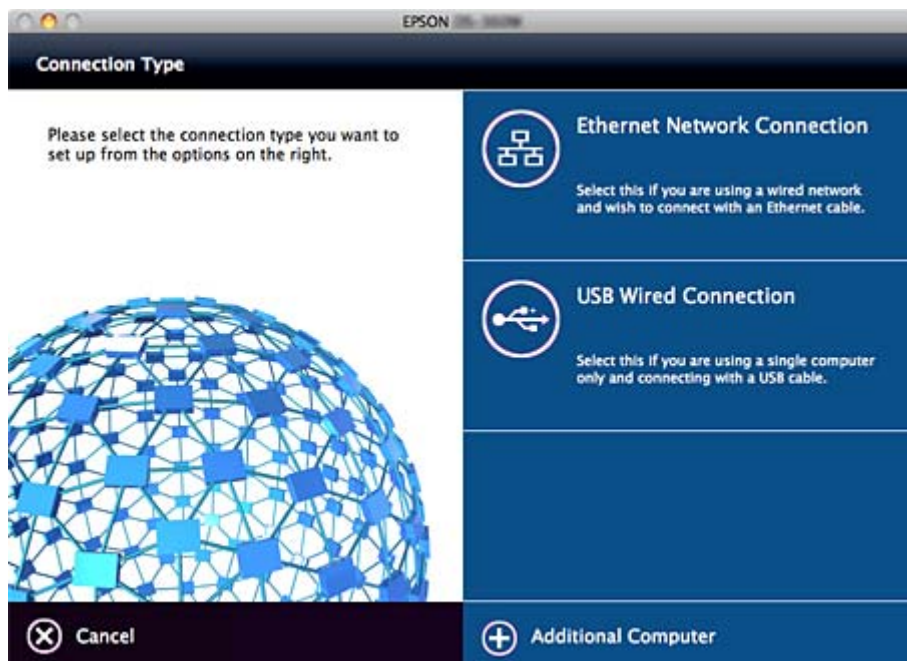
Connection

Follow the on-screen instructions. The necessary software is installed.

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 browser-based application for configuring the scanner's settings.

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

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

There are two setting pages as below.

❏ **Basic Settings**

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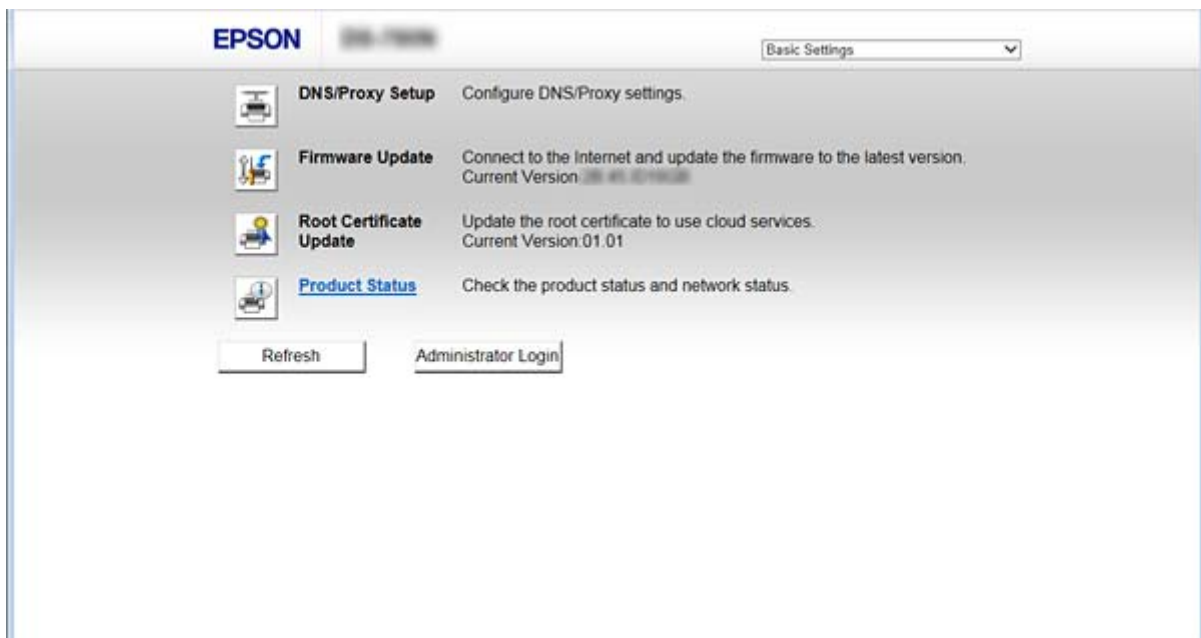
❏ **Advanced Settings**

You can configure the advanced settings for the scanner. This page is mainly for an administrator.
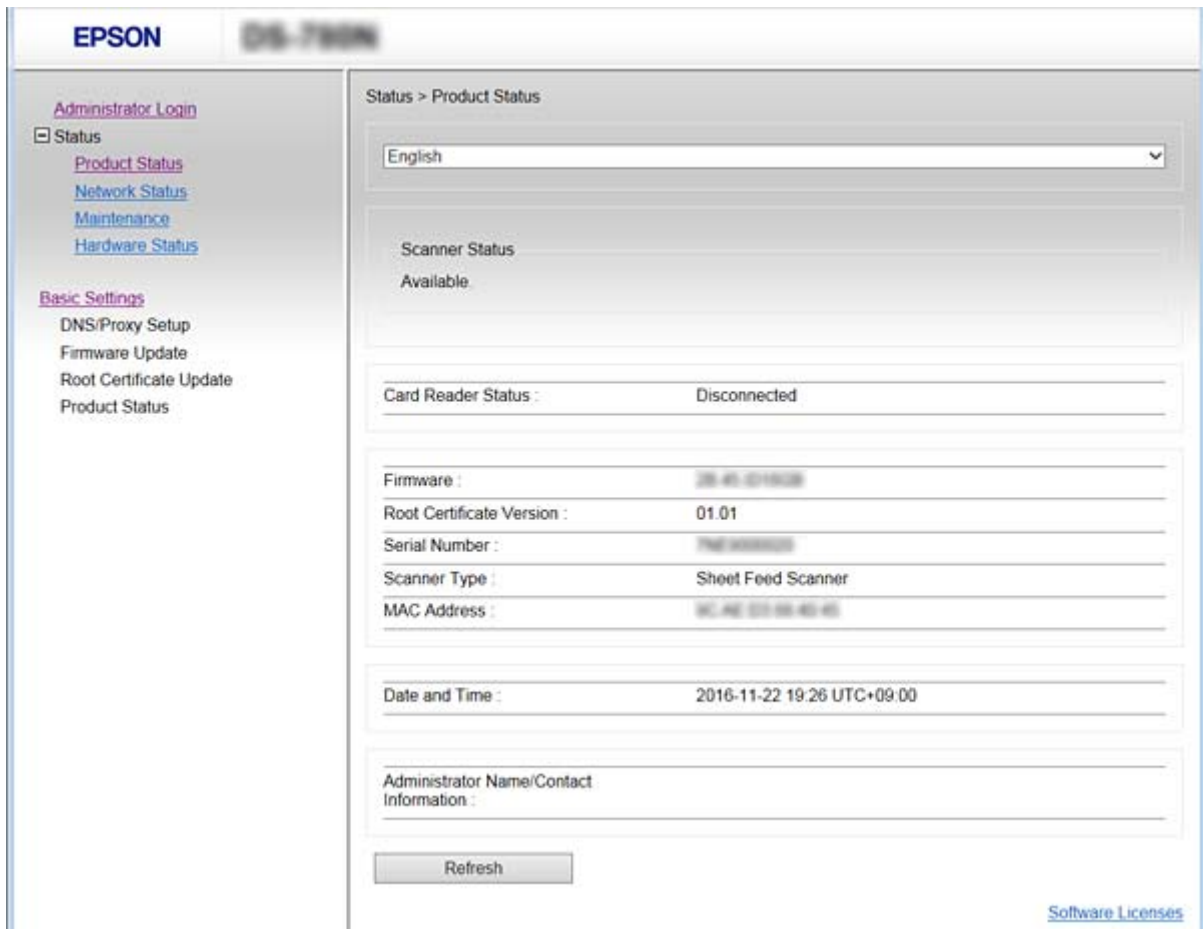
Accessing Web Config

Enter the scanner'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 scanner, is used.

❏ Accessing via HTTPS

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

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

❏ Accessing via HTTP

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

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

Note:
❏ *Examples*

   IPv4:

   https://192.0.2.111/

   http://192.0.2.111/

   IPv6:

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

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

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

Related Information

➡

➡

Using Scan Functions

Depending on how you use the scanner, install the following software and make settings using it.

❏ **Scan from computer**

   ❏ Confirm the validity of the network scan service with Web Config (valid at factory shipment).

   ❏ Install Epson Scan 2 on your computer and set the IP address

   ❏ When scanning using jobs, install Document Capture Pro (Document Capture) and set job settings.

❏ **Scan from operation panel**

   ❏ When using Document Capture Pro or Document Capture Pro Server:

      Install Document Capture Pro or Document Capture Pro Server

      Make settings for Document Capture Pro or Document Capture Pro Server (server mode, client mode).

   ❏ When using the WSD protocol:

      Confirm the validity of WSD on Web Config or operation panel (valid at factory shipment)

      Additional device settings (Windows computer).

Scanning From a Computer

Install the software and check that the network scan service is enabled to scan via a network from the computer.

Related Information

➡

➡

Software to be installed

❏ Epson Scan 2

This is a scanner driver. If you use the device from a computer, install the driver on each client computer. If Document Capture Pro/Document Capture is installed, you can perform the operations assigned to the buttons of the device.

With EpsonNet SetupManager, printer drivers can also be distributed together in packages.

❏ Document Capture Pro (Windows) / Document Capture (Mac OS)

Install on the client computer. You can call and execute jobs registered on a computer with Document Capture Pro / Document Capture installed on the network from the computer and scanner's operation panel.

You can also scan from the computer via the network. Epson Scan 2 is required to scan.

Related Information

➡ "EpsonNet SetupManager" on page 56

Set the scanner's IP address to Epson Scan 2

Specify the IP address of the scanner so that the scanner can be used on the network.

1. Start **Epson Scan 2 Utility** from **Start** > **All Programs** > **EPSON** > **Epson Scan 2**.

   If another scanner is already registered, go to step 2.

   If not registered, go to step 4.

2. Click ▼ on **Scanner**.

3. Click **Settings**.

4. Click **Enable Editing**, and then click **Add**.

5. Select the scanner model name from **Model**.

6. Select the IP address of the scanner to be used from **Address** in **Search for Network**.

   Click and click to update the list. If you can not find the IP address of the scanner, select **Enter address** and enter the IP address.

7. Click **Add**.

8. Click **OK**.

Enable Network Scan

You can set the network scan service when you scan from a client computer over the network. The default setting is enabled.

1. Access Web Config and select **Services** > **Network Scan**.

2. Make sure that **Enable scanning** of **EPSON Scan** is selected.

   If it is selected, this task is completed. Close Web Config.

   If it is cleared, select it and go to next step.

3. Click **Next**.

4. Click **OK**.

   The network is re-connected, and then the settings are enabled.

Related Information

➡

Scanning using the control panel

The scan to folder function and the scan to mail function using the scanner's control panel, as well as the transfer of scan results to mail, folders, etc. are performed by executing a job from the computer.

When transferring scan results, set up the job with Document Capture Pro Server or Document Capture Pro.

For details about settings and setting up the job, see the documentation or help for Document Capture Pro Server or Document Capture Pro.

Related Information

➡
➡

Software to install on the computer

❏ **Document Capture Pro Server**

   This is the server version of Document Capture Pro. Install it on a Windows server. Multiple devices and jobs can be centrally managed by the server. Jobs can be executed simultaneously from multiple scanners.

   By using the certified version of Document Capture Pro Server, you can manage jobs and scan history linked to users and groups.

   For details of Document Capture Pro Server, contact your local Epson office.

❏ **Document Capture Pro (Windows) / Document Capture (Mac OS)**

   Just like scanning from a computer, you can call up jobs registered on the computer from the control panel and execute them. It is not possible to run computer jobs simultaneously from multiple scanners.

Document Capture Pro Server / Document Capture Pro settings

Make settings for using the scanning function from the scanner's operation panel.

