EPSON

DS-790WN

Administrator's Guide

Required Settings to Suit Your Purpose

Network Settings

Required Settings for Scanning

Basic Security Settings

Advanced Security Settings

Authentication Settings

NPD6726-05 EN

Copyright

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Seiko Epson Corporation. No patent liability is assumed with respect to the use of the information contained herein. Neither is any liability assumed for damages resulting from the use of the information herein. The information contained herein is designed only for use with this Epson product. Epson is not responsible for any use of this information as applied to other products.

Neither Seiko Epson Corporation nor its affiliates shall be liable to the purchaser of this product or third parties for damages, losses, costs, or expenses incurred by the purchaser or third parties as a result of accident, misuse, or abuse of this product or unauthorized modifications, repairs, or alterations to this product, or (excluding the U.S.) failure to strictly comply with Seiko Epson Corporation's operating and maintenance instructions.

Seiko Epson Corporation and its affiliates shall not be liable for any damages or problems arising from the use of any options or any consumable products other than those designated as Original Epson Products or Epson Approved Products by Seiko Epson Corporation.

Seiko Epson Corporation shall not be held liable for any damage resulting from electromagnetic interference that occurs from the use of any interface cables other than those designated as Epson Approved Products by Seiko Epson Corporation.

© 2022-2026 Seiko Epson Corporation

The contents of this manual and the specifications of this product are subject to change without notice.

Trademarks

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION and their logos are registered trademarks or trademarks of Seiko Epson.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa and PaSoRi are registered trademarks of the Sony Corporation.
- ❏ MIFARE is a registered trademark of the NXP Semiconductor Corporation.
- ❏ 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.

Contents

Copyright

Trademarks

Introduction

The Contents of This Document. 8
Using this Guide. 8
Marks and Symbols. 8
Descriptions Used in this Manual. 8
Operating System References. 9

Notes on the Administrator Password

Notes on the Administrator Password. 11
Initial Administrator Password. 11
Operations that Require the Administrator Password. 11
Changing the Administrator Password. 11
Resetting the Administrator Password. 11

Required Settings to Suit Your Purpose

Required Settings to Suit Your Purpose. 13

Network Settings

Connecting the Scanner to the Network. 16
Before Making a Network Connection. 16
Connecting to the Network from the Control Panel. 18
Adding or Replacing the Computer or Devices. . . . 22
Connecting to a Scanner that has been Connected to the Network. 22
Connecting a Smart Device and Scanner Directly (Wi-Fi Direct). 24
Resetting the Network Connection. 26
Checking the Network Connection Status. 28
Checking the Network Connection Status from the Control Panel. 28
Network Specifications. 29
Wi-Fi Specifications. 29
Ethernet Specifications. 31
Network Functions and IPv4/IPv6. 31
Security Protocol. 31
Network Ports for the Scanner. 32
Solving Problems. 33
Cannot connect to a Network. 33

Software for Setting Up the Scanner

Web Config. 37
Running Web Config on a Web Browser. 37
Running Web Config on Windows. 38
Epson Device Admin. 38
Configuration Template. 39

Required Settings for Scanning

Registering an Email Server. 44
Enabling SMTP AUTH in Exchange Online. . . . 45
Setting Up OAuth2.0 Authentication for the Email Server. 45
Checking a Mail Server Connection. 47
Setting a Shared Network Folder. 48
Creating the Shared Folder. 49
Making Contacts Available. 64
Contacts Configuration Comparison. 65
Registering a Destination to Contacts using Web Config. 65
Registering Destinations as a Group Using Web Config. 67
Backing Up and Importing Contacts. 68
Export and Bulk Registration of Contacts Using Tool. 69
Cooperation between the LDAP Server and Users. 70
Using Document Capture Pro Server. 74
Setting Server Mode. 74
Setting Up AirPrint. 74
Problems when Preparing Network Scanning. 75
Hints to Solving Problems. 75
Cannot Access Web Config. 75
Cannot Send Scanned Images to an Email when Using Microsoft Exchange Online. 76

Customizing the Control Panel Display

Registering Presets. 80
Menu Options of Presets. 81
Editing the Home Screen of the Control Panel. 82
Changing the Layout of the Home Screen. 82

Add Icon. 83
Remove Icon. 84
Move Icon. 85

Basic Security Settings

Introduction of Product Security Features. 88
Administrator Settings. 88
Configuring the Administrator Password. 88
Using Lock Setting for the Control Panel. 90
Logging in as an Administrator from the Control Panel. 93
Disabling the External Interface. 94
Monitoring a Remote Scanner. 95
Checking Information for a Remote Scanner. . . . 95
Receiving Email Notifications When Events Occur. 95
Solving Problems. 96
Forgot Your Administrator's Password. 96

Advanced Security Settings

Security Settings and Prevention of Danger. 98
Security Feature Settings. 99
Controlling Using Protocols. 99
Controlling protocols. 99
Protocols you can Enable or Disable. 99
Protocol Setting Items. 100
Using a Digital Certificate. 102
About Digital Certification. 102
Configuring a CA-signed Certificate. 102
Updating a Self-signed Certificate. 106
Configuring a CA Certificate. 106
SSL/TLS Communication with the Scanner. 107
Configuring Basic SSL/TLS Settings. 107
Configuring a Server Certificate for the Scanner 108
Encrypted Communication Using IPsec/IP Filtering. 108
About IPsec/IP Filtering. 108
Configuring Default Policy. 108
Configuring Group Policy. 112
Configuration Examples of IPsec/IP Filtering. . . 118
Configuring a Certificate for IPsec/IP Filtering. 119
Connecting the Scanner to an IEEE802.1X Network. 119
Configuring an IEEE802.1X Network. 119
Configuring a Certificate for IEEE802.1X. 121
Solving Problems for Advanced Security. 121
Restoring the Security Settings. 121
Problems Using Network Security Features. . . . 121
Problems on Using a Digital Certificate. 123

Authentication Settings

About Authentication Settings. 128
Available Functions for Authentication Settings 128
About Authentication Method. 129
Software for Setting Up. 131
Updating the Scanner's Firmware. 131
Connecting and Configuring an Authentication Device. 131
Card Reader Compatible List. 131
Connecting Authentication Device. 134
Authentication Device Settings. 135
Registering and Setting Information. 136
Setting Up. 136
Enabling Authentication. 137
Authentication Settings. 137
Registering User Settings. 139
Synchronizing with the LDAP Server. 145
Setting the Email Server. 148
Setting Scan to My Folder. 149
Customize One-touch Functions. 151
Job History Reports Using Epson Device Admin. . 151
Items that can be Included in the Report. 151
Logging in as an Administrator from the Control Panel. 151
Disabling Authentication Settings. 152
Deleting Authentication Settings Information (Restore Default Settings). 152
Solving Problems. 153
Cannot Read the Authentication Card. 153

Maintenance

Cleaning Outside the Scanner. 155
Cleaning Inside the Scanner. 155
Replacing the Roller Assembly Kit. 160
Roller Assembly Kit Codes. 165
Resetting the Number of Scans. 165
Energy Saving. 165
Transporting the Scanner. 166
Backing Up the Settings. 167
Export the settings. 167
Import the settings. 168
Restore Default Settings. 168
Updating Applications and Firmware. 169

Updating the Scanner's Firmware using the Control Panel. 169
Updating Firmware Using Web Config. 170
Updating Firmware without Connecting to the Internet. 170

Introduction

The Contents of This Document. 8

Using this Guide. 8

The Contents of This Document

This document provides the following information for scanner administrators.

❏ Network settings

❏ Preparing the scanning function

❏ Enable and manage security settings

❏ Enable and manage Authentication Settings

❏ Perform daily maintenance

For the standard methods of using the scanner, see the *User's Guide*.

Note:
This document explains the Authentication Settings that provide standalone authentication without having to use an authentication server. In addition to the Authentication Settings introduced in this manual, you can also build an authentication system using an authentication server. To build a system, use Document Capture Pro Server Authentication Edition (the abbreviated name is Document Capture Pro Server AE).

For further information, contact your local Epson office.

Using this Guide

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:
Provides complementary and reference information.

Related Information

➡ Links to related sections.

Descriptions Used in this Manual

❏ Screenshots for the applications are from Windows 10 or macOS High Sierra. The content displayed on the screens varies depending on the model and situation.

❏ Illustrations used in this manual are for reference only. Although they may differ slightly from the actual product, the operating methods are the same.

Operating System References

Windows

In this manual, terms such as "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012", and "Windows Server 2008 R2" refer to the following operating systems. Additionally, "Windows" is used to refer to all versions and "Windows Server" is used to refer to "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012", and "Windows Server 2008 R2".

- ❏ Microsoft® Windows® 10 operating system
- ❏ Microsoft® Windows® 8.1 operating system
- ❏ Microsoft® Windows® 8 operating system
- ❏ Microsoft® Windows® 7 operating system
- ❏ Microsoft® Windows Server® 2019 operating system
- ❏ 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

Mac OS

In this manual, "Mac OS" is used to refer to macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan, and OS X Yosemite.

Notes on the Administrator Password

Notes on the Administrator Password. 11

Initial Administrator Password. 11

Operations that Require the Administrator Password. 11

Changing the Administrator Password. 11

Resetting the Administrator Password. 11

Notes on the Administrator Password

This device allows you to set an administrator password to prevent unauthorized third parties from accessing or changing the device settings or the network settings stored in the device when it is connected to a network.

If you set an administrator password, you need to enter the password when changing settings in configuration software such as Web Config.

The initial administrator password is set on the scanner, but you can change it to any password.

Initial Administrator Password

The initial administrator password varies depending on the label attached to the product. If there is a "PASSWORD" label attached to the back, the password is the 8-digit number shown on the label. If there is no "PASSWORD" label attached, the password is the serial number on the label attached to the back of the product.

We recommend changing the initial administrator password from the default setting.

Note:
No user name is set as default.

Operations that Require the Administrator Password

If you are prompted, enter the administrator password during the following operations:

- ❏ When logging on to the advanced settings for Web Config
- ❏ When operating a menu on the control panel that has been locked by the administrator
- ❏ When changing the device settings in the application
- ❏ When updating the firmware for the device
- ❏ When changing or resetting the administrator password

Changing the Administrator Password

You can change from the product's control panel or in Web Config.

When changing the password, the new password must be 8 to 20 characters long and only contain single-byte alphanumeric characters and symbols.

Resetting the Administrator Password

You can reset the administrator password to the initial setting from the product's control panel or in Web Config.

If you have forgotten the password and cannot reset it to the default settings, the product needs to be repaired. Contact your local dealer.

Required Settings to Suit Your Purpose

Required Settings to Suit Your Purpose. 13

Required Settings to Suit Your Purpose

See the following to make the necessary settings to suit your purpose.

Connecting the Scanner to the Network

Purpose	Required Settings
I want to connect the scanner to the network.	Set up your scanner for network scanning. "Connecting the Scanner to the Network" on page 16
I want to connect the scanner to a new computer.	Set the network settings for your scanner on the new computer. "Adding or Replacing the Computer or Devices" on page 22

Settings for Scanning

Purpose	Required Settings
I want to send scanned images by email. (Scan to Email)	1. Setup the email server you want to link. "Registering an Email Server" on page 44 2. Register the recipient's email address in **Contacts** (optional). By registering the email address you do not have to enter it every time you want to send something, you can just select it from your Contacts. "Making Contacts Available" on page 64
I want to save scanned images to a folder on the network. (Scan to Network Folder/FTP)	1. Create a folder on the network where you want to save the images. "Setting a Shared Network Folder" on page 48 2. Register the path to the folder in **Contacts** (optional). By registering the folder path you do not have to enter it every time you want to send something, you can just select it from your Contacts. "Making Contacts Available" on page 64
I want to save scanned images to a cloud service. (Scan to Cloud)	Setup Epson Connect. See the Epson Connect portal website for details on setting up. When setting up, you need a user account for the online storage service you want to link to. https://www.epsonconnect.com/ http://www.epsonconnect.eu (Europe only)

Customizing the Control Panel Display

Purpose	Required Settings
I want to change the items displayed on the scanner's control panel.	Set **Presets** or **Edit Home**. You can register your favorite scanning settings to the control panel and edit the items displayed. "Customizing the Control Panel Display" on page 79

Setting Basic Security Functions

Purpose	Required Settings
I want to prevent anyone other than the administrator from changing the scanner settings.	Set an administrator password for the scanner. "Administrator Settings" on page 88
I want to disable the use of scanners with USB connections.	Disable the external interface. "Disabling the External Interface" on page 94

Setting Advanced Security Functions

Purpose	Required Settings
I want to control which protocols to use.	Enable or disable the protocols. "Controlling Using Protocols" on page 99
I want to encrypt the communication path.	1. Setup your digital certificate. "Using a Digital Certificate" on page 102 2. Setup SSL/TLS communication. "SSL/TLS Communication with the Scanner" on page 107
I want to use encrypted communication (IPsec). I want to be able to use the software only from a specific computer (IP filtering).	Setup policies for filtering traffic. "Encrypted Communication Using IPsec/IP Filtering" on page 108
I want to use a scanner in an IEEE802.1X network.	Setup IEEE802.1X for the scanner. "Connecting the Scanner to an IEEE802.1X Network" on page 119

Setting Functions to be Authenticated by the Scanner

Purpose	Required Settings
I want to enable Authentication Settings.	See the following for more information on the available Authentication Settings and Authentication Method. "About Authentication Settings" on page 128 "About Authentication Method" on page 129

Using a Server's Authentication System

With Document Capture Pro Server Authentication Edition (abbreviated to Document Capture Pro Server AE), you can build an authentication system that uses a server for authentication.

For further information, contact your local Epson office.

Network Settings

Connecting the Scanner to the Network. 16

Adding or Replacing the Computer or Devices. 22

Checking the Network Connection Status. 28

Network Specifications. 29

Solving Problems. 33

Connecting the Scanner to the Network

This section explains how to connect the scanner to the network using the scanner's control panel.

Note:
If your scanner and computer are in the same segment, you can also connect using the installer.

❏ *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 models that come with a software disc and users with Windows computers with disc drives.)*

Insert the software disc into the computer, and then follow the on-screen instructions.