1. Access Web Config and select **Services** > **Document Capture Pro**.

Function Settings

2. Select **Operation Mode**.

  ❏ Server Mode:

  Select this when using Document Capture Pro Server or when using Document Capture Pro only for jobs that have been set for a specific computer.

  ❏ Client Mode:

  Set this when you select the job setting of Document Capture Pro (Document Capture) installed on each client computer in the network without specifying the computer.

3. Set the following according to the selected mode.

  ❏ Server Mode:

  In **Server Address**, specify the server on which Document Capture Pro Server is installed. It can be 2 to 252 characters in IPv4, IPv6, host name, FQDN format. In the FQDN format, US - ASCII letters, numbers, alphabets, and hyphens (except leading and trailing) can be used.

  ❏ Client Mode:

  Specify **Group Settings** to use a scanner group specified from Document Capture Pro (Document Capture).

4. Click **Settings**.

Related Information

➡

Settings of Servers and Folders

Document Capture Pro and Document Capture Pro Server save the scanned data to the server or client computer once and use the transfer function to execute the scan to folder function and scan to mail function.

You need the authority and information to transfer from the computer on which Document Capture Pro, Document Capture Pro Server is installed to the computer or cloud service.

Prepare the information on the function you will use, referring to the following.

You can make settings for these functions using Document Capture Pro or Document Capture Pro Server. For details about the settings, see the documentation or help for Document Capture Pro Server or Document Capture Pro.

Name	Settings	Requirement
Scan to Network Folder (SMB)	Create and set up sharing of the save folder	The administrative user account to the computer that creates save folders.
	Destination for Scan to Network Folder (SMB)	User name and password to log on to the computer that has the save folder, and the privilege to update the save folder.
Scan to Network Folder (FTP)	Setup for FTP server log on	Logon information for the FTP server and the privilege to update the save folder.
Scan to Email	Setup for email server	Setup information for email server

Function Settings

Name	Settings	Requirement
Scan to Document Capture Pro (when using Document Capture Pro Server)	Setup for logging on cloud services	Internet connection environment Registration of the account for cloud services

Use WSD scan (Windows only)

If the computer uses Windows Vista or later, you can use WSD scan.

When the WSD protocol can be used, the **Computer (WSD)** menu will be displayed on the scanner control panel.

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

2. Confirm that **Enable WSD** is checked in **WSD Settings**.

    If it is checked, your task is complete and you may close Web Config.

    If it is not checked, check it and proceed to the next step.

3. Click the **Next** button.

4. Confirm the settings and click **Settings**.

Making System Settings

Making System Settings on the Control Panel

Set screen brightness

Set the LCD screen brightness.

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

2. Tap **Common Settings** > **LCD Brightness**.

3. Tap ⊕ or ⊖ to adjust the brightness.

    You can adjust from 1 to 9.

4. Tap **OK**.

Set sound

Set panel operation sound and error sound.

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

2. Tap **Common Settings** > **Sound**.

3. Set the following items as necessary.

   ❏ Operation sound

      Set the volume of the operation sound of the operation panel.

   ❏ Error sound

      Set the volume of the error sound.

4. Tap **OK**.

Related Information

➡ "Accessing Web Config" on page 23

Detect double feed of original

Determine the function to detect double feed of the document to be scanned and to stop the scan when multiple feed occurs.

To scan originals that are deemed to be multi-fed, such as envelopes or paper with stickers, set them to off.

Note:
It can also be set from Web Config or Epson Scan 2.

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

2. Tap **External Scan Settings** > **Ultrasonic Double Feed Detection**.

3. Tap **Ultrasonic Double Feed Detection** to switch it on or off.

4. Tap **Close**.

Set low speed mode

Set to scan at low speed so that paper jams do not occur when scanning thin documents such as slips.

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

2. Tap **External Scan Settings** > **Slow**.

3. Tap **Slow** to switch it on or off.

4. Tap **Close**.

Making System Settings Using Web Config

Power Saving Settings During Inactivity

Make the power saving setting for the scanner's period of inactivity. Set the time depending on your usage environment.

Note:
You can also make the power saving settings on the scanner's control panel.

1. Access Web Config and select **System Settings** > **Power Saving**.

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

    You can set up to 240 minutes by the minute.

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

4. Click **OK**.

Related Information

➡ "Accessing Web Config" on page 23

Setting the Control Panel

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

1. Access Web Config and select **System Settings** > **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.

3. Click **OK**.

Related Information

➡ "Accessing Web Config" on page 23

Setting the Restriction for the External Interface

You can restrict the USB connection from the computer. Set it to limit scanning other than via the network.

1. Access Web Config and select **System Settings** > **External Interface**.

2. Select **Enable** or **Disable**.

   To restrict, select **Disable**.

3. Click **OK**.

Synchronizing the Date and Time with Time Server

If you use a CA certificate, you can prevent trouble with the time.

1. Access Web Config and select **System Settings** > **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

➡ "Accessing Web Config" on page 23

Basic Security Settings

This chapter explains the basic security settings that do not require a special environment.

Introduction of Basic Security Features

We introduce he basic security features of Epson Devices.

Feature name	Feature type	What to set	What to prevent
Setup for the administrator password	Lock the settings related to the system, such as network and USB connection settings, so that it can not be changed except by the administrator.	An administrator sets a password to the device. Configuration or update are available anywhere from Web Config, the control panel, Epson Device Admin, and EpsonNet Config.	Prevent from illegally reading and changing the information stored in the device such as ID, password, and network settings. Also, reduce a wide range of security risks such as leakage of information for the network environment or security policy.
Controls protocols	Controls protocols used for communication between devices and computers, and enables / disables functions.	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.

Related Information

➡ "About Web Config" on page 22

➡ "EpsonNet Config" on page 55

➡ "Epson Device Admin" on page 55

➡ "Configuring the Administrator Password" on page 32

➡ "Controlling protocols" on page 35

Configuring the Administrator Password

When you set the administrator password, users other than the administrators will not be able to change the settings for the system administration. You can set and change the administrator password using either Web Config, the scanner's control panel, or software (Epson Device Admin or EpsonNet Config). When using the software, see the documentation for each software.

Related Information

➡ "Configuring the Administrator Password from the Control Panel" on page 33

➡ "Configuring the Administrator Password Using Web Config" on page 33

➡ "EpsonNet Config" on page 55

➡ "Epson Device Admin" on page 55

Configuring the Administrator Password from the Control Panel

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

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

2. Tap **System Administration** > **Admin Settings**.

   If the item is not displayed, flick the screen upward to display the item.

3. Tap **Admin Password** > **Register**.

4. Enter the new password, and then tap **OK**.

5. Enter the password again, and then tap **OK**.

6. Tap **OK** on the confirmation screen.

   The administrator settings screen is displayed.

7. Tap **Lock Setting**, and then tap **OK** on the confirmation screen.

   Lock Setting is set to **On**, and the administrator password will be required when you operate the locked menu item.

Note:
❏ *If you set **Settings** > **Common Settings** > **Operation Time Out** to **On**, the scanner will log you off after a period of inactivity on the control panel.*

❏ *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 usingWeb Config.

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

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.
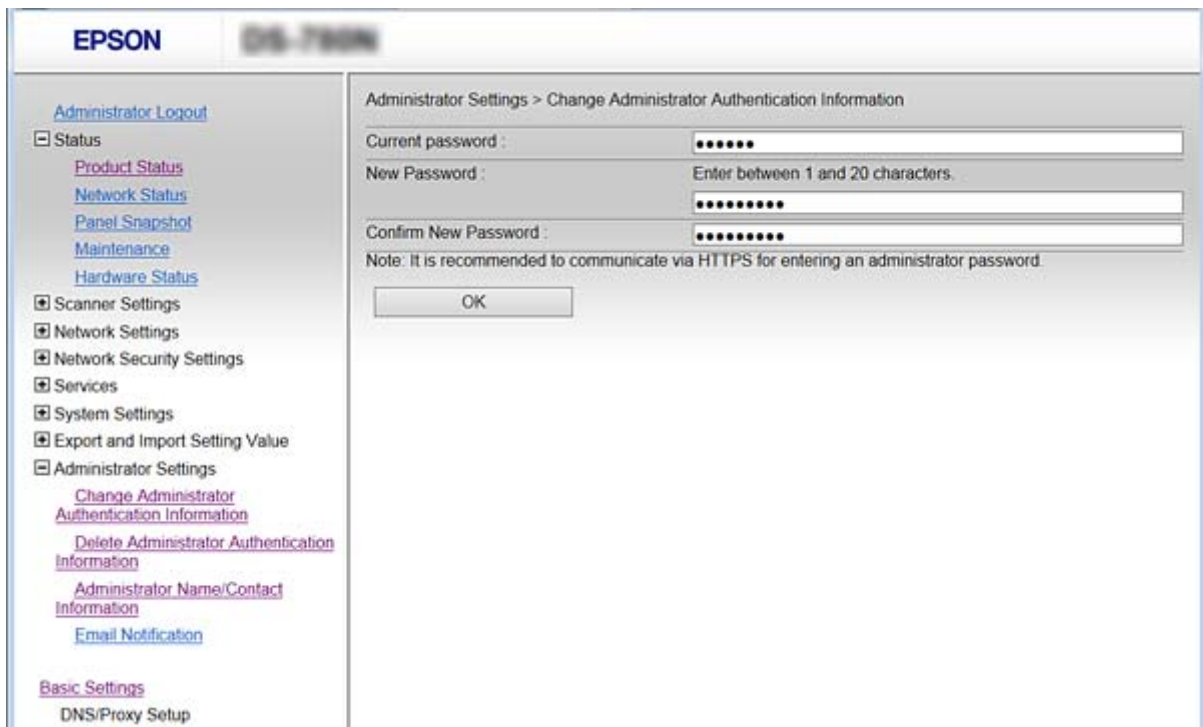
3. Select **OK**.

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

    ❏ *To delete the administrator password, click**Administrator Settings** > **Delete Administrator Authentication Information**, and then enter the administrator password.*

Related Information

➡

Items to be Locked by Administrator Password

Administrators have setting and change privileges for all features on devices.

Also, if you set the administrator password on the device, you can lock it so that you can not change items related to device management.

The following are the items that an administrator can control.

Item	Description
Scanner setting	Setting of double feed detection and low speed mode.
Ethernet connection settings	Change the name of devices and the IP address, setup of the DNS server or proxy server, and setting changes related to network connections.

Basic Security Settings

Item	Description
User services setting	Setup for controling communication protocols, Network scan, and Document Capture Pro services.
Email server setting	Setup of an email server that devices directly communicate with.
Security setting	Settings for network security, such as SSL/TLS communication, IPsec/IP filtering, and IEEE802.1X.
Root Certificate Update	Update of root certificates required for Document Capture Pro Server authentication and firmware update from Web Config.
Firmware update	Check and update the firmware of devices.
Time, timer setting	Sleep transition time, auto power off, date/time, non-operation timer, other settings related to a timer.
Restore to default settings	Setting for the scanner to be re-set to factory settings.
Administrator setting	Setting of the administrator lock or administrator password.
Certified device setting	ID setting of the authentication device. Set when using the scanner on an authentication system that supports authentication devices.

Controlling protocols

You can scan using a variety of pathways and protocols. You can also use network scanning from an unspecified number of network computers. For example, scanning using only specified pathways and protocols are allowed. You can lower unintended security risks by restricting scanning from specific pathways or by controlling the available functions.

Configure the protocol settings.

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

2. Configure each item.

3. Click **Next**.

4. Click **OK**.

    The settings are applied to the scanner.

Related Information

➡ "Accessing Web Config" on page 23
➡ "Protocols you can Enable or Disable" on page 36
➡ "Protocol Setting Items" on page 37

Protocols you can Enable or Disable

Protocol	Description
Bonjour Settings	You can specify whether to use Bonjour. Bonjour is used to search for devices, scan and so on.
SLP Settings	You can enable or disable the SLPfunction. SLP is used for Epson Scan 2 and network searching in EpsonNet Config.
WSD Settings	You can enable or disable the WSD function. When this is enabled, you can add WSD devices or scan 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.
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.

Related Information

➡

➡

Protocol Setting Items

Items	Setting value and Description
Bonjour Settings	

Basic Security 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	You can display and set the Bonjour service name.
Location	Displays the Bonjour location name.
SLP Settings	
Enable SLP	Select this to enable the SLP function. It is used for network discovery in Epson Scan 2 and EpsonNet Config.
WSD Settings	
Enable WSD	Select this to enable adding devices using WSD, and print and scan from the WSD port.
Scanning Timeout (sec)	Enter the communication timeout value for WSD scanning between 3 to 3,600 seconds.
Device Name	Displays the WSD device name.
Location	Displays the WSD location name.
LLTD Settings	
Enable LLTD	Select this to enable LLTD. The scanner is displayed in the Windows network map.
Device Name	Displays the LLTD device name.
LLMNR Settings	
Enable LLMNR	Select this to enable LLMNR. You can use name resolution without NetBIOS even if you cannot use DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Select to enable SNMPv1/v2c. Only scanners 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	
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.

Basic Security Settings

Items	Setting value and Description
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.
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.

Related Information

Operation and Management Settings

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

Confirm Information of a Device

You can check the following information of the operating device 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.

❏ Panel Snapshot

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

❏ Maintenance

Check the Start Date, Scanning Information, etc.

❏ Hardware Status

Check the status of the scanner.

Related Information

➡

Managing Devices (Epson Device Admin)

You can manage and operate many devices using Epson Device Admin. Epson Device Admin allows you to manage devices located on a different network. The following outlines the main management features.

For more information about functions and using the software, see the documentation or help of Epson Device Admin.

❏ Discovering devices

You can discovering devices on the network, and then register them to a list. If Epson devices such as printers and scanners are connected to the same network segment as the administrator's computer, you can find them even if they have not been assigned an IP address.

You can also discover devices that are connected to computers on the network by USB cables. You need to install the Epson Device USB Agent on the computer.

❏ Setting devices

You can make a template containing setting items such as the network interface and the paper source, and apply it to other devices as shared settings. When it is connected to the network, you can assign an IP address on a device that has not been assigned an IP address.

Operation and Management Settings

❏ Monitoring devices

You can regularly acquire the status and detailed information for devices on the network. You can also monitor devices that are connected to computers on the network by USB cables and devices from other companies that have been registered to the device list. To monitor devices connected by USB cables, you need to install the Epson Device USB Agent.

❏ Managing alerts

You can monitor alerts about the status of devices and consumables. The system automatically sends notification emails to the administrator based on set conditions.

❏ Managing reports

You can create regular reports as the system accumulates data on device usage and consumables. You can then save these created reports and send them by email.

Related Information

➡ "Epson Device Admin" on page 55

Receiving Email Notifications When Events Occur

About Email Notifications

You can use this feature to receive alerts by email when events occur. You can register up to 5 email addresses and choose which events you want to receive notifications for.

The mail server must be configured to use this function.

Related Information

➡ "Configuring a Mail Server" on page 42

Configuring Email Notification

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

1. Access Web Config and select **Administrator Settings** > **Email Notification**.

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

3. Select the language for the email notifications.

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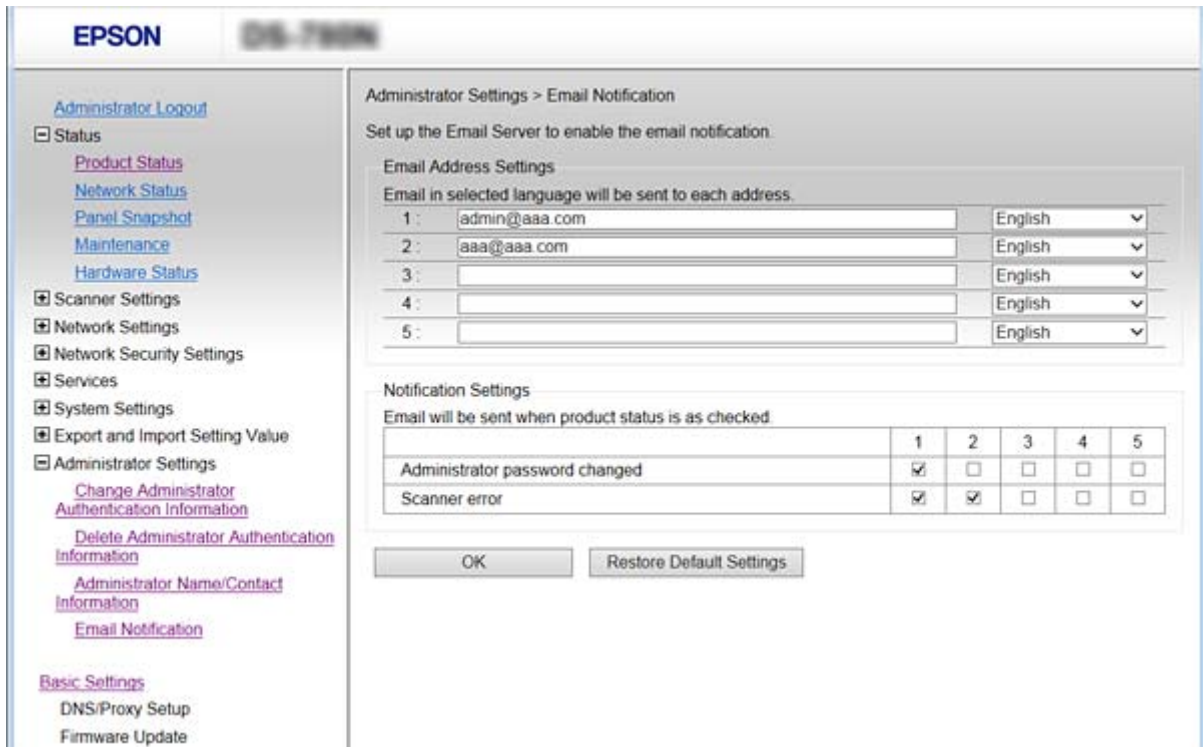
5. Click **OK**.

Related Information

➡ "Accessing Web Config" on page 23

➡ "Configuring a Mail Server" on page 42

Configuring a Mail Server

Check the following before configuring.

❑ The scanner is connected to a network.

❑ The computer's email server information.

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

2. Enter a value for each item.

3. Select **OK**.

The settings you have selected are displayed.

Related Information

➡ "Accessing Web Config" on page 23

➡ "Mail Server Setting Items" on page 43

Mail Server Setting Items

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

Operation and Management Settings

Items	Settings and Explanation	
Secure Connection	Specify the secure connection method for the email server.	
	None	If you select **POP before SMTP** in **Authentication Method**, the connection method is set to **None**.
	SSL/TLS	This is available when **Authentication Method** is set to **Off** or **SMTP AUTH**.
	STARTTLS	This is available when **Authentication Method** is set to **Off** or **SMTP AUTH**.
Certificate Validation	The certificate is validated when this is enabled. We recommend this is set to **Enable**.	
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

1. Access Web Config and select **Network Settings** > **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	Explanation
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 scanner is not connected to a network ❏ SMTP server is down ❏ Network connection is disconnected while communicating ❏ Received incomplete data

Operation and Management Settings

Messages	Explanation
POP3 server communication error. Check the following. - Network Settings	This message appears when ❏ The scanner 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.
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 scanner'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 scanner 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.

Operation and Management Settings

Messages	Explanation
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 product until processing is complete.	This message appears when the scanner is busy.

Related Information

Updating Firmware

Updating Firmware UsingWeb Config

Updates firmware using Web Config. The device must be connected to the Internet.

1. Access Web Config and select **Basic Settings** > **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 device's firmware. See the Epson Device Admin guide or help for more details.

Related Information

Updating Firmware by Using Epson Firmware Updater

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 device by USB cable.

3. Double-click the downloaded .exe file.

   Epson Firmware Updater starts.

4. Follow the on-screen instructions.

Backing Up the Settings

By exporting the setting items on Web Config, you can copy the items to the other scanners.

Export the settings

Export each setting for the scanner.

1. Access Web Config, and then select **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 scanner's network settings such as the scanner name and IP address, select **Enable to select the individual settings of device** and select more items. Only use the selected values for the replacement scanner.*

Related Information

➡ "Accessing Web Config" on page 23

Import the settings

Import the exported Web Config file to the scanner.

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

1. Access Web Config, and then select **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**.

5. Click **OK**.

The settings are applied to the scanner.

Operation and Management Settings

Related Information

➡

Solving Problems

Tips for Solving Problems

You can find more information in the following manual.

❏ User's Guide

Provides instructions on using the scanner, maintenance, and solving 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.

Initializing the Network Settings

Restoring the Network Settings from the Control Panel

You can restore all network settings to their defaults.

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

2. Tap **System Administration** > **Restore Default Settings** > **Network Settings**.

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

4. When a completion message is displayed, tap **Close**.

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

Checking the Communication between Devices and Computers

Checking the Connection Using a Ping Command - Windows

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

1. Check the scanner's IP address for the connection that you want to check.

   You can check this using Epson Scan 2.

Solving Problems

2. Display the computer's command prompt screen.

   ❑ Windows 10

   Right-click the start button or press and hold it, and then select **Command Prompt**.

   ❑ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

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

   ❑ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 or earlier
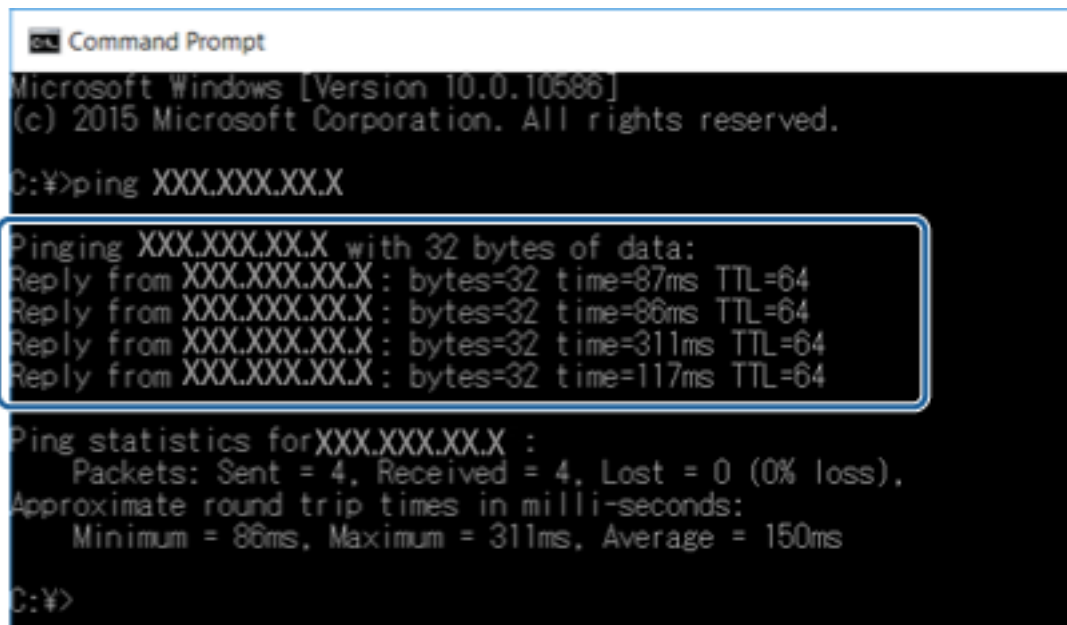
   Click the start button, select **All Programs** or **Programs** > **Accessories** > **Command Prompt**.