Before Making a Network Connection

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

Gathering Information on the Connection Setting

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

Divisions	Items	Note
Device connection method	❏ Ethernet ❏ Wi-Fi	Decide how to connect the scanner to the network. For Wired LAN, connects to the LAN switch. For Wi-Fi, connects to the network (SSID) of the access point.
LAN connection information	❏ IP address ❏ Subnet mask ❏ Default gateway	Decide the IP address to assign to the scanner. When you assign the IP address statically, all values are required. When you assign the IP address dynamically using the DHCP function, this information is not required because it is set automatically.
Wi-Fi connection information	❏ SSID ❏ Password	These are the SSID (network name) and the password of the access point that the scanner connects to. If MAC address filtering has been set, register the MAC address of the scanner in advance to register the scanner. See the following for the supported standards. "Network Specifications" on page 29
DNS server information	❏ IP address for primary DNS ❏ IP address for secondary DNS	These are required when specifying DNS servers. The secondary DNS is set when the system has a redundant configuration and there is a secondary DNS server. If you are in a small organization and do not set the DNS server, set the IP address of the router.

Divisions	Items	Note
Proxy server information	❏ Proxy server name	Set this when your network environment uses the proxy server to access the internet from the intranet, and you use the function that the scanner directly accesses to the internet. For the following functions, the scanner directly connects to the internet . ❏ Epson Connect Services ❏ Cloud services of other companies ❏ Firmware updating ❏ Sending scanned images to SharePoint(WebDAV)
Port number information	❏ Port number to release	Check the port number used by the scanner and computer, then release the port that is blocked by a firewall, if necessary. See the following for the port number used by the scanner. "Network Ports for the Scanner" on page 32

IP Address Assignment

These are the following types of IP address assignment.

Static IP address:

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

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

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

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

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

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

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

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

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

DNS Server and Proxy Server

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

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

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

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

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

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

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

The proxy server is placed at the gateway between the network and the Internet, and it communicates to the computer, 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.

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

Connecting to the Network from the Control Panel

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

Assigning the IP Address

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

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

1. Turn on the scanner.
2. Select **Settings** on the home screen on the scanner's control panel.
3. Select **Network Settings** > **Advanced** > **TCP/IP**.
4. Select **Manual** for **Obtain IP Address**.

   When you set the IP address automatically by using the DHCP function of router, select **Auto**. In that case, the **IP Address**, **Subnet Mask**, and **Default Gateway** on step 5 to 6 are also set automatically, so go to step 7.
5. Enter the IP address.

   Focus moves to the forward segment or the back segment separated by a period if you select ◀ and ▶.

   Confirm the value reflected on the previous screen.
6. Set up the **Subnet Mask** and **Default Gateway**.

   Confirm the value reflected on the previous screen.

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

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

   Confirm the value reflected on the previous screen.

   Note:
   *When you select **Auto** for the IP address assignment settings, you can select the DNS server settings from **Manual** or **Auto**. If you cannot obtain the DNS server address automatically, select **Manual** and enter the DNS server address. Then, enter the secondary DNS server address directly. If you select **Auto**, go to step 9.*

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

   Confirm the value reflected on the previous screen.

9. Tap **Start Setup**.

Setting the Proxy Server

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

- ❏ The proxy server is built for Internet connection.
- ❏ When using a function in which a scanner directly connects to the Internet, such as Epson Connect service or another company's cloud services.

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

   When configuring settings after IP address setting, the **Advanced** screen is displayed. Go to step 3.

2. Select **Network Settings** > **Advanced**.

3. Select **Proxy Server**.

4. Select **Use** for **Proxy Server Settings**.

5. Enter the address for the proxy server in IPv4 or FQDN format.

6. Enter the port number for the proxy server.

7. Tap **Start Setup**.

Connecting to Ethernet

Connect the scanner to the network by using a LAN cable, and then check the connection.

1. Connect the scanner and hub (LAN switch) with a LAN cable.

2. Select on the home screen.

3. Select **Router**.

4. Make sure that the Connection and IP Address settings are correct.

5. Tap **Close**.

Connecting to the Wireless LAN (Wi-Fi)

You can connect the scanner to the wireless LAN (Wi-Fi) in several ways. Choose the connection method that matches the environment and conditions that you are using.

If you know the information for the wireless router such as SSID and password, you can configure settings manually.

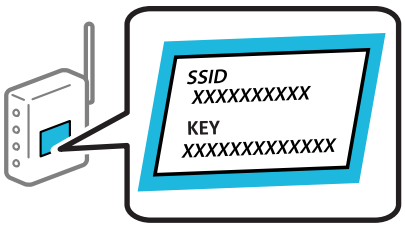
If the wireless router supports WPS, you can configure settings by using push button setup.

After connecting the scanner to the network, connect to the scanner from the device that you want to use (computer, smart device, and tablet.)

Making Wi-Fi Settings by Entering the SSID and Password

You can set up a Wi-Fi network by entering the information necessary to connect to a wireless router from the scanner's control panel. To set up using this method, you need the SSID and password for a wireless router.

Note:
If you are using a wireless router with its default settings, the SSID and password are on the label. If you do not know the SSID and password, contact the person who set up the wireless router, or see the documentation provided with the wireless router.



1. Tap on the home screen.

2. Select **Router**.

3. Tap **Start Setup**.

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

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

5. Follow the on-screen instructions to select the SSID, enter the password for the wireless router, and start setup.

   If you want to check the network connection status for the scanner after setup is complete, see the related information link below for details.

Note:

- ❏ *If you do not know the SSID, check if it is written on the label of the wireless router. If you are using the wireless router with its default settings, use the SSID written on the label. If you cannot find any information, see the documentation provided with the wireless router.*
- ❏ *The password is case-sensitive.*
- ❏ *If you do not know the password, check if the information is written on the label of the wireless router. On the label, the password may be written "Network Key", "Wireless Password", and so on. If you are using the wireless router with its default settings, use the password written on the label.*

Related Information

➡ "Checking the Network Connection Status" on page 28

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

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

- ❏ The wireless router is compatible with WPS (Wi-Fi Protected Setup).
- ❏ The current Wi-Fi connection was established by pressing a button on the wireless router.

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

1. Tap on the home screen.
2. Select **Router**.
3. Tap **Start Setup**.

   If the network connection is already set up, the connection details are displayed. Tap **Change to Wi-Fi connection.** or **Change Settings** to change the settings.
4. Select **Push Button Setup(WPS)**.
5. Follow the on-screen instructions.

   If you want to check the network connection status for the scanner after setup is complete, see the related information link below for details.

   Note:
   If connection fails, restart the wireless router, move it closer to the scanner, and try again.

Related Information

➡ "Checking the Network Connection Status" on page 28

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

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

1. Tap on the home screen.
2. Select **Router**.
3. Tap **Start Setup**.

   If the network connection is already set up, the connection details are displayed. Tap **Change to Wi-Fi connection.** or **Change Settings** to change the settings.
4. Select **Others** > **PIN Code Setup(WPS)**
5. Follow the on-screen instructions.

   If you want to check the network connection status for the scanner after setup is complete, see the related information link below for details.

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

Related Information

➡ "Checking the Network Connection Status" on page 28

Adding or Replacing the Computer or Devices

Connecting to a Scanner that has been Connected to the Network

When the scanner has already been connected to the network, you can connect a computer or a smart device to the scanner over the network.

Using a Network Scanner from a Second Computer

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.

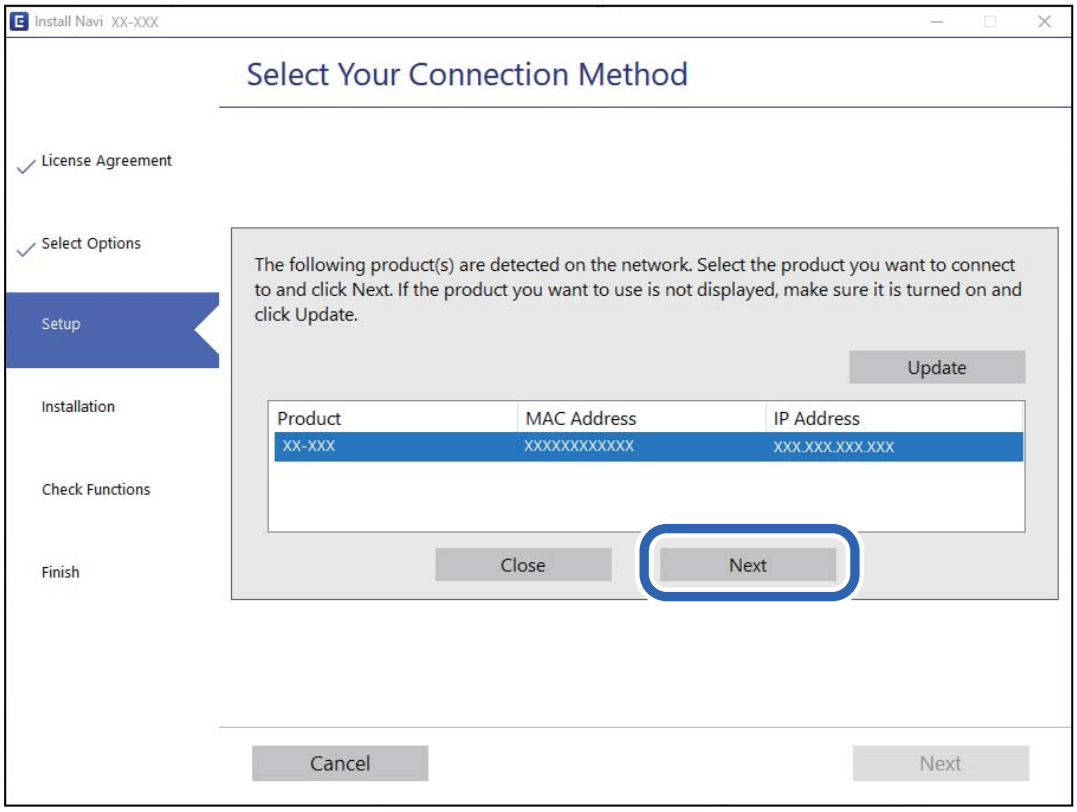
http://epson.sn

❏ Setting up using the software disc (only for the models that come with a software disc and users with Windows computers with disc drives.)

Insert the software disc into the computer, and then follow the on-screen instructions.

Selecting the Scanner

Follow the on-screen instructions until the following screen is displayed, select the scanner name you want to connect to, and then click **Next**.



Follow the on-screen instructions.

Using a Network Scanner from a Smart Device

You can connect a smart device to the scanner using one of the following methods.

Connecting over a wireless router

Connect the smart device to the same Wi-Fi network (SSID) as the scanner.

See the following for more details.

"Making Settings for Connecting to the Smart Device" on page 27

Connecting by Wi-Fi Direct

Connect the smart device to the scanner directly without a wireless router.

See the following for more details.

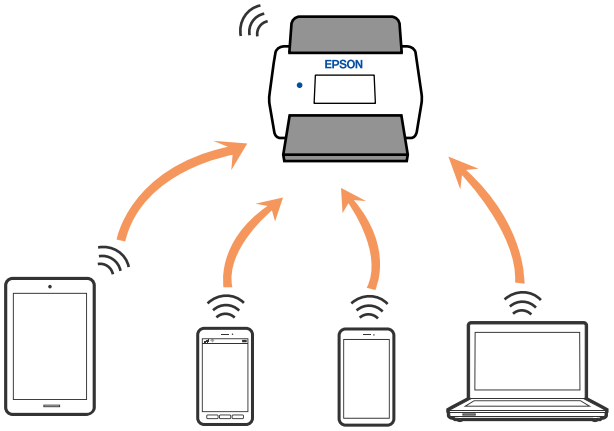
"Connecting a Smart Device and Scanner Directly (Wi-Fi Direct)" on page 24

Connecting a Smart Device and Scanner Directly (Wi-Fi Direct)

Wi-Fi Direct (Simple AP) allows you to connect a smart device directly to the scanner without a wireless router and scan from the smart device.

About Wi-Fi Direct

Use this connection method when you are not using Wi-Fi at home or at the office, or when you want to connect the scanner and the computer or smart device directly. In this mode, the scanner acts as a wireless router and you can connect up to 8 devices to the scanner without having to use a standard wireless router. However, devices directly connected to the scanner cannot communicate with each other through the scanner.



The scanner can be connected by Wi-Fi or Ethernet, and Wi-Fi Direct (Simple AP) connection simultaneously. However, if you start a network connection in Wi-Fi Direct (Simple AP) connection when the scanner is connected by Wi-Fi, the Wi-Fi is temporarily disconnected.

Connecting to a Smart Device using Wi-Fi Direct

This method allows you to connect the scanner directly to smart devices without a wireless router.

1. Select on the home screen.
2. Select **Wi-Fi Direct**.
3. Select **Start Setup**.
4. Start Epson Smart Panel on your smart device.
5. Follow the instructions displayed on the Epson Smart Panel to connect to your scanner.

   When your smart device is connected to the scanner, go to the next step.
6. On the scanner's control panel, select **Complete**.

Disconnecting Wi-Fi Direct (Simple AP) Connection

There are two methods available to disable a Wi-Fi Direct (Simple AP) connection; you can disable all connections by using the scanner's control panel, or disable each connection from the computer or the smart device.

When you want to disable all connections, select > **Wi-Fi Direct** > **Start Setup** > **Change** > **Disable Wi-Fi Direct**.

Important:

When Wi-Fi Direct (Simple AP) connection disabled, all computers and smart devices connected to the scanner in Wi-Fi Direct (Simple AP) connection are disconnected.

Note:

If you want to disconnect a specific device, disconnect from the device instead of the scanner. Use one of the following methods to disconnect the Wi-Fi Direct (Simple AP) connection from the device.

- ❏ *Disconnect the Wi-Fi connection to the scanner's network name (SSID).*
- ❏ *Connect to another network name (SSID).*

Changing the Wi-Fi Direct (Simple AP) Settings Such as the SSID

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

Change Network Name

Change the Wi-Fi Direct (simple AP) network name (SSID) used for connecting to the scanner to your arbitrary name. You can set the network name (SSID) in ASCII characters that is displayed on the software keyboard on the control panel. You can enter up to 22 characters.

When changing the network name (SSID), all connected devices are disconnected. Use the new network name (SSID) if you want to re-connect the device.

Change Password

Change the Wi-Fi Direct (simple AP) password for connecting to the scanner to your arbitrary value. You can set the password in ASCII characters that is displayed on the software keyboard on the control panel. You can enter 8 to 22 characters.

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

Change Frequency Range

Change the frequency range of Wi-Fi Direct used for connecting to the scanner. You can select 2.4 GHz or 5 GHz.

When changing the frequency range, all connected devices are disconnected. Re-connect the device.