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

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

4. Check the communication status.

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

Solving Problems

If the scanner and the computer are not communicating, the following message is displayed.
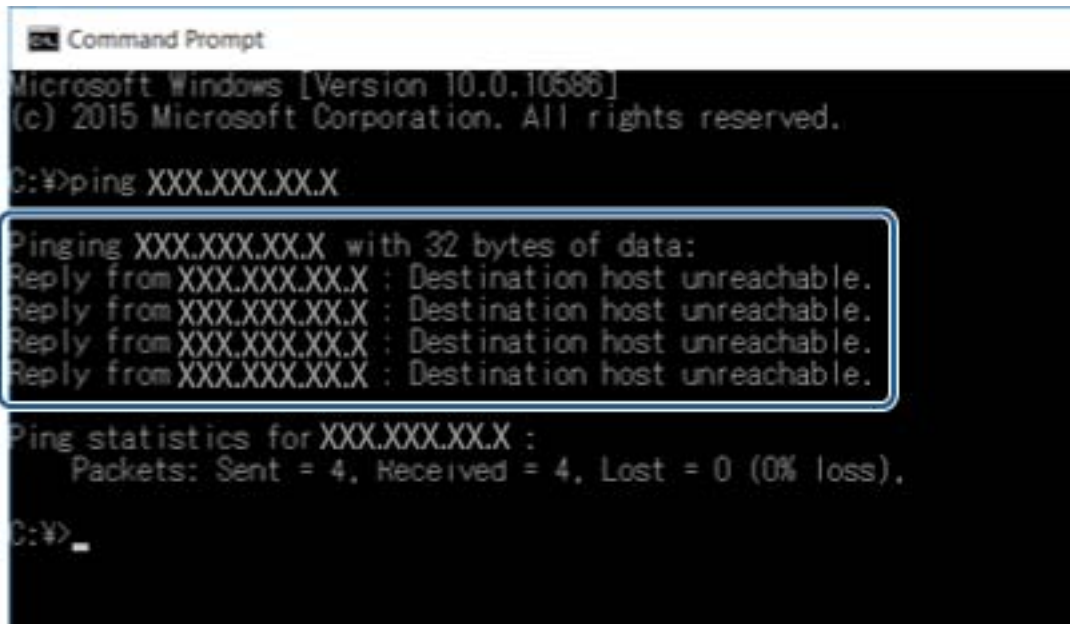
Checking the Connection Using a Ping Command - Mac OS

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

1. Check the scanner's IP address for the connection that you want to check.

   You can check this using Epson Scan 2.

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**.
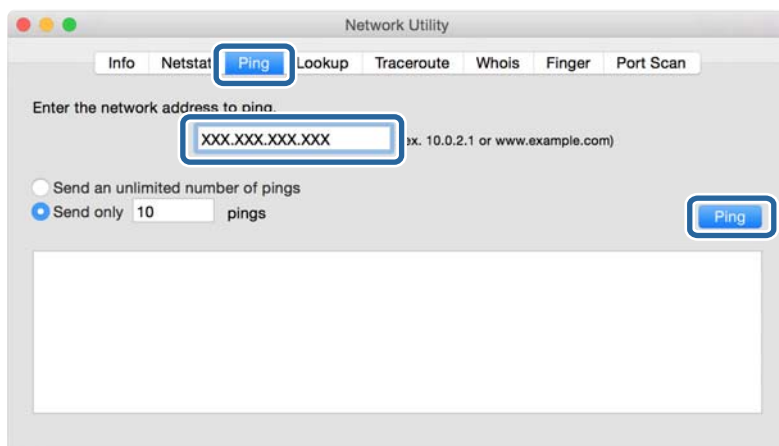
4. Check the communication status.

   If the scanner and the computer are communicating, the following message is displayed.
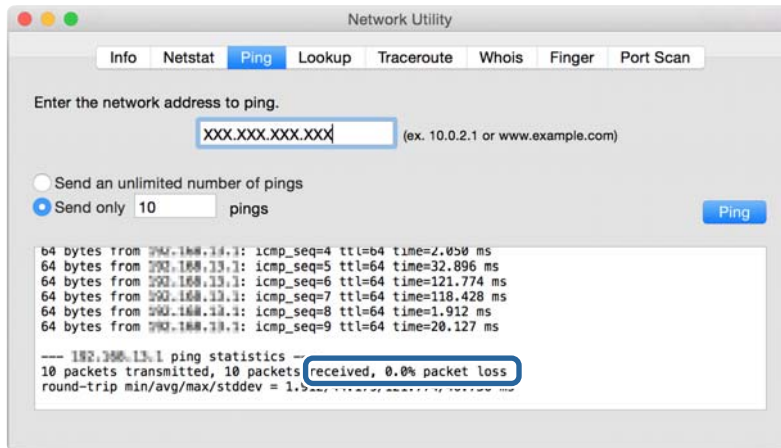
If the scanner and the computer are not communicating, the following message is displayed.
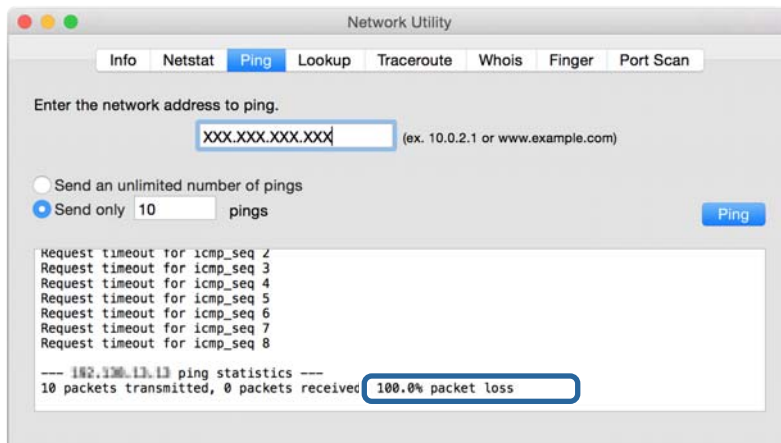
Problems Using Network Software

Cannot Access Web Config

Is the IP address of the scanner properly configured?

Configure the IP address using Epson Device Admin or EpsonNet Config.

Does your browser support the bulk encryptions for the Encryption Strength for SSL/TLS?

The bulk encryptions for the Encryption Strength for SSL/TLS are as follows. Web Config can only be accessed in a browser supporting the following bulk encryptions. Check your browser's encryption support.

❏ 80bit: AES256/AES128/3DES

❏ 112bit: AES256/AES128/3DES

❏ 128bit: AES256/AES128

❏ 192bit: AES256

❏ 256bit: AES256

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

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

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

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

The scanner is being accessed via a proxy server.

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

❏ Windows:

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

❏ Mac OS:

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

Example:

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

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

Related Information

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

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

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

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

Is the communication error timeout setting too short?

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

Solving Problems

Related Information

➡

➡

Appendix

Introduction of Network Software

The following describes the software that configures and manages devices.

Epson Device Admin

Epson Device Admin is an application that allows you to install devices on the network, and then configure and manage the devices. You can acquire detailed information for devices such as status and consumables, send notifications of alerts, and create reports for device usage. You can also make a template containing setting items and apply it to other devices as shared settings. 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 allows the administrator to configure the scanner's network settings, such as assigning an IP address and changing the connection mode. The batch setting feature is supported on Windows. For more information, see the documentation or help of EpsonNet Config.

Appendix

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 SetupManager

EpsonNet SetupManager is a software to create a package for a simple scanner installation, such as installing and configuring the scanner driver, and installing Document Capture Pro. This software allows the administrator to create unique software packages and distribute them among groups.

For more information, visit your regional Epson website.

Assigning an IP Address Using EpsonNet Config

You can assign an IP address to the scanner using EpsonNet Config. EpsonNet Config allows you to assign an IP address to a scanner that has not been assigned one after connecting using an Ethernet cable.

Assigning IP Address Using Batch Settings

Creating the File for Batch Settings

Using the MAC address and model name as the keys, you can create a new SYLK file to set the IP address.

1. Open a spreadsheet application (such as Microsoft Excel) or a text editor.

2. Enter "Info_MACAddress", "Info_ModelName", and "TCPIP_IPAddress" in the first row as the setting item names.

   Enter setting items for the following text strings. To distinguish between upper case/lower case and double-byte/single-byte characters, if only one character is different, the item will not be recognized.

   Enter the setting item name as described below; otherwise, EpsonNet Config cannot recognize the setting items.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Enter the MAC address, model name, and IP address for each network interface.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

Appendix

0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4.   Enter a name and save as a SYLK file (*.slk).

Making Batch Settings Using the Configuration File

Assign IP addresses in the configuration file (SYLK file) at one time. You need to create the configuration file before assigning.

1.   Connect all devices to the network using Ethernet cables.

2.   Turn on the scanner.

3.   Start EpsonNet Config.

A list of the scanners on the network is displayed. It may take a while before they are displayed.

4.   Click **Tools** > **Batch Settings**.

5.   Click **Open**.

6.   On the file selection screen, select the SYLK file (*.slk) containing the settings, and then click **Open**.

Appendix

7. Select the devices for which you want to perform batch settings with the **Status** column set to **Unassigned**, and the **Process Status** set to **Assign Successful**.

When making multiple selections, press Ctrl or Shift and click or drag your mouse.
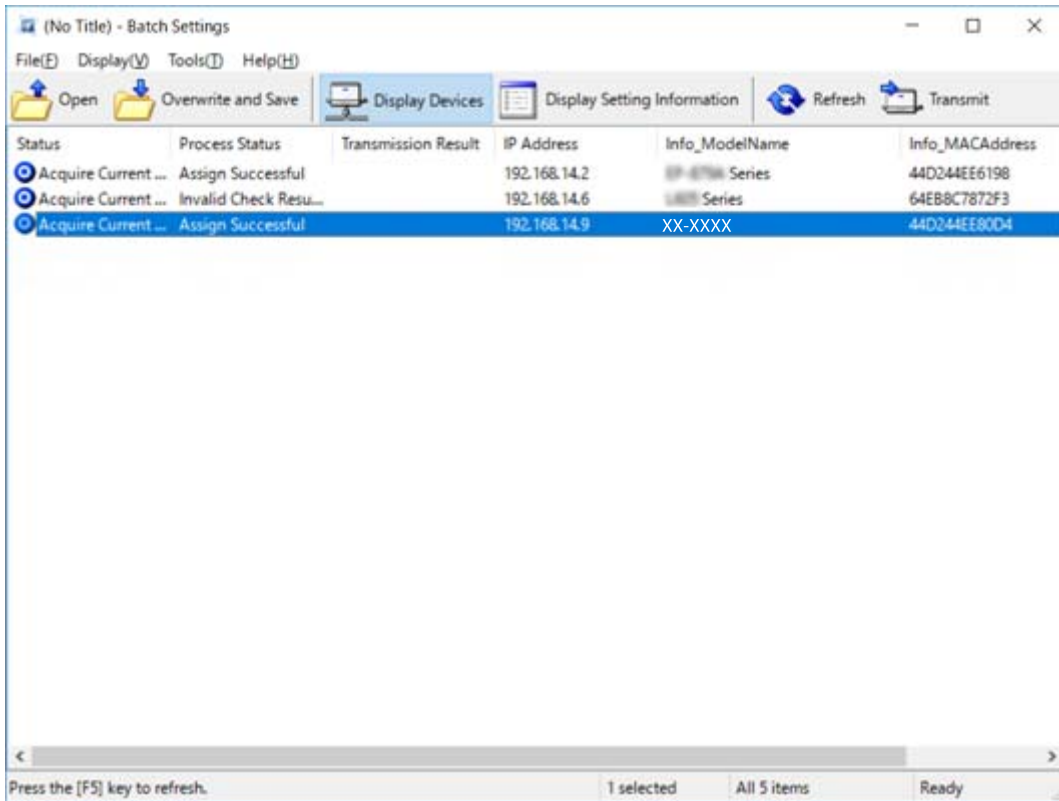
8. Click **Transmit**.

9. When the password entry screen is displayed, enter the password, and then click **OK**.

Transmit the settings.

Note:
The information is transmitted to the network interface until the progress meter is finished. Do not turn off the device or the wireless adapter, and do not send any data to the device.

10. On the **Transmitting Settings** screen, click **OK**.

Appendix

11. Check the status of the device you set.

    For devices that show ![icon] or ![icon], check the contents of the settings file, or that the device has rebooted normally.

Icon	Status	Process Status	Explanation
●	Setup Complete	Setup Successful	Setup completed normally.
●	Setup Complete	Rebooting	When information has been transmitted, each device needs to reboot to enable the settings. A check is performed to determine whether or not the device can be connected to after rebooting.
●	Setup Complete	Reboot Failed	Cannot confirm the device after transmitting settings. Check that the device is turned on, or if it has rebooted normally.
●	Setup Complete	Searching	Searching for the device indicated in the settings file.[*]
●	Setup Complete	Search Failed	Cannot check devices that have already been setup. Check that the device is turned on, or if it has rebooted normally.[*]

*Only when setting information is displayed.

Related Information

➡ "Running EpsonNet Config - Windows" on page 56
➡ "Running EpsonNet Config - Mac OS" on page 56

Assigning an IP Address to Each Device

Assign an IP address to the scanner using EpsonNet Config.

1. Turn on the scanner.

2. Connect the scanner to the network using an Ethernet cable.

3. Start EpsonNet Config.

   A list of the scanners on the network is displayed. It may take a while before they are displayed.

4. Double-click the scanner that you want to assign to.

   Note:
   If you have connected multiple scanners of the same model, you can identify the scanner using the MAC address.

5. Select **Network** > **TCP/IP** > **Basic**.

Appendix

6. Enter the addresses for **IP Address**, **Subnet Mask**, and **Default Gateway**.
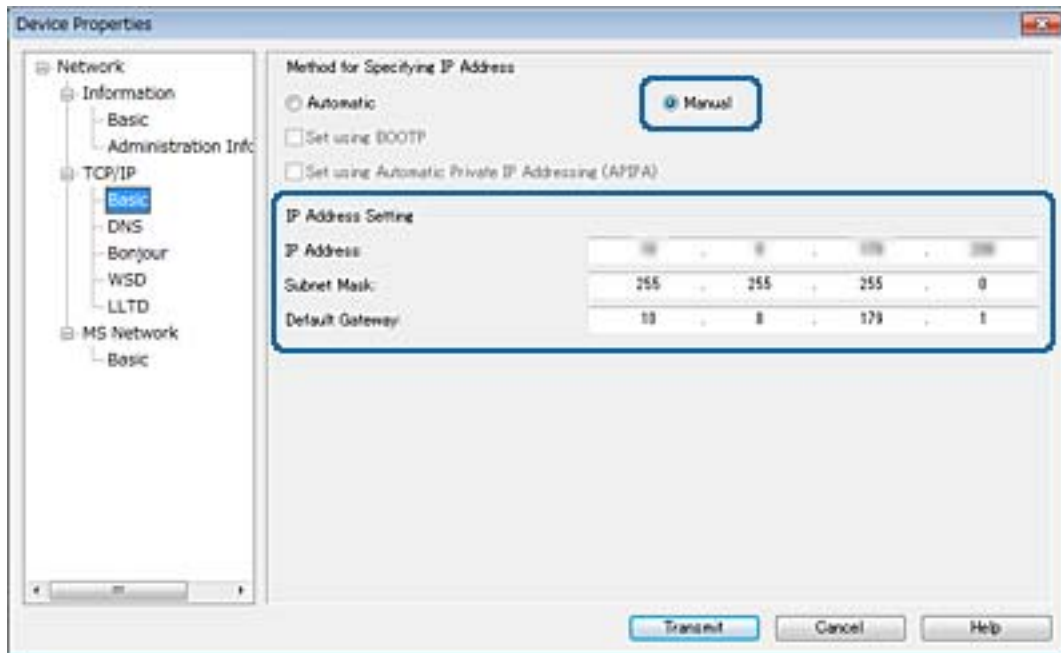
Note:
Enter a static address when you connect the scanner to a secure network.

7. Click **Transmit**.

The screen confirming transmission of the information is displayed.

8. Click **OK**.

The transmission completion screen is displayed.

Note:
The information is transmitted to the device, and then the message "Configuration successfully completed." is displayed.
Do not turn off the device, and do not send any data to the service.

9. Click **OK**.

Related Information

➡ "Running EpsonNet Config - Windows" on page 56
➡ "Running EpsonNet Config - Mac OS" on page 56

Using Port for the Scanner

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

Appendix

Sender (Client)	Use	Destination (Server)	Protocol	Port Number
Scanner	Email sending (Email notification)	SMTP server	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP before SMTP connection (Email notification	POP server	POP3 (TCP)	110
	Control WSD	Client computer	WSD (TCP)	5357
	Search the computer when push scanning from Document Capture Pro	Client computer	Network Push Scan Discovery	2968
	Collecting the job information when push scanning from Document Capture Pro	Client computer	Network Push Scan	2968
Client Computer	Discover the scanner from an application such as EpsonNet Config and scanner driver.	Scanner	ENPC (UDP)	3289
	Collect and set up the MIB information from an application such as EpsonNet Config and scanner driver.	Scanner	SNMP (UDP)	161
	Searching WSD scanner	Scanner	WS-Discovery (UDP)	3702
	Forwarding the scan data from Document Capture Pro	Scanner	Network Scan (TCP)	1865

Advanced Security Settings for Enterprise

In this chapter, we describe advanced security features.

Security Settings and Prevention of Danger

When a device is connected to a network, you can access it from a remote location. In addition, many people can share the device, 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 device in an environment where you can access the Internet, the risks are even higher.

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

Set the device 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 communication	The communication path of a computer and a device is encrypted using SSL/TLS communication. The content of the communication via a browser is protected.	Set a CA certificate for the server that is certificate signed by a CA (Certificate Authority) to the device.	Prevent leakage of setting information and the contents of transferred data to the scanner from the computer. Access to the Epson server on the Internet from the device can be also protected by using a firmware update, etc.
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 scanning protocol.	Create a basic policy and individual policy to set the client or type of data that can access the device.	Protect unauthorized access, and tampering and interception of communication data to the device.
SNMPv3	Features are added, such as monitoring of connected devices in the network, integrity of the data to the SNMP protocol to control, encryption, user authentication, etc.	Enable SNMPv3, then set the authentication and encryption method.	Ensure change settings via the network, confidentiality in state monitoring.
IEEE802.1X	Allows only a user who is authenticated to Ethernet to connect. Allows only a permitted user to use the device.	Authentication setting to the RADIUS server (authentication sever).	Protect unauthorized access and use to the device.

Advanced Security Settings for Enterprise

Name	Feature type	What to set	What to prevent
Read ID card	You can use the device by holding over an ID card to the authenticated device that is connected. You can limit the acquiring of logs for each user and device, and limit the available use of devices and the available features of each user and group.	Connect an authentication device to the device, and then set the information of a user in the authentication system.	Prevent unauthorized use and spoofing of the device.

Related Information

➡ "SSL/TLS Communication with the Scanner" on page 63

➡ "Encrypted Communication Using IPsec/IP Filtering" on page 71

➡ "Using SNMPv3 Protocol" on page 82

➡ "Connecting the Scanner to an IEEE802.1X Network" on page 84

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.

SSL/TLS Communication with the Scanner

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

About Digital Certification

❏ Certificate signed by a CA

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

❏ CA certificate

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

❏ Self-signed certificate

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

Related Information

➡ "Obtaining and Importing a CA-signed Certificate" on page 64

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

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

   A CSR creating page is opened.

3. Enter a value for each item.

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

4. Click **OK**.

   A completion message is displayed.

5. Select **Network Security Settings**. 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 scanner.

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

Related Information

Advanced Security Settings for Enterprise

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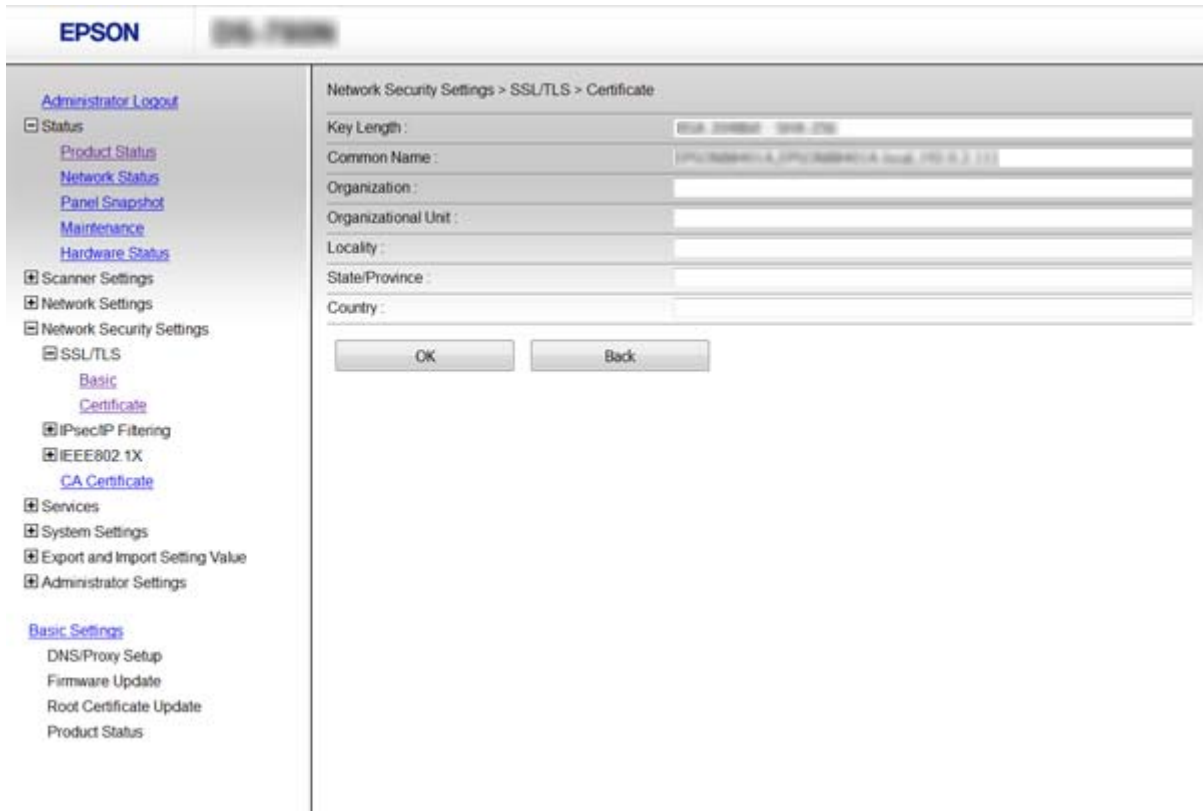
Items	Settings and Explanation
Key Length	Select a key length for a CSR.
Common Name	You can enter between 1 and 128 characters. If this is an IP address, it should be a static IP address. Example: URL for accessing Web Config: https://10.152.12.225 Common name: 10.152.12.225
Organization/ Organizational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

Related Information

Importing a CA-signed Certificate

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

Advanced Security Settings for Enterprise

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

    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 scanner 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 23
➡ "CA-signed Certificate Importing Setting Items" on page 67

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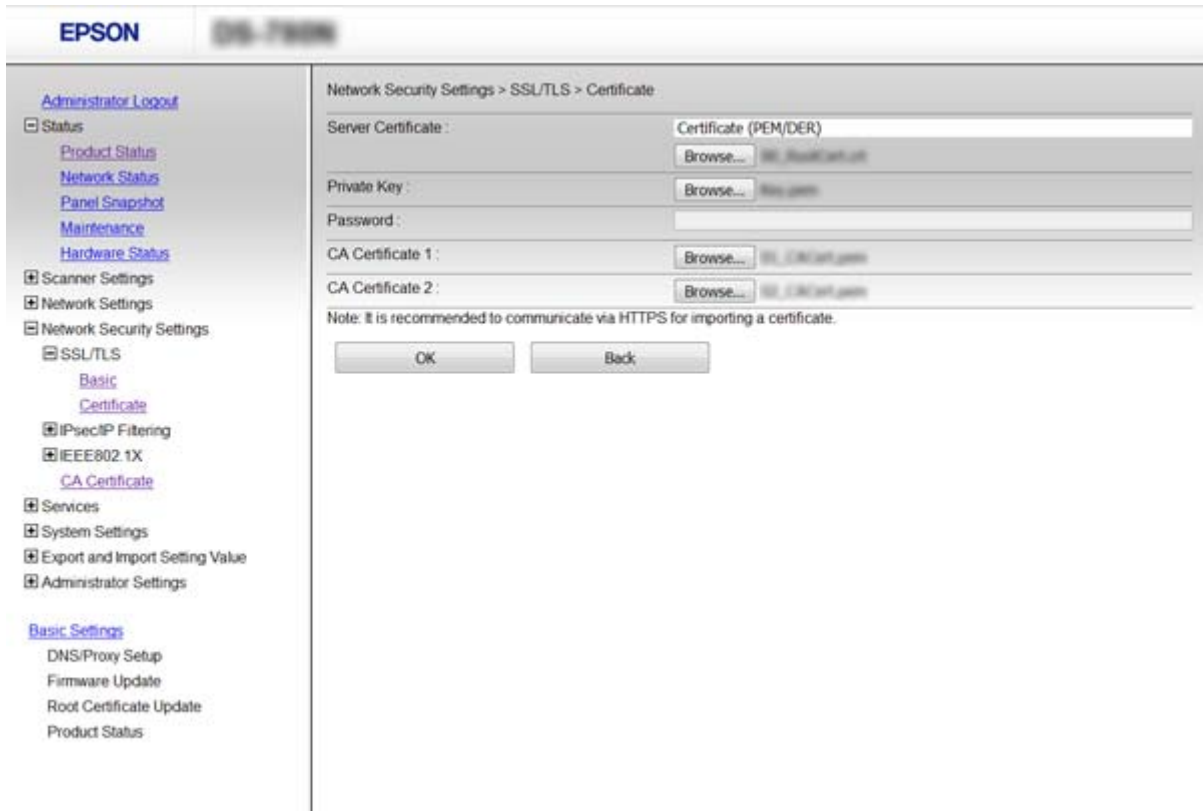
Items	Settings and Explanation
Server Certificate or Client Certificate	Select a certificate's format.
Private Key	If you obtain a certificate of the PEM/DER format by using a CSR created from a computer, specify a private key file that is match a certificate.
Password	Enter a password to encrypt a private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

Related Information

➡

Deleting a CA-signed Certificate

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

Advanced Security Settings for Enterprise

> ❗ *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 **Network Security Settings**. 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.