Note that you cannot re-connect from devices that do not support 5 GHz frequency range when changing to 5 GHz.

Depending on the region, this setting may not be displayed.

Disable Wi-Fi Direct

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

Restore Default Settings

Restore all Wi-Fi Direct (simple AP) settings to their defaults.

The Wi-Fi Direct (simple AP) connection information of the smart device saved to the scanner is deleted.

Note:
*You can also set up from the **Network** tab > **Wi-Fi Direct** on Web Config for the following settings.*

- ❏ *Enabling or disabling Wi-Fi Direct (simple AP)*
- ❏ *Changing network name (SSID)*
- ❏ *Changing password*
- ❏ *Changing the frequency range*
  Depending on the region, this setting may not be displayed.
- ❏ *Restoring the Wi-Fi Direct (simple AP) settings*

Resetting the Network Connection

This section explains how to configure the network connection settings and change the connection method when replacing the wireless router or the computer.

When Replacing the Wireless Router

When you replace the wireless router, configure settings for the connection between the computer or the smart device and the scanner.

You need to configure these settings if you change your Internet service provider or make other related changes.

Making Settings for Connecting to the Computer

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 Windows 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. On the **Select Your Operation** screen, select **Set up Scanner connection again (for new network router or changing USB to network, etc.)** , and then click **Next**.

Follow the on-screen instructions to finish setup.

If you cannot connect, see the following to try to solve the problem.

"Cannot connect to a Network" on page 33

Making Settings for Connecting to the Smart Device

You can use the scanner from a smart device when you connect the scanner to the same Wi-Fi network (SSID) as the smart device. To use the scanner from a smart device, access the following website, and then enter the product name. Go to **Setup**, and then start setting up.

http://epson.sn

Access to the website from the smart device that you want to connect to the scanner.

When Changing the Computer

When changing the computer, configure connection settings between the computer and the scanner.

Making Settings for Connecting to the Computer

We recommend using the installer to connect the scanner to a computer. You can run the installer using the following method.

❏ 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 Windows computers with disc drives.)

Insert the software disc into the computer, and then follow the on-screen instructions.

Follow the on-screen instructions.

Changing the Connection Method to the Computer

This section explains how to change the connection method when the computer and the scanner have been connected.

Changing the Network Connection from Ethernet to Wi-Fi

Change the Ethernet connection to Wi-Fi connection from the scanner's control panel. The changing connection method is basically the same as the Wi-Fi connection settings.

Related Information

➡ "Connecting to the Wireless LAN (Wi-Fi)" on page 20

Changing the Network Connection from Wi-Fi to Ethernet

Follow the steps below to change from a Wi-Fi connection to an Ethernet connection.

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

2. Select **Network Settings** > **Wired LAN Setup**.
3. Set each item.

Changing from USB to a Network Connection

Using the installer and re-set up in a different connection method.

❏ 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 Windows computers with disc drives.)

Insert the software disc into the computer, and then follow the on-screen instructions.

Selecting Change the Connection Methods

Follow the on-screen instructions. On the **Select Your Operation** screen, select **Set up Scanner connection again (for new network router or changing USB to network, etc.)** , and then click **Next**.

Select the network connection that you want to use, **Connect via wireless network (Wi-Fi)** or **Connect via wired LAN (Ethernet)**, and then click **Next**.

Follow the on-screen instructions to finish setup.

Checking the Network Connection Status

You can check the network connection status in the following way.

Checking the Network Connection Status from the Control Panel

You can check the network connection status using the network icon or the network information on the scanner's control panel.

Checking the Network Connection Status using the Network Icon

You can check the network connection status and strength of the radio wave using the network icon on the scanner's home screen.

	Displays the network connection status. Select the icon to check and change the current settings. This is the shortcut for the following menu. **Settings** > **Network Settings** > **Wi-Fi Setup**	
		The scanner is not connected to a wireless (Wi-Fi) network.
		The scanner is searching for an SSID, the IP address has not been set, or the scanner is having a problem with a wireless (Wi-Fi) network.
		The scanner is connected to a wireless (Wi-Fi) network. The number of bars indicates the signal strength of the connection. The more bars there are, the stronger the connection.
		The scanner is not connected to a wireless (Wi-Fi) network in Wi-Fi Direct (Simple AP) mode.
		The scanner is connected to a wireless (Wi-Fi) network in Wi-Fi Direct (Simple AP) mode.
		The scanner is not connected to a wired (Ethernet) network or network connection settings have not been set.
		The scanner is connected to a wired (Ethernet) network.

Displaying Detailed Network Information on the Control Panel

When your scanner is connected to the network, you can also view other network-related information by selecting the network menus you want to check.

1. Select **Settings** on the home screen.
2. Select **Network Settings** > **Network Status**.
3. To check the information, select the menus that you want to check.
   - ❏ Wired LAN/Wi-Fi Status

     Displays the network information (device name, connection, signal strength, and more) for Ethernet or Wi-Fi connections.
   - ❏ Wi-Fi Direct Status

     Displays whether Wi-Fi Direct is enabled or disabled, and the SSID, password and more for Wi-Fi Direct connections.
   - ❏ Email Server Status

     Displays the network information for email server.

Network Specifications

Wi-Fi Specifications

See the following table for Wi-Fi specifications.

Countries or regions except for those listed below	Table A
Australia New Zealand Taiwan South Korea	Table B

Table A

Standards	IEEE802.11b/g/n*1
Frequency Range	2.4 GHz
Maximum radio-frequency power transmitted	2400-2483.5 MHz: 20 dBm (EIRP)
Channels	1/2/3/4/5/6/7/8/9/10/11/12/13
Connection Modes	Infrastructure, Wi-Fi Direct (Simple AP)*2*3
Security Protocols*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Only available for the HT20

*2 Not supported for IEEE 802.11b

*3 Infrastructure and Wi-Fi Direct modes or an Ethernet connection can be used simultaneously.

*4 Wi-Fi Direct supports WPA2-PSK (AES) only.

*5 Complies with WPA2 standards with support for WPA/WPA2 Personal.

Table B

Standards	IEEE802.11a/b/g/n*1/ac		
Frequency Ranges	IEEE802.11b/g/n: 2.4 GHz, IEEE802.11a/n/ac: 5 GHz		
Channels	Wi-Fi	2.4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2.4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48) W58 (149/153/157/161/165)
Connection Modes	Infrastructure, Wi-Fi Direct (Simple AP) *4*5		
Security Protocols*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Only available for the HT20

*2 Not available in Taiwan

*3 The availability of these channels and use of the product outdoors over these channels varies by location. For more information, see http://support.epson.net/wifi5ghz/

*4 Not supported for IEEE 802.11b

*5 Infrastructure and Wi-Fi Direct modes or an Ethernet connection can be used simultaneously.

*6 Wi-Fi Direct only supports WPA2-PSK (AES) .

*7 Complies with WPA2 standards with support for WPA/WPA2 Personal.

Ethernet Specifications

Standards	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Energy Efficient Ethernet)*2
Communication Mode	Auto, 10 Mbps Full duplex, 10 Mbps Half duplex, 100 Mbps Full duplex, 100 Mbps Half duplex
Connector	RJ-45

*1 Use a category 5e or higher STP (Shielded twisted pair) cable to prevent risk of radio interference.

*2 The connected device should comply with IEEE802.3az standards.

Network Functions and IPv4/IPv6

Functions	Supported
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4, IPv6

Security Protocol

IEEE802.1X*	
IPsec/IP Filtering	
SSL/TLS	HTTPS Server/Client
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* You need to use a connection device that complies with IEEE802.1X.

Network Ports for the Scanner

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

When the Sender (Client) is the Scanner

Use	Destination (Server)	Protocol	Port Number
File sending (When scan to network folder is used from the scanner)	FTP/FTPS server	FTP/FTPS (TCP)	20
			21
	File server	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	WebDAV server	Protocol HTTP(TCP)	80
		Protocol HTTPS(TCP)	443
Email sending (When scan to mail is used from the scanner)	SMTP server	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP before SMTP connection (When scan to mail is used from the scanner)	POP server	POP3 (TCP)	110
When Epson Connect is used	Epson Connect Server	HTTPS	443
		XMPP	5222
Collecting user information (Use the contacts from the scanner)	LDAP server	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
User authentication when collecting user information (When using the contacts from the scanner) User authentication when using the scan to network folder (SMB) from the scanner	KDC server	Kerberos	88
Control WSD	Client computer	WSD (TCP)	5357
Search the computer when push scanning to an application	Client computer	Network Push Scan Discovery	2968

When the Sender (Client) is the Client Computer

Use	Destination (Server)	Protocol	Port Number
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 an application	Scanner	Network Scan (TCP)	1865
Collecting the job information when push scanning from an application	Scanner	Network Push Scan	2968
Web Config	Scanner	HTTP(TCP)	80
		HTTPS(TCP)	443

Solving Problems

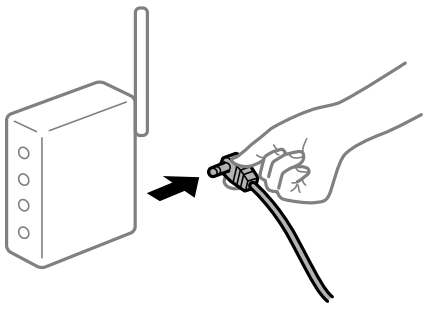
Cannot connect to a Network

The problem could be one of the following issues.

Something is wrong with the network devices for Wi-Fi connection.

Solutions

Turn off the devices you want to connect to the network. Wait for about 10 seconds, and then turn on the devices in the following order; wireless router, computer or smart device, and then scanner. Move the scanner and computer or smart device closer to the wireless router to help with radio wave communication, and then try to configure network settings again.



Devices cannot receive signals from the wireless router because they are too far apart.

Solutions

After moving the computer or the smart devices and the scanner closer to the wireless router, turn off the wireless router, and then turn it back on.

When changing the wireless router, the settings do not match the new router.

Solutions

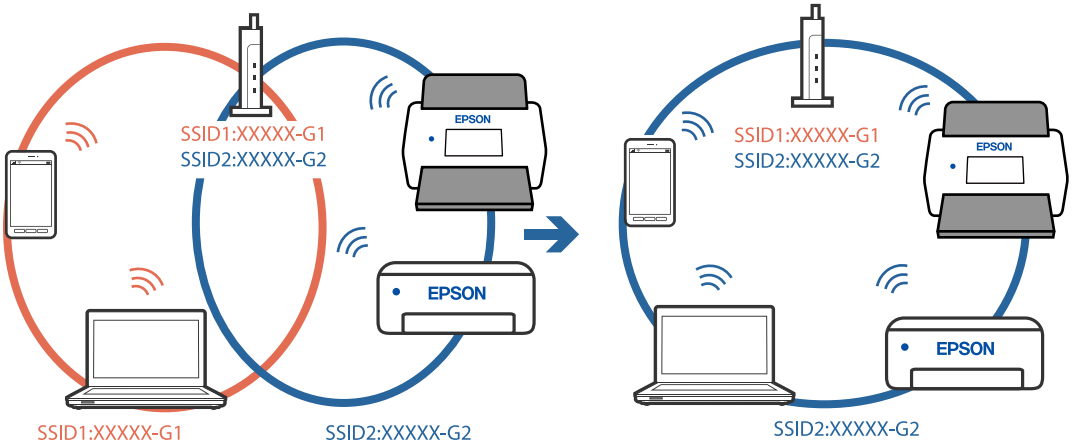
Reconfigure the settings so that they match the new wireless router.

The SSIDs connected from the computer or smart device and computer are different.

Solutions

When you are using multiple wireless routers at the same time or the wireless router has multiple SSIDs and devices are connected to different SSIDs, you cannot connect to the wireless router.

Connect the computer or smart device to the same SSID as the scanner.



A privacy separator on the wireless router is enabled.

Solutions

Most wireless routers have a privacy separator feature that blocks communication between connected devices. If you cannot communicate between the scanner and the computer or smart device even if they are connected to the same network, disable the privacy separator on the wireless router. See the manual provided with the wireless router for details.

The IP address is incorrectly assigned.

Solutions

If the IP address assigned to the scanner is 169.254.XXX.XXX, and the subnet mask is 255.255.0.0, the IP address may not be assigned correctly.

Select **Settings** - **Network Settings** - **Advanced** - **TCP/IP** on the scanner's control panel, and then check the IP address and the subnet mask assigned to the scanner.

Restart the wireless router or reset the network settings for the scanner.

There is a problem with the network settings on the computer.

Solutions

Try accessing any website from your computer to make sure that your computer's network settings are correct. If you cannot access any website, there is a problem on the computer.

Check the network connection of the computer. See the documentation provided with the computer for details.

The scanner has been connected by Ethernet using devices that support IEEE802.3az (Energy Efficient Ethernet).

Solutions

When you connect the scanner by Ethernet using devices that support IEEE802.3az (Energy Efficient Ethernet), the following problems may occur depending on the hub or router that you are using.

- ❏ Connection becomes unstable, the scanner is connected and disconnected again and again.
- ❏ Cannot connect to the scanner.
- ❏ The communication speed becomes slow.

Follow the steps below to disable IEEE802.3az for the scanner and then connect.

1. Remove the Ethernet cable connected to the computer and the scanner.
2. When IEEE802.3az for the computer is enabled, disable it.

   See the documentation provided with the computer for details.
3. Connect the computer and the scanner with an Ethernet cable directly.
4. On the scanner, check the network settings.

   Select **Settings** > **Network Settings** > **Network Status** > **Wired LAN/Wi-Fi Status**.
5. Check the scanner's IP address.
6. On the computer, access Web Config.

   Launch a Web browser, and then enter the scanner's IP address.

   “Running Web Config on a Web Browser” on page 37
7. Select the **Network** tab > **Wired LAN**.
8. Select **OFF** for **IEEE 802.3az**.
9. Click **Next**.
10. Click **OK**.
11. Remove the Ethernet cable connected to the computer and the scanner.
12. If you disabled IEEE802.3az for the computer in step 2, enable it.
13. Connect the Ethernet cables that you removed in step 1 to the computer and the scanner.

If the problem still occurs, devices other than the scanner may be causing the problem.

The scanner is off.

Solutions

Make sure the scanner is turned on.

Also, wait until the status light stops flashing indicating that the scanner is ready to scan.

Software for Setting Up the Scanner

Web Config. 37

Epson Device Admin. 38

Web Config

Web Config is an application that runs in web browsers, such as Microsoft Edge and Safari, on a computer. You can confirm the scanner status or change the network service and scanner settings. Since the scanners are accessed and operated directly from the network, it is suitable for setting up one scanner at a time. To use Web Config, connect your computer to the same network as the scanner.

The following browsers are supported. Use the latest version.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome, Safari

Note:
You may be prompted to enter the administrator password while using this device. See the following for details on the administrator password.

"Notes on the Administrator Password" on page 11

Related Information

➡ "Cannot Access Web Config" on page 75

Running Web Config on a Web Browser

1. Check the scanner's IP address.

   Select **Settings** > **Network Settings** > **Network Status** on the scanner's control panel. Then select the active connection method (**Wired LAN/Wi-Fi Status** or **Wi-Fi Direct Status**) to confirm the scanner's IP address.

2. Launch a Web browser from a computer or a smart device, and then enter the scanner's IP address.

   Format:

   IPv4: http://scanner's IP address/

   IPv6: http://[scanner's IP address]/

   Example:

   IPv4: http://192.168.100.201/

   IPv6: http://[2001:db8::1000:1]/

   Note:
   Since the scanner uses a self-signed certificate when accessing HTTPS, a warning is displayed on the browser when you start Web Config; this does not indicate a problem and can be safely ignored.

3. Login as an administrator to change the scanner settings.

   Click **Log in** at the top-right of the screen. Enter the **User Name** and **Current password**, and then click **OK**.

Note:

❏ *The following provides the initial values for the Web Config administrator information.*

·User name: none (blank)

·Password: Depends on the label attached to the back of the product.

If there is a "PASSWORD" label attached to the back, enter the 8-digit number shown on the label.

If there is no "PASSWORD" label attached, enter the serial number on the label attached to the back of the product for the initial administrator password.

❏ *If **Log out** is displayed at the top-right of the screen, you are already logged in as an administrator.*

❏ *You will be logged out automatically after approximately 20 minutes of inactivity.*

Running Web Config on Windows

When connecting a computer to the scanner using WSD, follow the steps below to run Web Config.

1. Open the scanner list on the computer.

   ❏ Windows 10

   Click on the start button, and then select **Windows System** > **Control Panel** > **View devices and printers** in **Hardware and Sound**.

   ❏ Windows 8.1/Windows 8

   Select **Desktop** > **Settings** > **Control Panel** > **View devices and printers** in **Hardware and Sound** (or **Hardware**).

   ❏ Windows 7

   Click the start button, and select **Control Panel** > **View devices and printers** in **Hardware and Sound**.

2. Right-click on your scanner and select **Properties**.

3. Select the **Web Service** tab and click the URL.

   Since the scanner uses a self-signed certificate when accessing HTTPS, a warning is displayed on the browser when you start Web Config; this does not indicate a problem and can be safely ignored.

   Note:

   ❏ *The following provides the initial values for the Web Config administrator information.*

   ·User name: none (blank)

   ·Password: Depends on the label attached to the back of the product.

   If there is a "PASSWORD" label attached to the back, enter the 8-digit number shown on the label.

   If there is no "PASSWORD" label attached, enter the serial number on the label attached to the back of the product for the initial administrator password.

   ❏ *If **Log out** is displayed at the top-right of the screen, you are already logged in as an administrator.*

   ❏ *You will be logged out automatically after approximately 20 minutes of inactivity.*

Epson Device Admin

Epson Device Admin is a multifunctional application that allows you to manage devices on a network.

You can use configuration templates to apply unified settings to multiple scanners on a network, making it suitable for installing and managing multiple scanners.

You can download Epson Device Admin from the Epson support website. For details on how to use this application, see the documentation or help for Epson Device Admin.

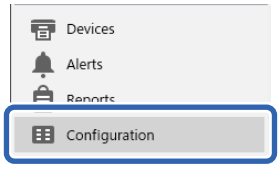
Configuration Template

Creating the Configuration Template

Create the configuration template newly.

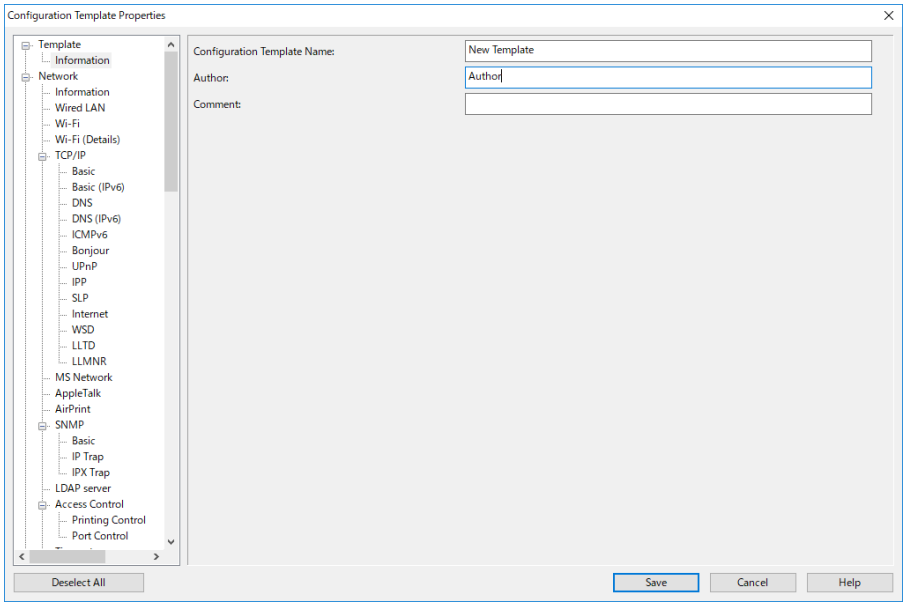
1. Start Epson Device Admin.

2. Select **Configuration** on the side bar task menu.



3. Select **New** on the ribbon menu.

4. Set each item.



Item	Explanation
Configuration Template Name	Name of the configuration template. Enter up to 1,024 characters in Unicode (UTF-8).
Author	Information on the creator of the template. Enter up to 1,024 characters in Unicode (UTF-8).
Comment	Enter arbitrary information. Enter up to 1,024 characters in Unicode (UTF-8).

5. Select the items you want to set on the left.

   Note:
   Click the menu items on the left to switch to each screen. The set value is retained if you switch the screen, but not if you cancel the screen. When you have finished all the settings, click ***Save****.*

Applying the Configuration Template

Apply the saved configuration template to the scanner. The items selected on the template are applied. If the target scanner does not have the appropriate function, it is not applied.

Note:
When an administrator password is set to the scanner, configure the password in advance.

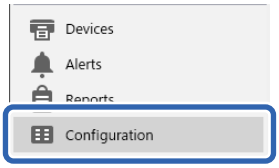
1. In the ribbon menu of the Device List screen, select ***Options*** *>* ***Password manager****.*

2. Select ***Enable automatic password management****, and then click* ***Password manager****.*

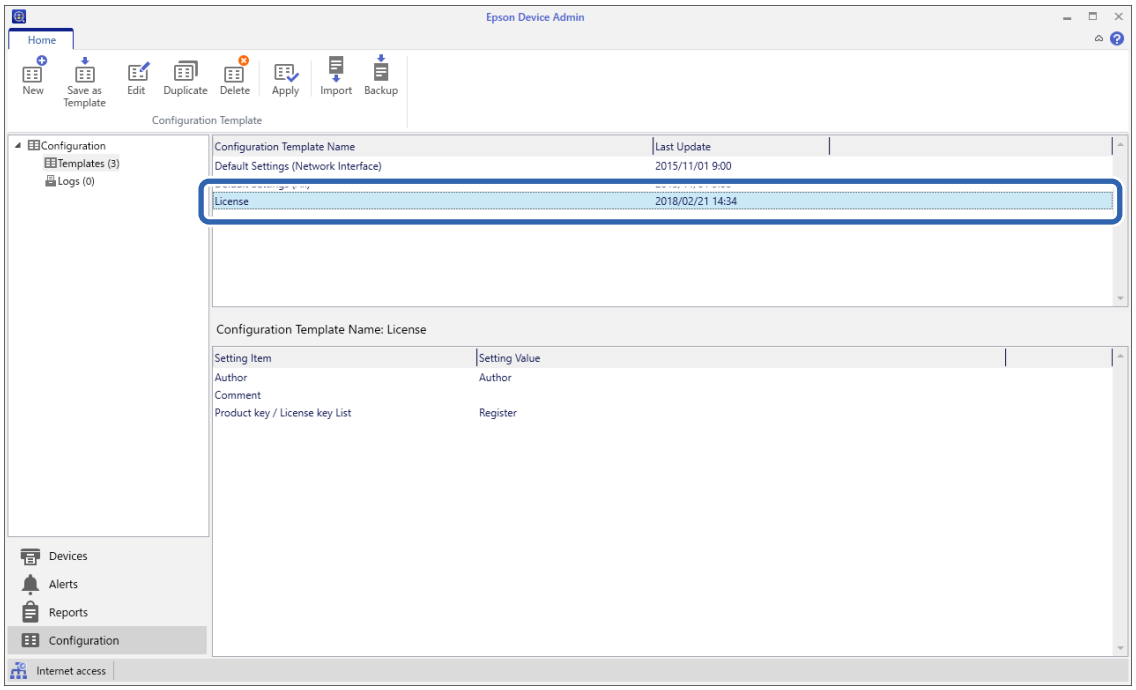
3. Select the appropriate scanner, and then click ***Edit****.*

4. Set the password, and then click ***OK****.*

1. Select **Configuration** on the side bar task menu.



2. Select the configuration template you want to apply from **Configuration Template Name**.



3. Click **Apply** on the ribbon menu.

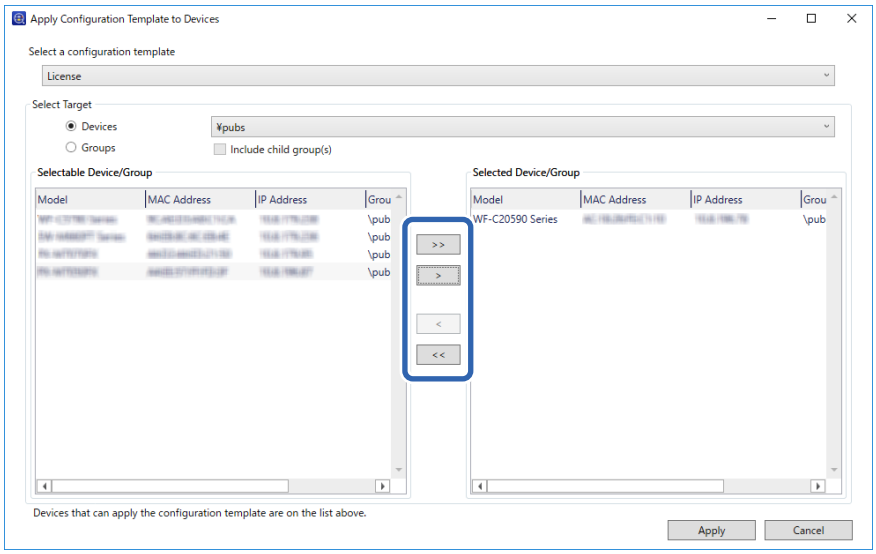
   The device selection screen is displayed.

4. Select the configuration template you want to apply.

Note:

- ❏ *When you select **Devices** and groups containing devices from the pull-down menu, each device is displayed.*
- ❏ *Groups are displayed when you select **Groups**. Select **Include child group(s)** to automatically select child groups within the selected group.*

5. Move the scanner or groups to which you want to apply the template to **Selected Device/Group**.



6. Click **Apply**.

   A confirmation screen for the configuration template to be applied is displayed.

7. Click **OK** to apply the configuration template.

8. When a message is displayed informing you that the procedure is complete, click **OK**.

9. Click **Details** and check the information.

   When is displayed on the items you applied, the application was completed successfully.

10. Click **Close**.

Required Settings for Scanning

Registering an Email Server. 44

Setting a Shared Network Folder. 48

Making Contacts Available. 64

Using Document Capture Pro Server. 74

Setting Up AirPrint. 74

Problems when Preparing Network Scanning. 75

Registering an Email Server

Check the following before configuring the email server.

❏ The scanner is connected to the network

❏ Setup information for email server

When you are using an Internet based email server, check the setting information from the provider or website.

How to Register

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

"Running Web Config on a Web Browser" on page 37

You can also make settings on the scanner's control panel. Select **Settings** > **Network Settings** > **Advanced** > **Email Server** > **Server Settings**.

Email Server Setting Items

Item	Settings and Explanation	
Authentication Method	Specify the authentication method for the scanner to access the mail server. **When using Microsoft Exchange Online:** Due to enhanced security in Microsoft Exchange Online, the previous Basic Authentication method has been discontinued and SMTP authentication (SMTP AUTH) has been disabled by default. Therefore, to use the email service from now on, you will need to use the **OAuth2** authentication method. If you use the email sending/email notification functions of a scanner, configure the email server settings to use **OAuth2** authentication. You should also enable SMTP AUTH in Exchange Online. "Enabling SMTP AUTH in Exchange Online" on page 45	
	Off	Authentication is disabled when communicating with a mail server.
	SMTP AUTH	The email server needs to support SMTP authentication.
	POP before SMTP	When you select this item, set a POP3 server.
	OAuth2	When you select this item, set an Email service.
Email service	If you select **OAuth2** as the **Authentication Method**, select an email service from the drop-down list. Click **Sign In**, and then follow the on-screen instructions to sign in to the email service. "Setting Up OAuth2.0 Authentication for the Email Server" on page 45 ***Note:*** *For personal use, select **Outlook.com**.*	
Authenticated Account	If you select **SMTP AUTH** or **POP before SMTP** as the **Authentication Method**, enter the authenticated account name. Enter within 0 to 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. Enter between 0 and 70 characters in ASCII (0x20-0x7E).	
Sender's Email Address	Set the email address that will be used to send emails from the scanner. Although you can use an existing email address, we recommend that you acquire and set up a dedicated email address so that it can be distinguished from emails sent from the scanner. Enter within 0 to 255 characters in ASCII (0x20 - 0x7E) except for : ( ) < > [ ] ; ¥. A period "." cannot be the first character.	