Related Information

➡

Updating a Self-signed Certificate

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

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

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

2. Click **Update**.

3. Enter **Common Name**.

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

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

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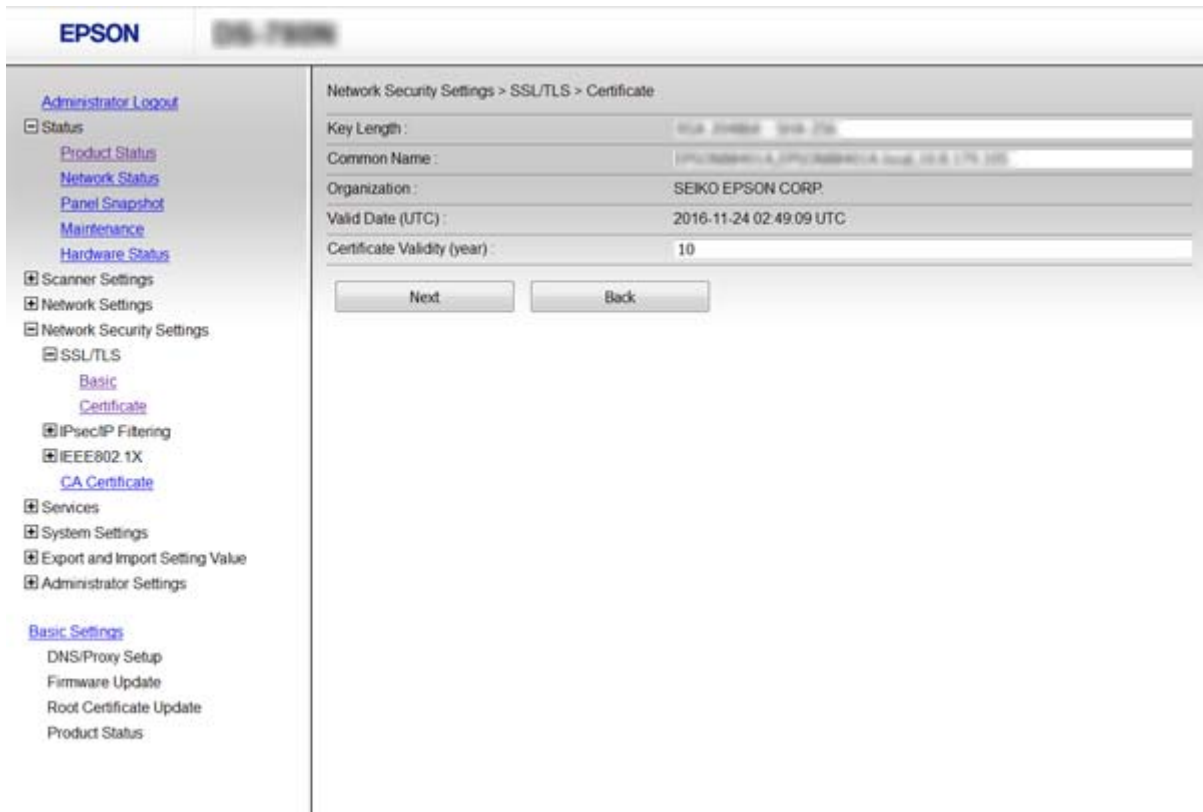
5. Click **Next**.

   A confirmation message is displayed.

6. Click **OK**.

   The scanner is updated.

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

Related Information

➡ "Accessing Web Config" on page 23

Configure CA Certificate

You can import, display, delete a CA Certificate.

Importing a CA Certificate

1. Access Web Config, and then select **Network Security Settings** > **CA Certificate**.

2. Click **Import**.

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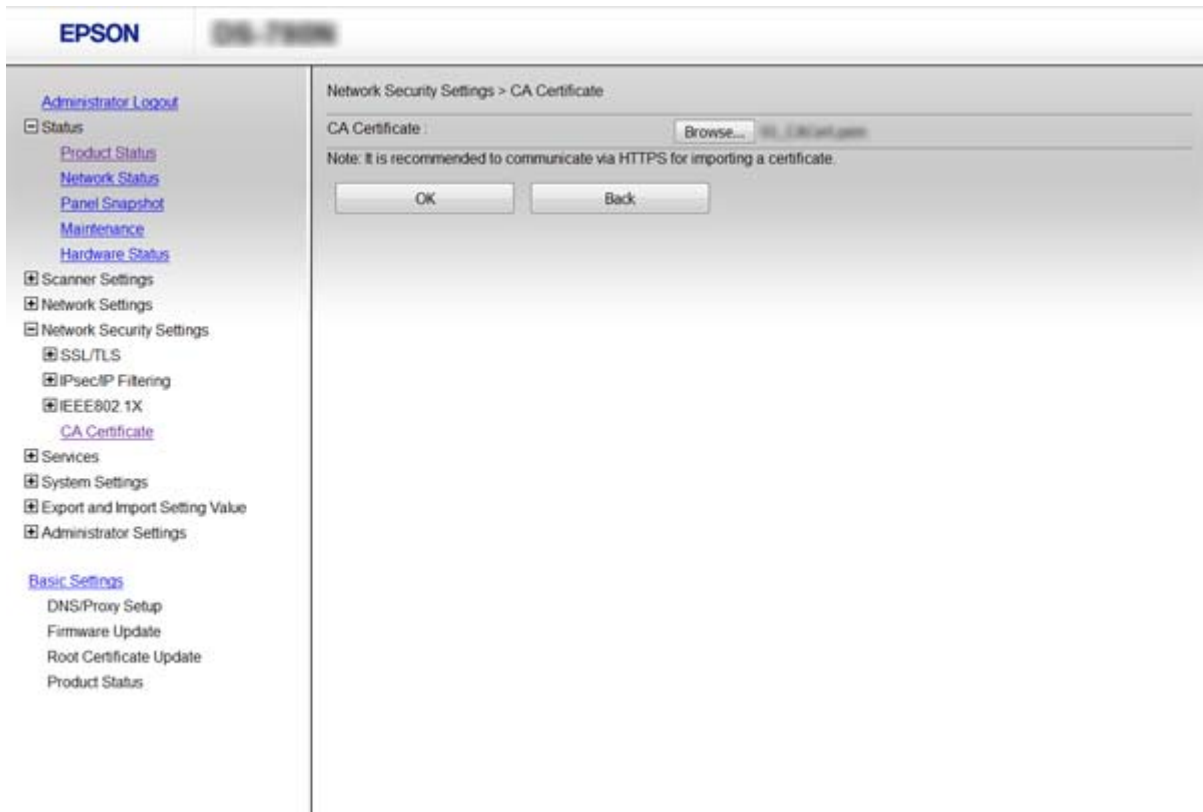
4. Click **OK**.

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

Related Information

Deleting a CA Certificate

You can delete the imported CA Certificate.

1. Access Web Config, and then select **Network Security Settings** > **CA Certificate**.

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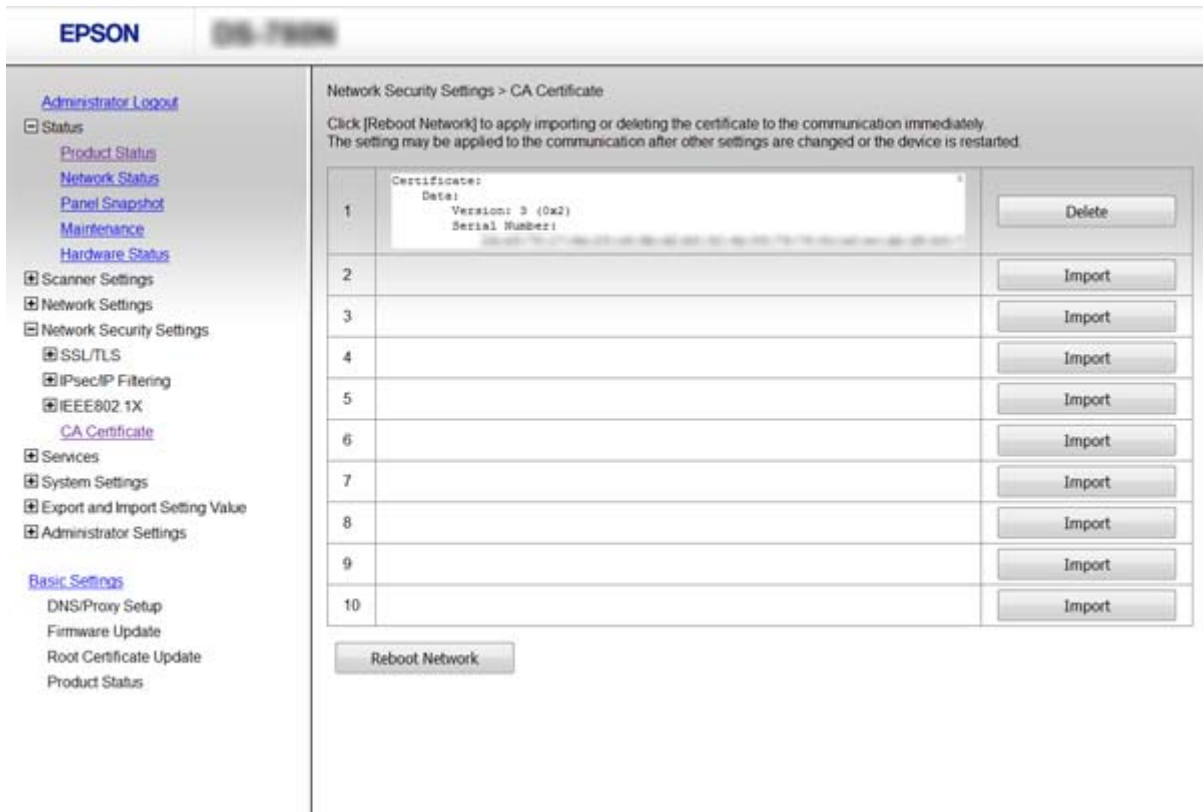
3. Confirm that you want to delete the certificate in the message displayed.

Related Information

➡ "Accessing Web Config" on page 23

Encrypted Communication Using IPsec/IP Filtering

About IPsec/IP Filtering

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

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

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

Configuring Default Policy

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

2. Enter a value for each item.

3. Click **Next**.

   A confirmation message is displayed.

4. Click **OK**.

   The scanner is updated.