Item	Settings and Explanation	
SMTP Server Address	Enter between 0 and 255 characters using A-Z a-z 0-9 . - . You can use IPv4 or FQDN format.	
SMTP Server Port Number	Enter a number between 1 and 65535.	
Secure Connection	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 (Web Config only)	The certificate is validated when this is enabled. We recommend setting this to **Enable** when **Secure Connection** is set to anything other than **None**.	
POP3 Server Address	If you select **POP before SMTP** as the **Authentication Method**, enter the server address of the POP3 server. You can enter between 0 and 255 characters using A-Z a-z 0-9. You can use IPv4 or FQDN format.	
POP3 Server Port Number	Set when you select **POP before SMTP** in **Authentication Method**. Enter a number between 1 and 65535.	

Enabling SMTP AUTH in Exchange Online

Products use the SMTP protocol to send emails, so you must enable SMTP AUTH in Exchange Online.

For detailed instructions, search for and refer to the document on the "Microsoft Learn" site.

Setup procedure

❏ In the **Exchange admin center**, disable **security defaults** for the entire organization and enable SMTP AUTH.

❏ In the **Microsoft 365 admin center**, enable SMTP AUTH for the product administrator's mailbox.

Setting Up OAuth2.0 Authentication for the Email Server

Use Web Config to configure OAuth 2.0 authentication for the email server.

1. Access Web Config.

   "Running Web Config on a Web Browser" on page 37

2. Select **Network** tab > **Email Server** > **Basic**.

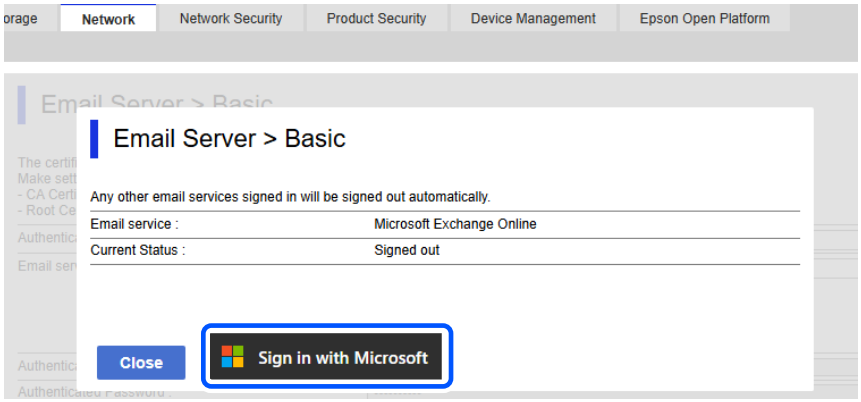
3. Select **OAuth2** as the **Authentication Method**.

4. Select **Microsoft Exchange Online** as the **Email service**.

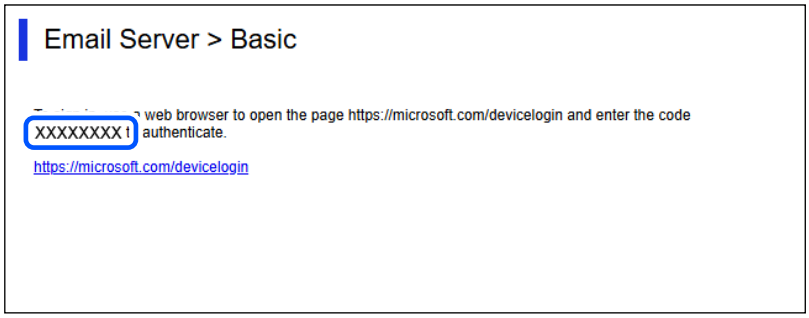
   Note:
   For personal use, select ***Outlook.com****.*

5. Sign in.

   Click **Sign In**, and then click **Sign in with Microsoft** on the screen that appears.



6. Copy the authentication code displayed on the screen, and then click the URL displayed to open the authentication screen.



7. On the authentication code entry screen, enter the code you copied, and then click **Next**.

8. On the Microsoft sign in screen, enter your account details, and then click **Next**.

   To sign in, your account must have at least the **Cloud Application Administrator** role assigned.

9. Enter the password and click **Sign In**.

   Note:
   If additional steps are required to sign in, follow the on-screen instructions.

10. On the requested permission screen, select "Consent on behalf of organization" and then click **Accept**.

    When authentication is complete, a sign-in message is displayed and you can close the browser screen.

    You can check the sign-in status on the **Network** tab > **Email Server** > **Basic** page in Web Config.

When the status shows **Signed in**, account information for OAuth 2.0 authentication is displayed.

11. Click **OK** to send the OAuth 2.0 authentication setting information to the product.

Checking a Mail Server Connection

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

1. Enter the IP address of the scanner in the browser and start Web Config.
2. Enter the administrator password to log in as an administrator.
3. Select in the following order.

   Network tab > **Email Server** > **Connection Test**
4. Select **Start**.

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

   Note:
   You can also check the connection to the mail server from the control panel. Access as below.

   Settings > ***Network Settings*** > ***Advanced*** > ***Email Server*** > ***Connection Check***

Mail Server Connection Test References

Messages	Cause
Connection test was successful.	This message appears when the connection with the server is successful.
SMTP server communication error. Check the following. - Network Settings	This message appears when ❏ The scanner is not connected to a network ❏ SMTP server is down ❏ Network connection is disconnected while communicating ❏ Received incomplete data
POP3 server communication error. Check the following. - Network Settings	This message appears when ❏ The 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 a POP3 server failed

Messages	Cause
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 a 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.
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.

Setting a Shared Network Folder

Set a shared network folder to save the scanned image.

When saving a file to the folder, the scanner logs on as the user of the computer on which the folder was created.

Creating the Shared Folder

Related Information

➡ "Before Creating the Shared Folder" on page 49

➡ "Checking the Network Profile" on page 49

➡ "Location Where the Shared Folder is Created and an Example of the Security" on page 49

➡ "Adding Group or User Which Permits Access" on page 61

Before Creating the Shared Folder

Before creating the shared folder, check the following.

❏ The scanner is connected to the network where it can access the computer where the shared folder will be created.

❏ A multi-byte character is not included in the name of the computer where the shared folder will be created.

Important:

When a multi-byte character is included in the computer name, saving the file to the shared folder may fail.

In that case, change to the computer that does not include the Multi-byte character in the name or change the computer name.

When changing the computer name, make sure to confirm with the administrator in advance because it may affect some settings, such as computer management, resource access, etc.

Checking the Network Profile

On the computer where the shared folder will be created, check whether folder sharing is available.

1. Log in to the computer where the shared folder will be created by the administrator authority user account.
2. Select **Control Panel** > **Network and Internet** > **Network and Sharing Center**.
3. Click **Change advanced sharing settings**, and then click for the profile with **(current profile)** in the displayed network profiles.
4. Check whether **Turn on file and printer sharing** is selected on **File and Printer Sharing**.

   If already selected, click **Cancel** and close the window.

   When you change the settings, click **Save Changes** and close the window.

Location Where the Shared Folder is Created and an Example of the Security

Depending on the location where the shared folder is created, security and convenience vary.

To operate the shared folder from the scanners or other computers, the following reading and changing permissions for the folder are required.

❏ **Sharing** tab > **Advanced Sharing** > **Permissions**

It controls the network access permission of the shared folder.

❏ Access permission of **Security** tab

It controls permission of the network access and local access of the shared folder.

When you set **Everyone** to the shared folder that is created on the desktop, as an example of creating a shared folder, all users who can access the computer will be permitted access.

However, the user who does not have authority cannot access them because the desktop (folder) is under the control of the user folder, and then the security settings of the user folder are handed down to it. The user who is permitted access on the **Security** tab (user logged in and administrator in this case) can operate the folder.

See below to create the proper location.

This example is when creating the "scan_folder" folder.

Related Information

➡ "Example of Configuration for File Servers" on page 50

➡ "Example of Configuration for a Personal Computer" on page 56

Example of Configuration for File Servers

This explanation is an example for creating the shared folder on the root of the drive on the shared computer, such as the file server under the following condition.

Access controllable users, such as someone who has the same domain of a computer to create a shared folder, can access the shared folder.

Set this configuration when you permit any user to read and write to the shared folder on the computer, such as the file server and the shared computer.

❏ Place for creating shared folder: Root of drive

❏ Folder path: C:\scan_folder

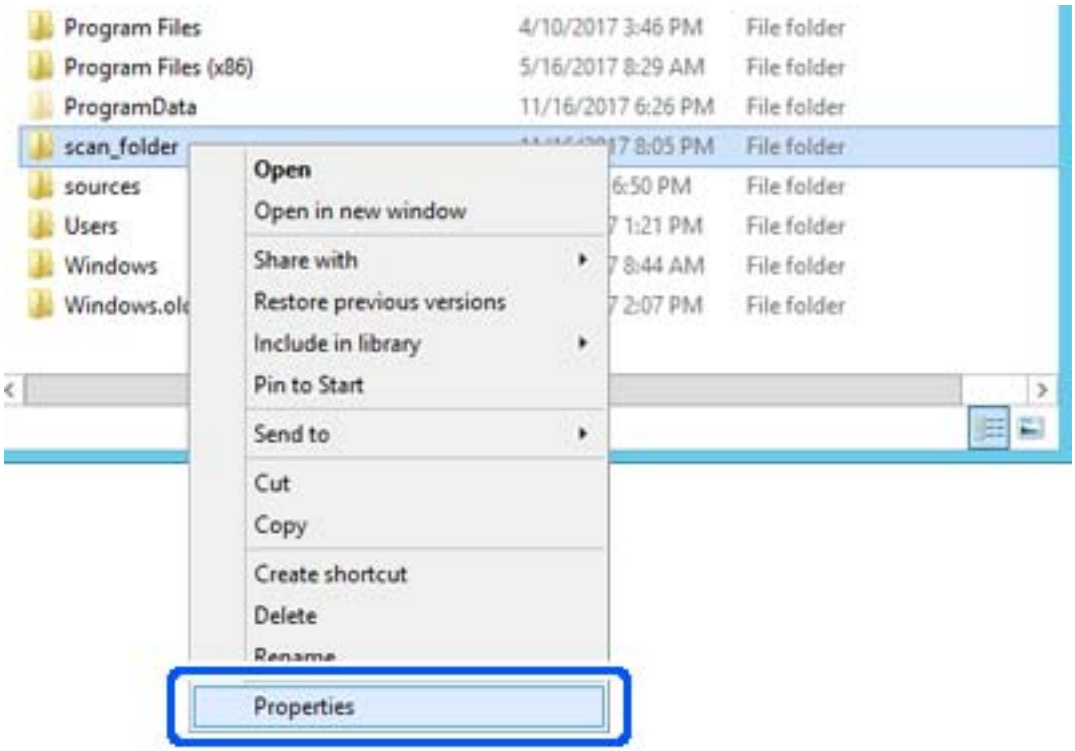
❏ Access permission via network (Share Permissions): Everyone

❏ Access permission on file system (Security): Authenticated Users

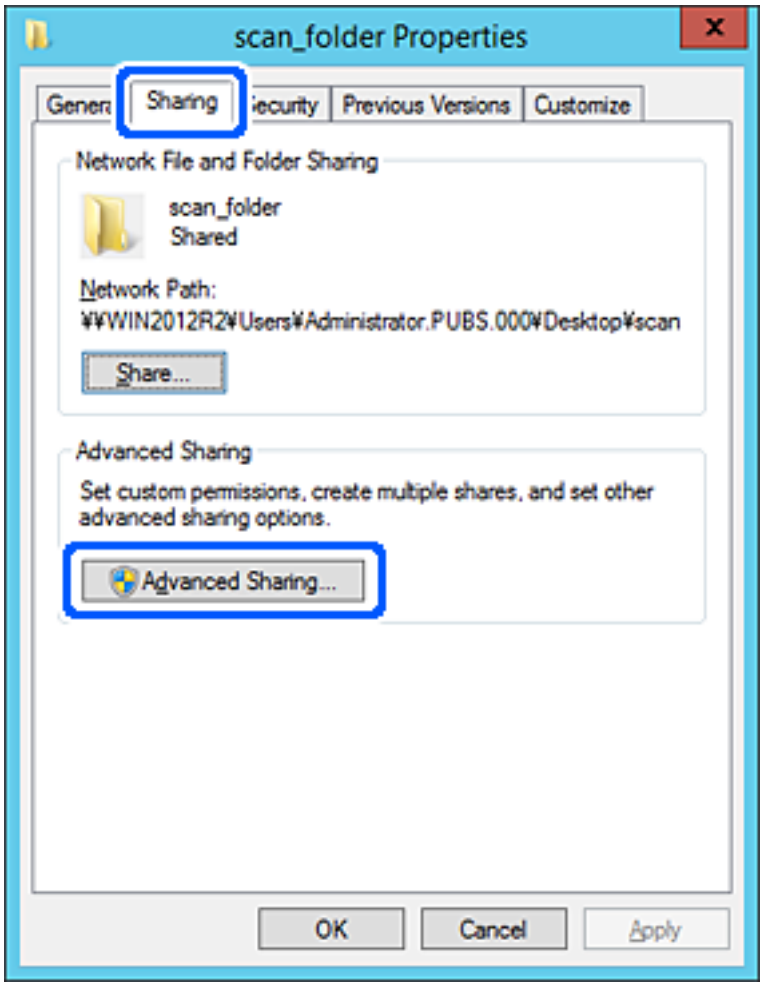
1. Log in to the computer where the shared folder will be created by the administrator authority user account.
2. Start explorer.
3. Create the folder on the root of drive, and then name it "scan_folder".

   For the folder name, enter between 1 and 12 alphanumeric characters. If the character limit of the folder name is exceeded, you may not be able to access it normally by the varied environment.

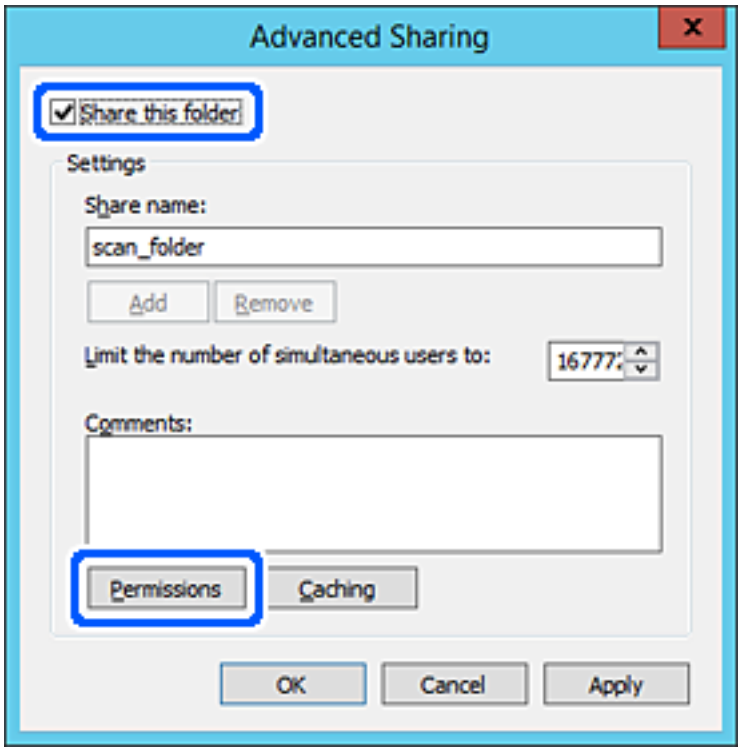
4. Right click the folder, and then select **Properties**.



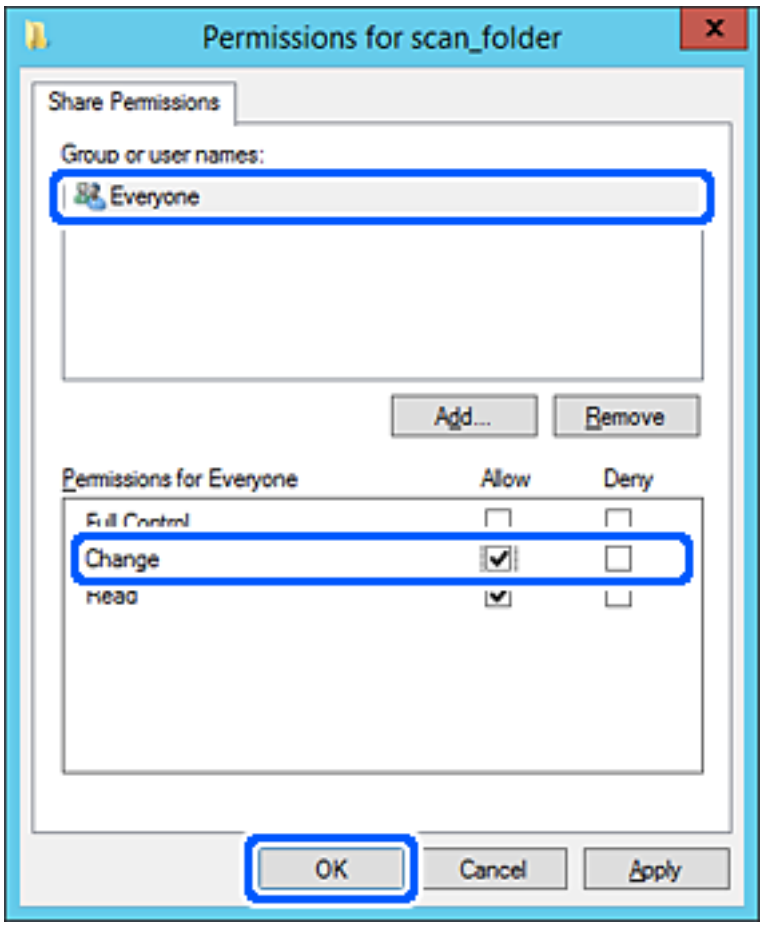
5. Click **Advanced Sharing** on the **Sharing** tab.



6. Select **Share this folder**, and then click **Permissions**.

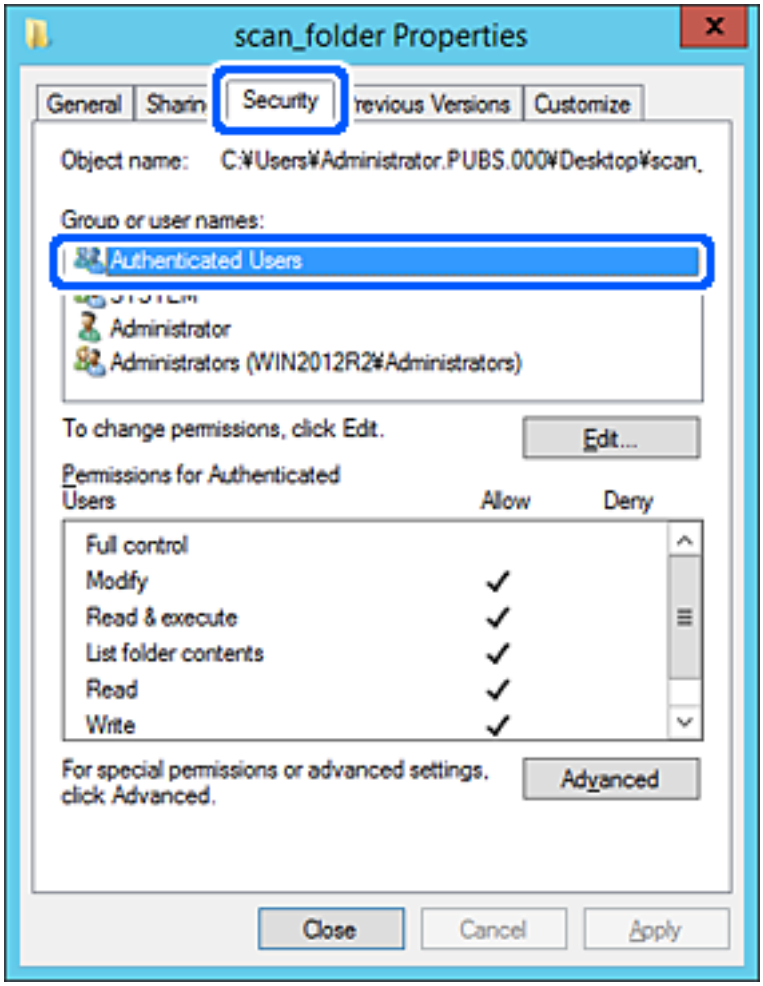


7. Select **Everyone** group of **Group or user names**, select **Allow** on **Change**, and then click **OK**.



8. Click **OK**.

9. Select **Security** tab, and then select **Authenticated Users** on the **Group or user names**.

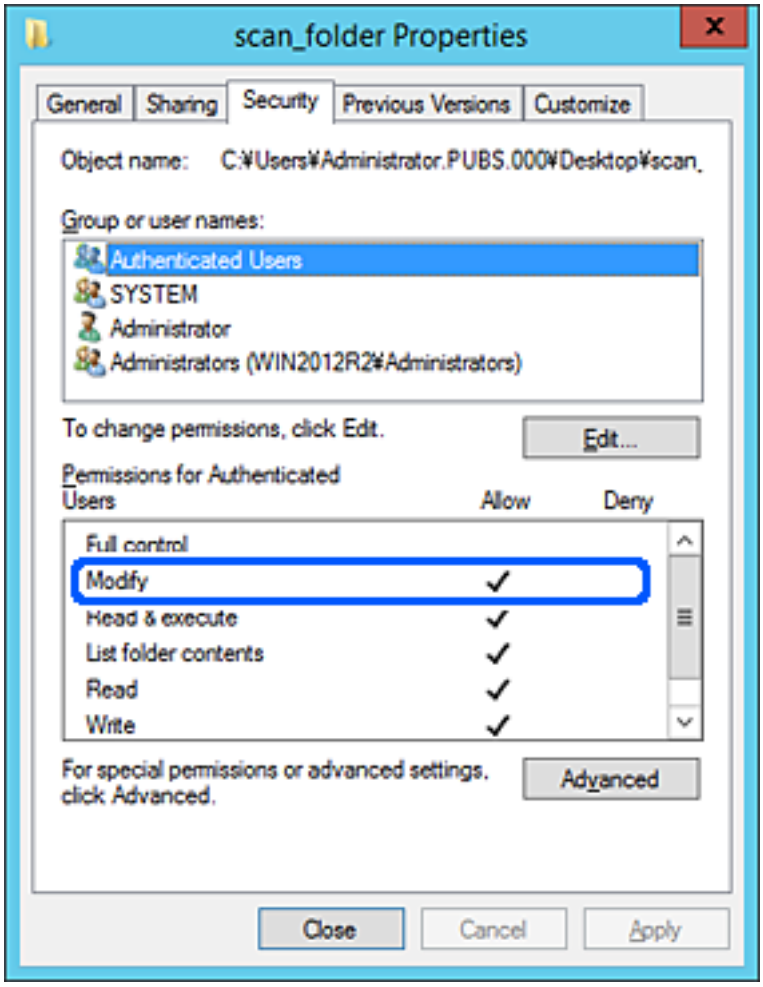


"Authenticated Users" is the special group that includes all users who can log in to the domain or computer. This group is displayed only when the folder is created just below the root folder.

If it is not displayed, you can add it by clicking **Edit**. For more details, see Related Information.

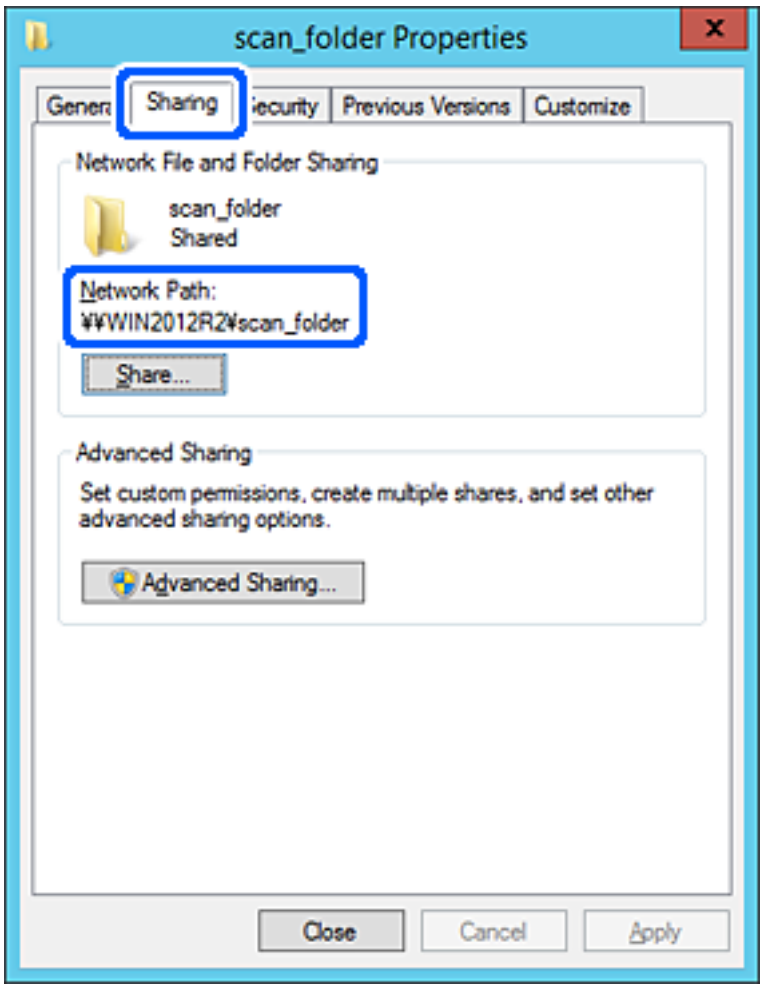
10. Check that **Allow** on **Modify** is selected in **Permissions for Authenticated Users**.

    If it is not selected, select **Authenticated Users**, click **Edit**, select **Allow** on **Modify** in **Permissions for Authenticated Users**, and then click **OK**.



11. Select **Sharing** tab.

    The network path of the shared folder is displayed. This is used when registering to the contacts of the scanner. Please write it down.



12. Click **OK** or **Close** to close the screen.

    Check whether the file can be written or read on the shared folder from the computers of the same domain.

Related Information

➡ "Adding Group or User Which Permits Access" on page 61

➡ "Registering a Destination to Contacts using Web Config" on page 65

Example of Configuration for a Personal Computer

This explanation is an example for creating the shared folder on the desktop of the user currently logging in to the computer.

The user who logs in to the computer and who has administrator authority can access the desktop folder and the document folder that are under the User folder.

Set this configuration when you DO NOT permit reading and writing to another user to the shared folder on a personal computer.

❏ Place for creating shared folder: Desktop

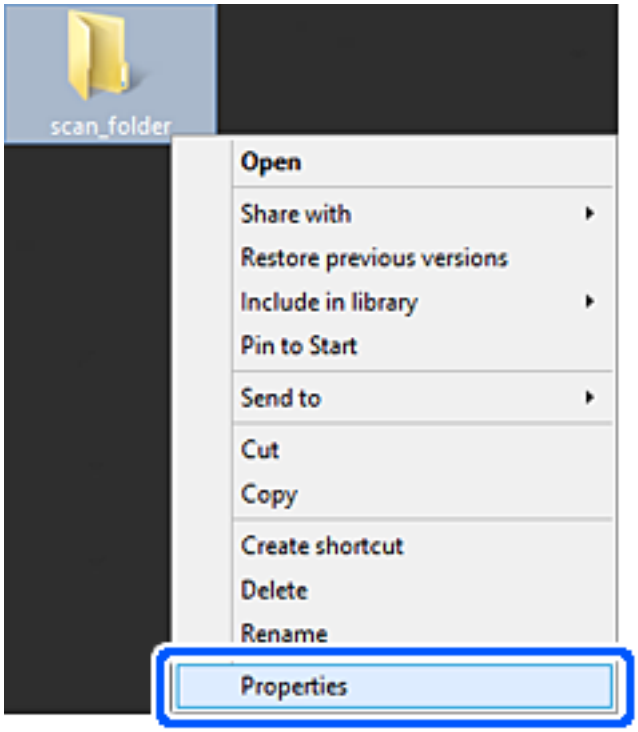
❏ Folder path: C:\Users\xxxx\Desktop\scan_folder

❏ Access permission via network (Share Permissions): Everyone

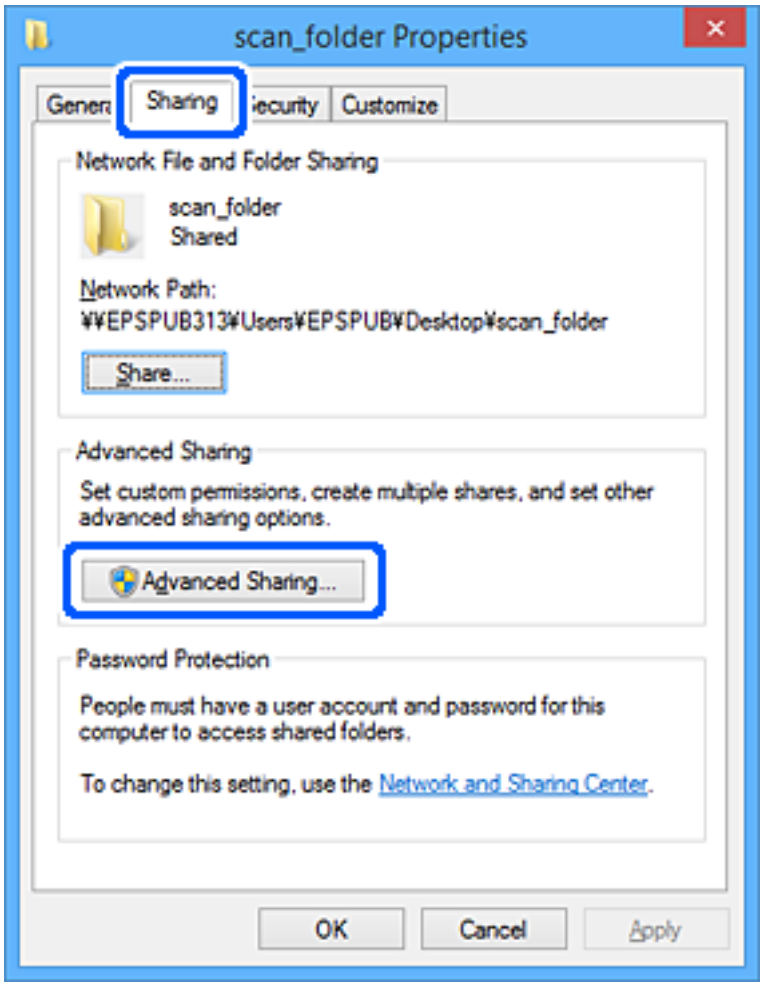
❏ Access permission on file system (Security): do not add, or add User/Group names to permit access

1. Log in to the computer where the shared folder will be created by the administrator authority user account.
2. Start explorer.
3. Create the folder on the desktop, and then name it "scan_folder".