Related Information

➡

➡

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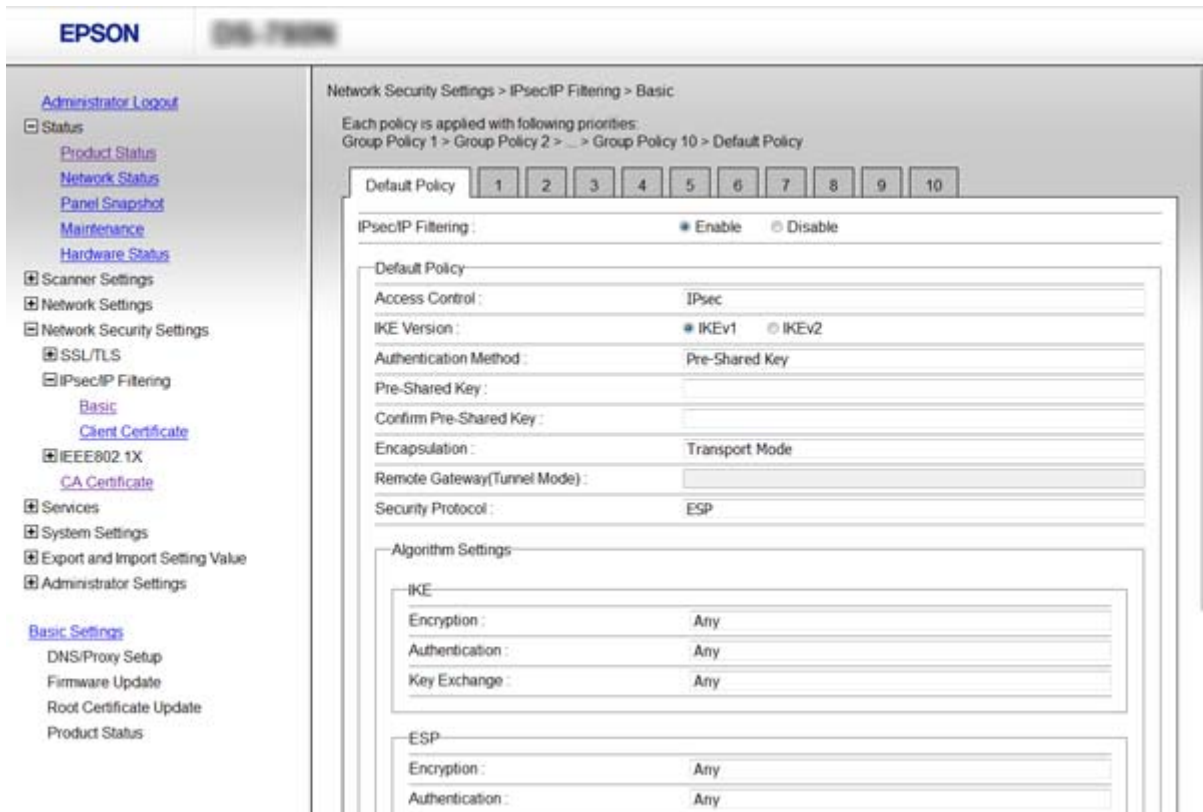
Items	Settings and Explanation
IPsec/IP Filtering	You can enable or disable an IPsec/IP Filtering feature.

Advanced Security Settings for Enterprise

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 scanner is connected to.	
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**.	
Local	Authentication Method	To select **Certificate**, you need to obtain and import a CA-signed certificate in advance.
	ID Type	Select the type of ID for the scanner.
	ID	Enter the scanner'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.

Advanced Security Settings for Enterprise

Items	Settings and Explanation	
Remote	Authentication Method	To select **Certificate**, you need to obtain and import a CA-signed certificate in advance.
	ID Type	Select the type of ID for the device that you want to authenticate.
	ID	Enter the scanner'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 scanner on the same LAN, select this. IP packets of layer 4 or later are encrypted.
	Tunnel Mode	If you use the scanner on the Internet-capable network such as IPsec-VPN, select this option. The header and data of the IP packets are encrypted.
Remote Gateway(Tunnel Mode)	If you select **Tunnel Mode** for **Encapsulation**, enter a gateway address between 1 and 39 characters.	
Security Protocol	**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.

Advanced Security Settings for Enterprise

Items	Settings and Explanation	
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**.

Related Information

➡

Configuring Group Policy

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

2. Click a numbered tab you want to configure.

3. Enter a value for each item.

4. Click **Next**.

   A confirmation message is displayed.

5. Click **OK**.

   The scanner 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.
Local Address (Scanner)	Select an IPv4 address or IPv6 address that matches your network environment. If an IP address is assigned automatically, you can select **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Enter a device's IP address to control access. The IP address must be 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.	

Advanced Security Settings for Enterprise

Items	Settings and Explanation	
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 scanner 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	Select the type of ID for the scanner.
	ID	Enter the scanner'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	Select the type of ID for the device that you want to authenticate.
	ID	Enter the scanner'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 scanner on the same LAN, select this. IP packets of layer 4 or later are encrypted.
	Tunnel Mode	If you use the scanner 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**.

Related Information

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

		Setting of Local Address (Scanner)		
		IPv4	IPv6[2]	Any addresses[3]
Setting of Remote Address(Host)	IPv4[1]	✓	–	✓
	IPv6[1][2]	–	✓	✓
	Blank	✓	✓	✓

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

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

Advanced Security Settings for Enterprise

*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 scanner from applications such as EpsonNet Config and the a scanner driver
SNMP	UDP	161	Any port	Acquiring and configuring of MIB from applications such as EpsonNet Config and a scanner driver
WSD	TCP	Any port	5357	Controlling WSD
WS-Discovery	UDP	3702	Any port	Searching for a scanner from WSD
Network Scan	TCP	1865	Any port	Forwarding scan data from Document Capture Pro
Network Push Scan Discovery	UDP	2968	Any port	Searching for a computer from the scanner.
Network Push Scan	TCP	Any port	2968	Acquiring job information of push scanning from Document Capture Pro or Document Capture
HTTP (Local)	TCP	80	Any port	HTTP(S) server (forwarding data of Web Config and WSD)
HTTPS (Local)	TCP	443	Any port	
HTTP (Remote)	TCP	Any port	80	HTTP(S) client (communicating between 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.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

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

Group Policy:

Advanced Security Settings for Enterprise

Do not configure.

Accepting scan using Epson Scan 2 and scanner settings

This example allows communications of scanning data and scanner 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**, **Network Scan**, **HTTP (Local)** and **HTTPS (Local)**.

Receiving access from a specified IP address only

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

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 scanner.

Configuring a Certificate for IPsec/IP Filtering

Configure the Client Certificate for IPsec/IP Filtering. If you want to configure the certification authority, go to **CA Certificate**.

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

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**.
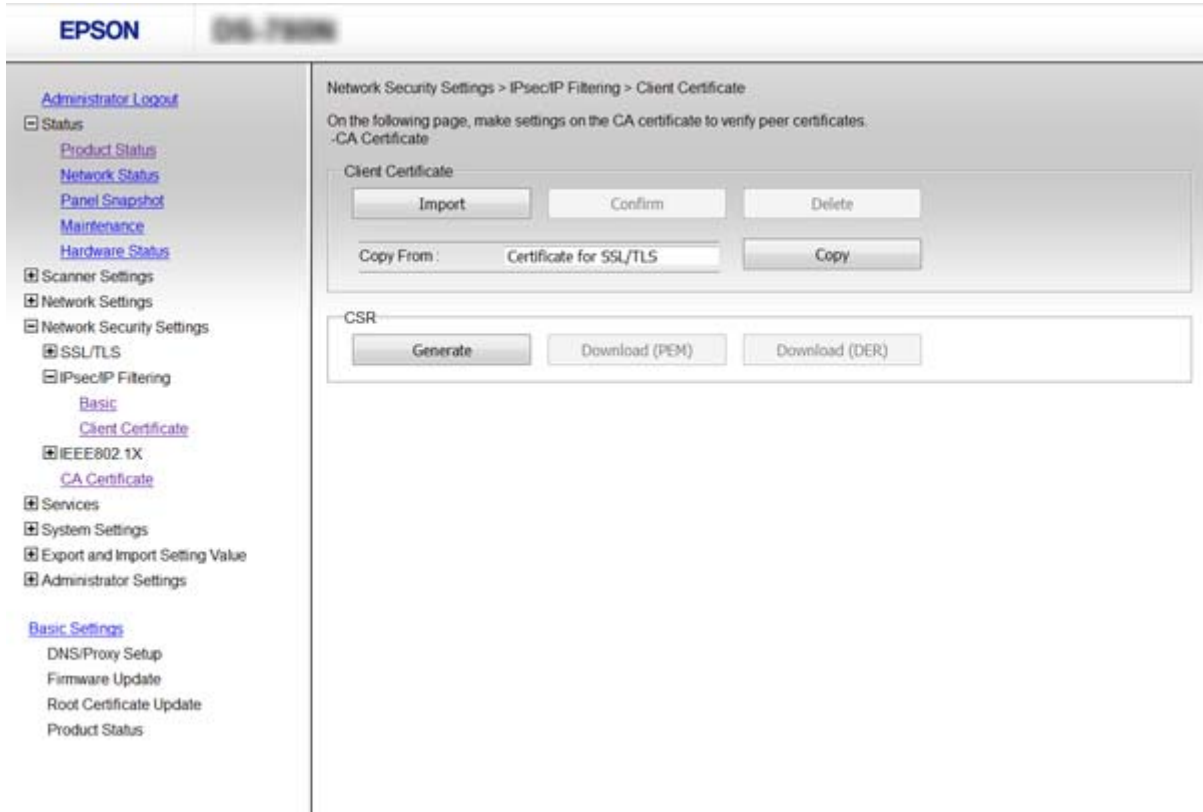
Related Information

Using SNMPv3 Protocol

About SNMPv3

SNMP is a protocol that carries out monitoring and control to collect the information of the devices that are connected to the network. SNMPv3 is the management security feature version that has been enhanced.

When using SNMPv3, state monitoring and setting changes of the SNMP communication (packet) can be authenticated and encrypted in order to protect the SNMP communication (packet) from network risks, such as wiretapping, impersonation, and tampering.

Configuring SNMPv3

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

Advanced Security Settings for Enterprise

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

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

3. Click **Next**.

   A confirmation message is displayed.

4. Click **OK**.

   The scanner is updated.

Related Information

➡ "Accessing Web Config" on page 23
➡ "SNMPv3 Setting Items" on page 83

SNMPv3 Setting Items
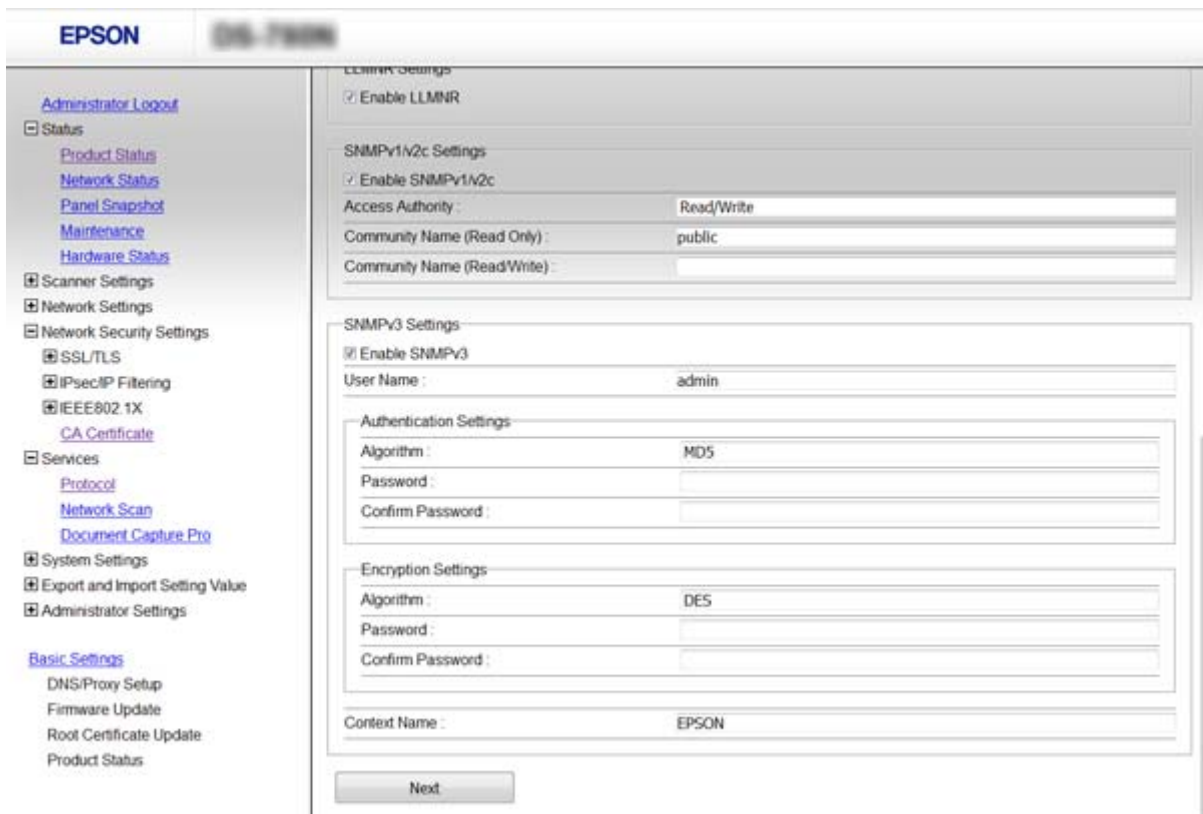
Items	Settings and Explanation
Enable SNMPv3	SNMPv3 is enabled when the box is checked.
User Name	Enter between 1 and 32 characters using 1 byte characters.
Authentication Settings	
Algorithm	Select an algorithm for an authentication.