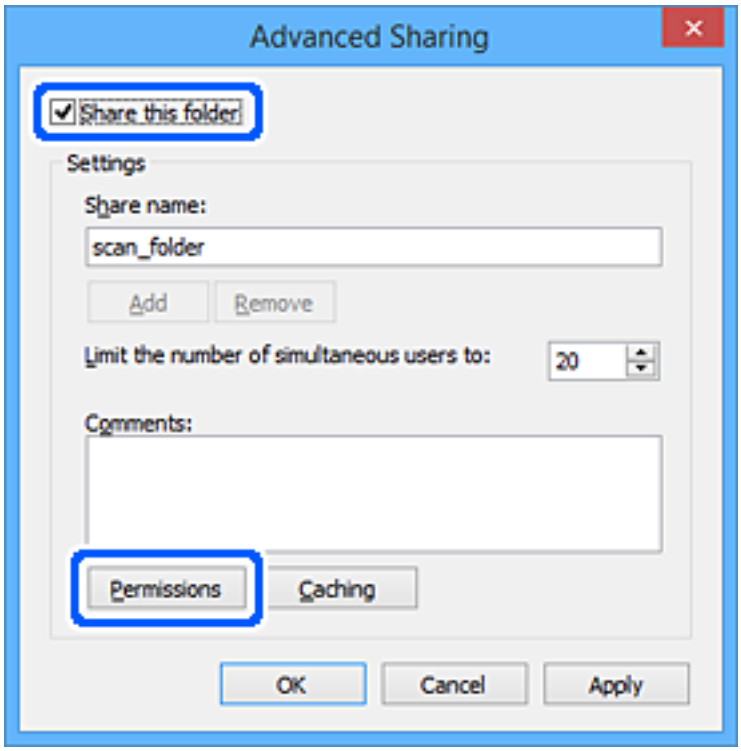
   For the folder name, enter between 1 and 12 alphanumeric characters. If the character limit of the folder name is exceeded, you may not be able to access it normally by the varied environment.
4. Right click the folder, and then select **Properties**.



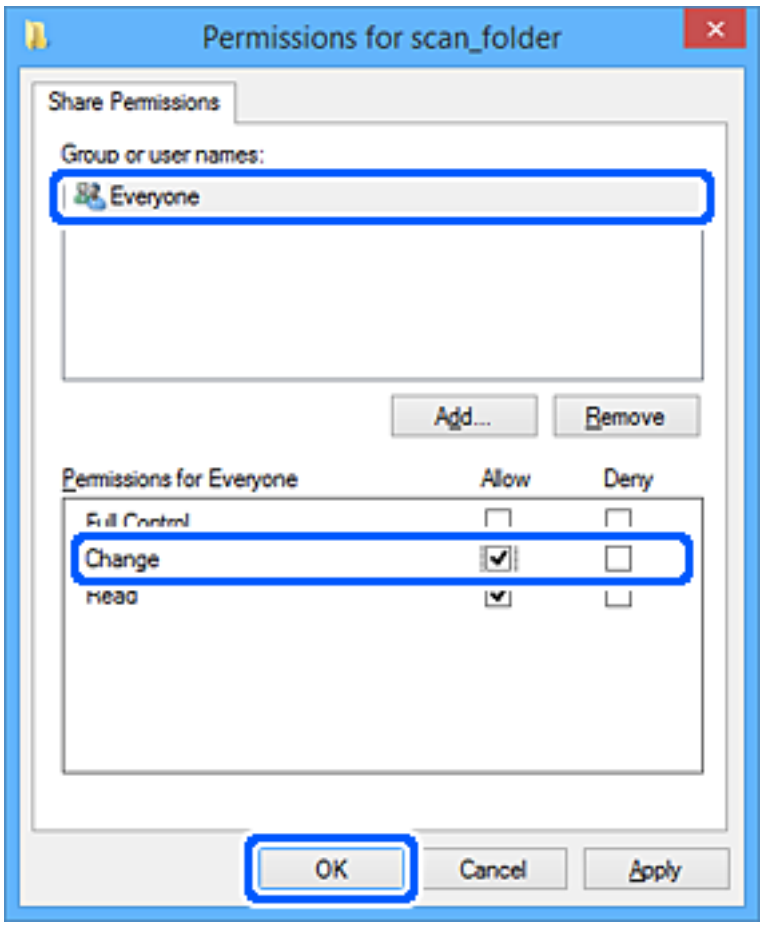
5. Click **Advanced Sharing** on the **Sharing** tab.



6. Select **Share this folder**, and then click **Permissions**.



7. Select **Everyone** group of **Group or user names**, select **Allow** on **Change**, and then click **OK**.

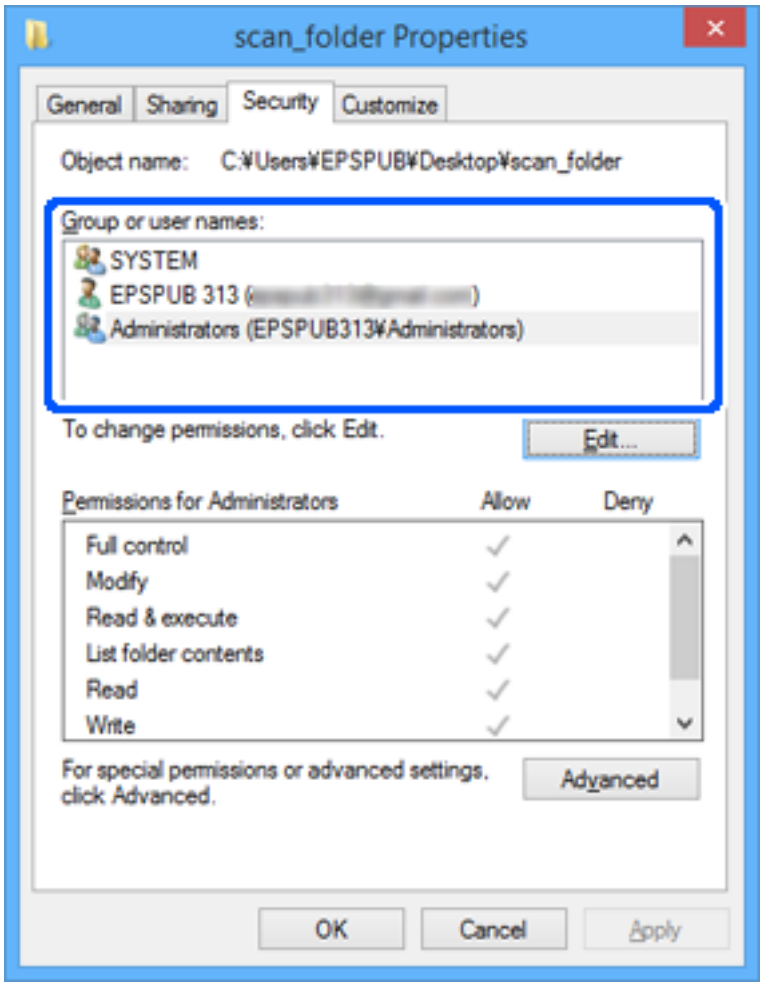


8. Click **OK**.
9. Select **Security** tab.
10. Check the group or the user in the **Group or user names**.

    The group or the user that is displayed here can access the shared folder.

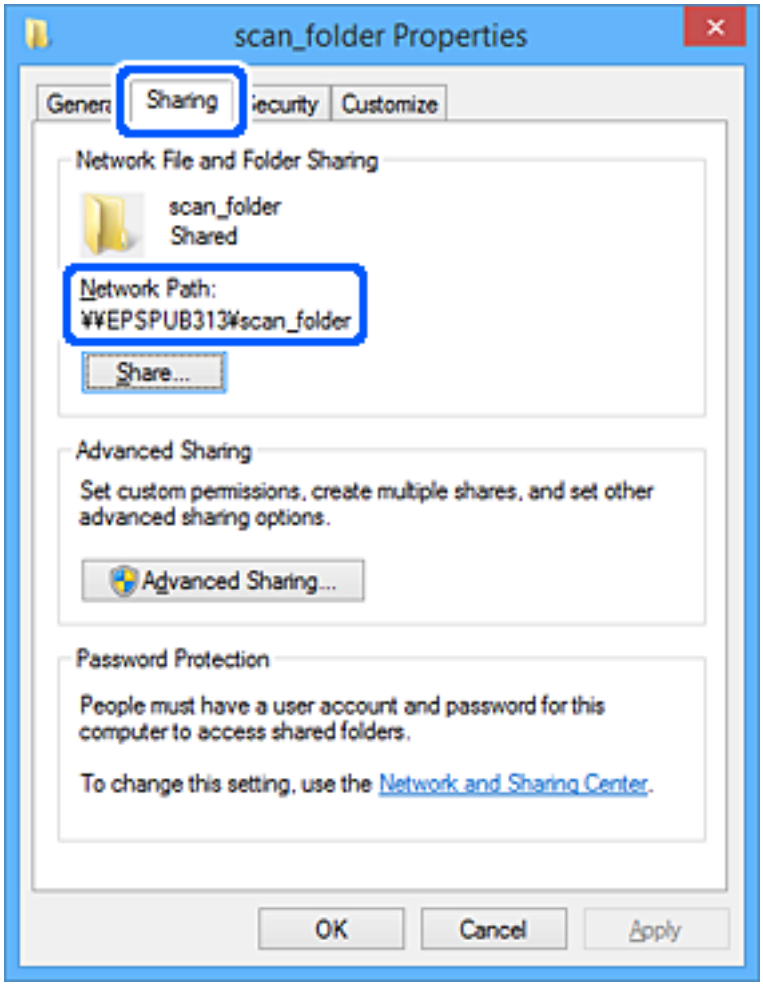
    In this case, the user who logs in to this computer and the Administrator can access the shared folder.

    Add access permission, if necessary. You can add it by clicking **Edit**. For more details, see Related Information.



11. Select **Sharing** tab.

    The network path of the shared folder is displayed. This is used when registering to the contacts of the scanner. Please write it down.



12. Click **OK** or **Close** to close the screen.

    Check whether the file can be written or read on the shared folder from the computers of users or groups with access permission.

Related Information

➡ "Adding Group or User Which Permits Access" on page 61
➡ "Registering a Destination to Contacts using Web Config" on page 65

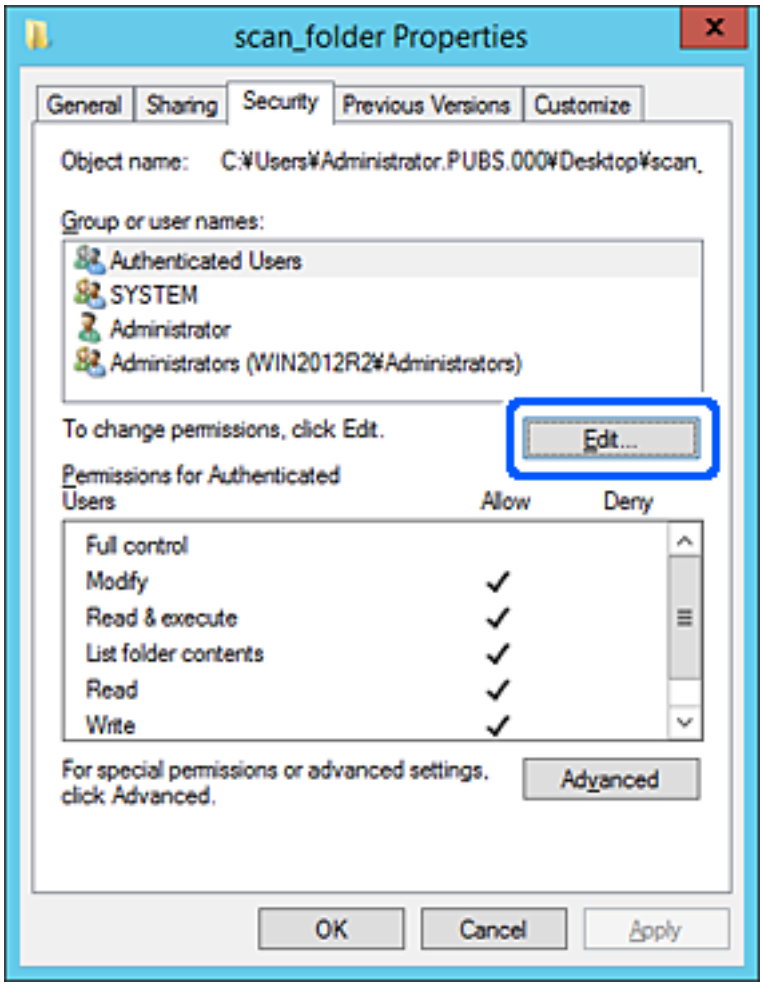
Adding Group or User Which Permits Access

You can add the group or user which permits access.