Advanced Security Settings for Enterprise

Items	Settings and Explanation
Password	Enter between 8 and 32 characters in ASCII (0x20-0x7E).
Confirm Password	Enter the password you configured for confirmation.
Encryption Settings	
Algorithm	Select an algorithm for an encryption.
Password	Enter between 8 and 32 characters in ASCII (0x20-0x7E).
Confirm Password	Enter the password you configured for confirmation.
Context Name	Enter between 1 and 32 characters using 1 byte characters.

Related Information

➡

Connecting the Scanner to an IEEE802.1X Network

Configuring an IEEE802.1X Network

If the scanner supports IEEE802.1X, you can use the scanner on a network with authentication that is connected to a RADIUS server and a hub as an authenticator.
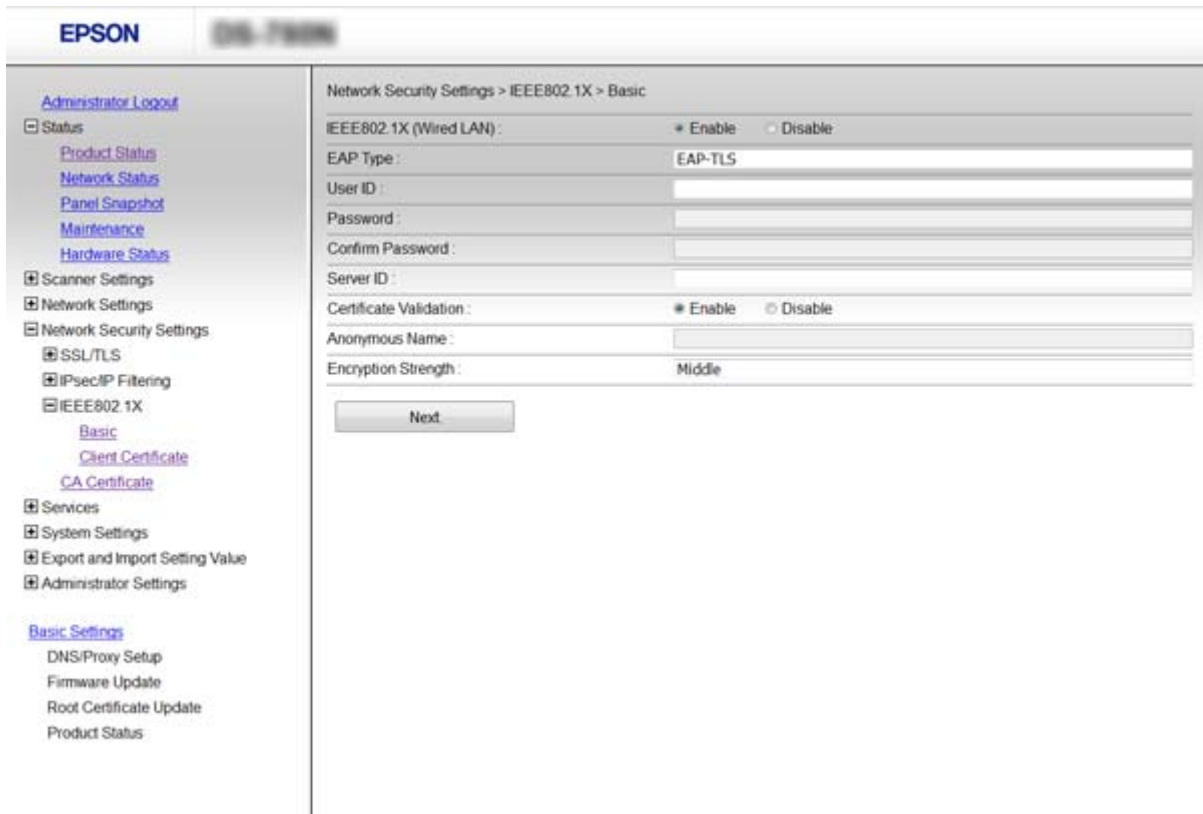
1. Access Web Config and select **Network Security Settings** > **IEEE802.1X** > **Basic**.

2. Enter a value for each item.

3. Click **Next**.

   A confirmation message is displayed.

4. Click **OK**.

   The scanner is updated.

Related Information

➡
➡
➡

Advanced Security Settings for Enterprise

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).	
EAP Type	Select an option for an authentication method between the scanner 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 scanner. 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**.	

Advanced Security Settings for Enterprise

Items	Settings and Explanation	
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. If you want to configure the certification authority certificate, go to **CA Certificate**.

1. Access Web Config and select **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.

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**.
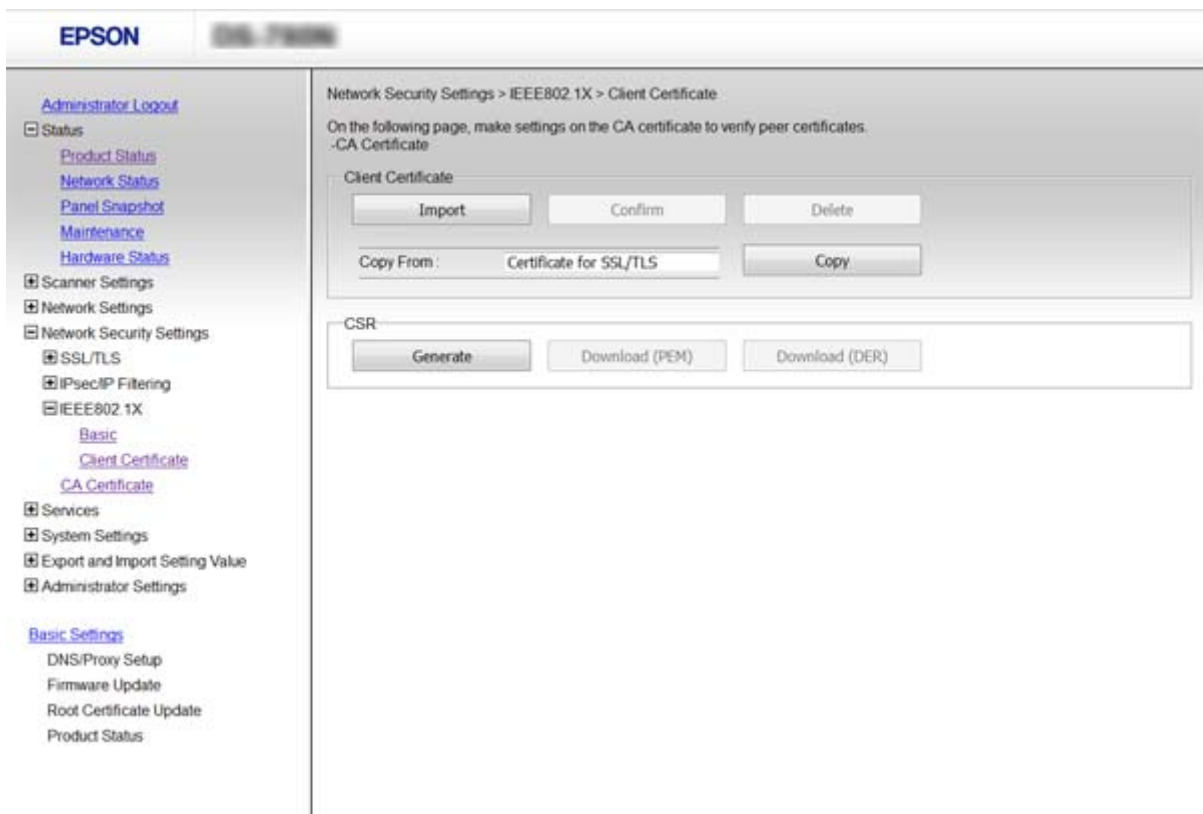
Related Information

➡

➡

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 scanner's control panel.

1. Tap **Settings** > **Network Settings**.

2. Tap **Change Settings**.

3. Tap the items that you want to disable.

   ❏ **IPsec/IP filtering**

   ❏ **IEEE802.1X**

4. When a completion message is displayed, tap **Proceed**.

Restoring the Security Function Using Web Config

For IEEE802.1X, devices may not be recognized on the network. In that case, disable the function using the scanner's control panel.

For IPsec/IP Filtering, you can disable the function if you can access the device from the computer.

Disabling IPsec/IP Filtering Using Web Config

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

2. Select **Disable** for **IPsec/IP Filtering** in **Default Policy**.

3. Click **Next**, and then clear **Enable this Group Policy** for all group policies.

4. Click **OK**.

Related Information

➡

Problems Using Network Security Features

Forgot a Pre–shared Key

Configure the key again using Web Config.

To change the key, access Web Config and select **Network Security Settings** > **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

➡

Cannot Communicate with IPsec Communication

Are you using an unsupported algorithm for the computer settings?

The scanner supports the following algorithms.

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

➡

Cannot Communicate Suddenly

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

Disable IPsec using the scanner's control panel.

Advanced Security Settings for Enterprise

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 scanner's Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) may not be found.

Use a static IP address.

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

Disable IPsec using the scanner'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 scanner's Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) may not be found.

Use a static IP address.

Related Information

➡ "Accessing Web Config" on page 23

➡ "Encrypted Communication Using IPsec/IP Filtering" on page 71

Cannot Connect After Configuring IPsec/IP Filtering

The set value may be incorrect.

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

Related Information

➡ "Encrypted Communication Using IPsec/IP Filtering" on page 71

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

The settings may be incorrect.

Disable IEEE802.1X from the scanner's control panel. Connect the scanner and a computer, and then configure IEEE802.1X again.

Related Information

➡ "Configuring an IEEE802.1X Network" on page 84

Problems on Using a Digital Certificate

Cannot Import a CA-signed Certificate

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

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

Advanced Security Settings for Enterprise

❏ 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 scanner after sending the CSR to a certificate authority?

Obtain the CA-signed certificate again with the CSR.

Is the CA-signed certificate more than 5KB?

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

Is the password for importing the certificate correct?

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

Related Information

➡ "Importing a CA-signed Certificate" on page 65

Cannot Update a Self-Signed Certificate

Has the Common Name been entered?

Common Name must be entered.

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

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

Is a comma or space included in the Common Name?

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

Related Information

➡ "Updating a Self-signed Certificate" on page 68

Cannot Create a CSR

Has the Common Name been entered?

The **Common Name** must be entered.

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

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

Is a comma or space included in the Common Name?

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

Advanced Security Settings for Enterprise

Related Information

➡ "Obtaining a CA-signed Certificate" on page 64

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.
Invalid date and time.	**Cause:** Date and time for the scanner have not been set. **What to do:** Set date and time using Web Config or EpsonNet Config.
Invalid password.	**Cause:** The password set for CA certificate and entered password do not match. **What to do:** Enter the correct password.

Advanced Security Settings for Enterprise

Messages	Cause/What to do
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 the product.	**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 scanner's date and time are set correctly.
Private key is required.	**Cause:** There is no paired private key with the certificate. **What to do:** ❏ If the certificate is the PEM/DER format and it is obtained from a CSR using a computer, specify the private key file. ❏ If the certificate is the PKCS#12 format and it is obtained from a CSR using a computer, create a file that contains the private key.
	Cause: You have re-imported the PEM/DER certificate obtained from a CSR using Web Config. **What to do:** If the certificate is the PEM/DER format and it is obtained from a CSR using Web Config, you can only import it once.

Advanced Security Settings for Enterprise

Messages	Cause/What to do
Setup failed.	**Cause:** Cannot finish the configuration because the communication between the scanner 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

Is there a backup file for the certificate?

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

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

Related Information

➡
➡