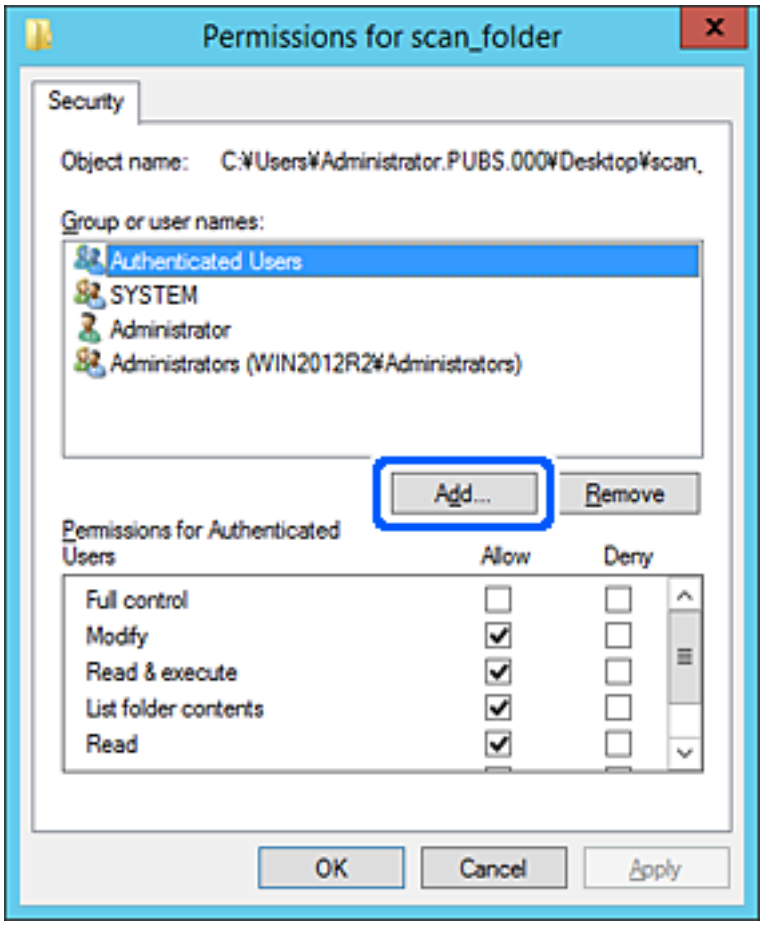
1. Right click the folder and select **Properties**.

2. Select **Security** tab.

3. Click **Edit**.


scan_folder Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:¥Users¥Administrator.PUBS.000¥Desktop¥scan
Group or user names:
Authenticated Users
SYSTEM
Administrator
Administrators (WIN2012R2¥Administrators)
To change permissions, click Edit.
Edit...
Permissions for Authenticated Users
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

4. Click **Add** under the **Group or user names**.

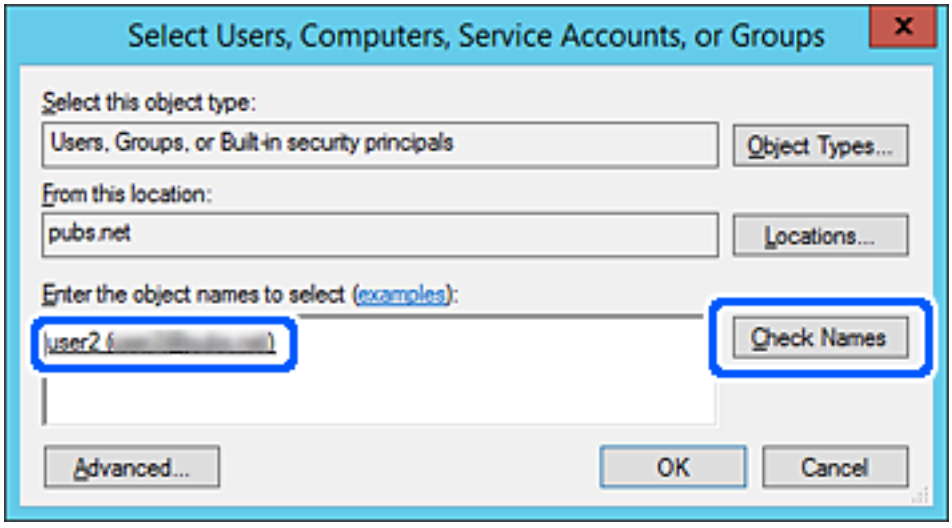


5. Enter the group or user name that you want to permit access, and then click **Check Names**.

   An underline is added to the name.

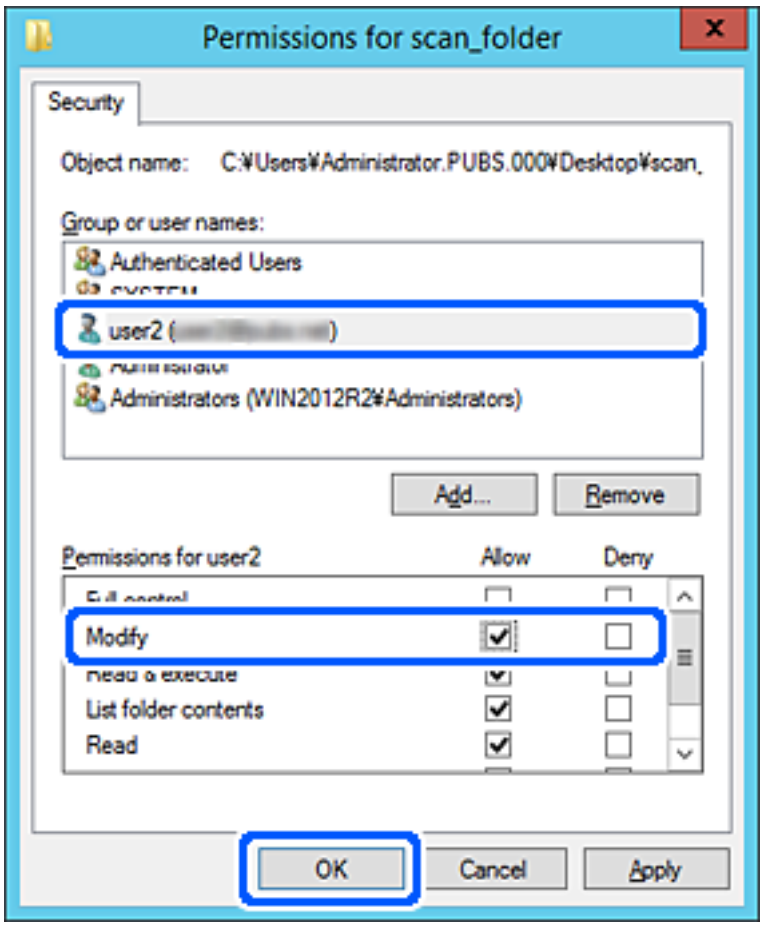
   Note:
   If you do not know the full name of the group or user, enter part of the name, and then click ***Check Names****. The group names or user names that match part of the name are listed, and then you can select the full name from the list.*

   If just one name matches, the full name with underlining is displayed in ***Enter the object name to select****.*



6. Click **OK**.

7. On the Permission screen, select the user name that is entered in **Group or user names** , select the access permission on **Modify**, and then click **OK**.



8. Click **OK** or **Close** to close the screen.

   Check whether the file can be written or read on the shared folder from the computers of users or groups with access permission.

Making Contacts Available

Registering destinations in the scanner's contacts list allows you to easily enter the destination when scanning.

You can register the following types of destinations in the contacts list. You can register up to 300 entries in total.

Note:
You can also use the LDAP server (LDAP search) to enter the destination.

Email	Destination for email. You need to configure the email server settings beforehand.
Network Folder	Destination for scan data. You need to prepare the network folder beforehand.

Related Information

➡ "Cooperation between the LDAP Server and Users" on page 70

Contacts Configuration Comparison

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

Features	Web Config*	Epson Device Admin	Scanner's control panel
Registering a destination	✓	✓	✓
Editing a destination	✓	✓	✓
Adding a group	✓	✓	✓
Editing a group	✓	✓	✓
Deleting a destination or groups	✓	✓	✓
Deleting all destinations	✓	✓	–
Importing a file	✓	✓	–
Exporting to a file	✓	✓	–

* Log on as an administrator to make settings.

Registering a Destination to Contacts using Web Config

Note:
You can also register the contacts on the scanner's control panel.

1. Access Web Config and select the **Scan** tab > **Contacts**.
2. Select the number that you want to register, and then click **Edit**.
3. Enter **Name** and **Index Word**.
4. Select the destination type as the **Type** option.

   Note:
   *You cannot change the **Type** option after registration is complete. If you want to change the type, delete the destination and then register again.*
5. Enter a value for each item, and then click **Apply**.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Destination Setting Items

Items	Settings and Explanation
Common Settings	
Name	Enter a name displayed in the contacts in 30 characters or less in Unicode (UTF-16). If you do not specify this, leave it blank.
Index Word	Enter a name using 30 characters or less in Unicode (UTF-16) to search the contacts on the scanner's control panel. If you do not specify this, leave it blank.
Type	Select the type of the address that you want to register.
Assign to Frequent Use	Select to set the registered address as a frequently used address. When setting as a frequently used address, it is displayed on the top screen of scan, and you can specify the destination without displaying the contacts.
Email	
Email Address	Enter between 1 and 255 characters using A-Z a-z 0-9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Network Folder (SMB)	
Save to	\\“Folder path” Enter the location where the target folder is located between 1 and 253 characters in Unicode (UTF-16), omitting "\\". Enter the network path displayed on the folder's property screen. See the following for details on setting the network path. “Example of Configuration for a Personal Computer” on page 56
User Name	Enter a user name to access a network folder in 30 characters or less in Unicode (UTF-16). However, avoid using control characters (0x00 to 0x1f, 0x7F).
Password	Enter a password to access a network folder between 0 and 20 characters in Unicode (UTF-16). However, avoid using control characters (0x00 to 0x1f, 0x7F).
FTP	
Secure Connection	Select FTP or FTPS according to the file transfer protocol the FTP server supports. Select **FTPS** to allow the scanner to communicate with security measures.
Save to	Enter the server name between 1 and 253 characters in Unicode (UTF-16), omitting "ftp://" or "ftps://".
User Name	Enter a user name to access an FTP server in 30 characters or less in Unicode (UTF-16). However, avoid using control characters (0x00 to 0x1f, 0x7F). If the server allows anonymous connections, enter a user name such as Anonymous and FTP. If you do not specify this, leave it blank.
Password	Enter a password to access to an FTP server between 0 and 20 characters in Unicode (UTF-16). However, avoid using control characters (0x00 to 0x1f, 0x7F). If you do not specify this, leave it blank.
Connection Mode	Select the connection mode from the menu. If a firewall is set between the scanner and the FTP server, select **Passive Mode**.
Port Number	Enter the FTP server port number between 1 and 65535.

Items	Settings and Explanation
Certificate Validation	The FTP server's certificate is validated when this is enabled. This is available when **FTPS** is selected for **Secure Connection**. To set up, you need to import the CA Certificate to the scanner.
SharePoint(WebDAV)*	
Secure Connection	Select HTTP or HTTPS according to the file transfer protocol the server supports. Select **HTTPS** to allow the scanner to communicate with security measures.
Save to	Enter the server name between 1 and 253 characters in Unicode (UTF-16), omitting "http://" or "https://".
User Name	Enter a user name to access a server in 30 characters or less in Unicode (UTF-16). However, avoid using control characters (0x00 to 0x1f, 0x7F). If you do not specify this, leave it blank.
Password	Enter a password to access to a server between 0 and 20 characters in Unicode (UTF-16). However, avoid using control characters (0x00 to 0x1f, 0x7F). If you do not specify this, leave it blank.
Certificate Validation	The server's certificate is validated when this is enabled. This is available when **HTTPS** is selected for **Secure Connection**. To set up, you need to import the CA Certificate to the scanner.
Proxy Server	Select whether or not to use a proxy server.

*SharePoint Online is not supported when scanning to network folder from the scanner's control panel.

If you want to save the scanned image to SharePoint Online, use Document Capture Pro after installing the SharePoint Online Connector. See the Document Capture Pro manual for details.

https://support.epson.net/dcp/

Registering Destinations as a Group Using Web Config

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

1. Access Web Config and select the **Scan** tab > **Contacts**.
2. Select the number that you want to register, and then click **Edit**.
3. Select a group from **Type**.
4. Click **Select** for **Contact(s) for Group**.
   The available destinations are displayed.
5. Select the destination that you want to register to the group, and then click **Select**.
6. Enter a **Name** and **Index Word**.
7. Select whether or not you assign the registered group to the frequently used group.

   Note:
   Destinations can be registered to multiple groups.

8. Click **Apply**.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Backing Up and Importing Contacts

Using Web Config or other tools, you can back up and import contacts.

For Web Config, you can back up contacts by exporting the scanner settings that include contacts. The exported file cannot be edited because it is exported as a binary file.

When importing the scanner settings to the scanner, contacts are overwritten.

For Epson Device Admin, only contacts can be exported from the device's property screen. Also, if you do not export the security-related items, you can edit the exported contacts and import them because this can be saved as a SYLK file or CSV file.

Importing Contacts Using Web Config

If you have a scanner that allows you to backup contacts and is compatible with this scanner, you can register contacts easily by importing the backup file.

Note:
For instructions on how to back up the scanner contacts, see the manual provided with the scanner.

Follow the steps below to import the contacts to this scanner.

1. Access Web Config, select **Device Management** tab > **Export and Import Setting Value** > **Import**.
2. Select the backup file you created in **File**, enter the password, and then click **Next**.
3. Select the **Contacts** checkbox, and then click **Next**.

Backing up Contacts Using Web Config

Contacts data may be lost due to a scanner malfunction. We recommend that you make a backup of the data whenever you update the data. Epson shall not be responsible for the loss of any data, for backing up or recovering data and/or settings even during a warranty period.

Using Web Config, you can back up the contact data stored in the scanner to the computer.

1. Access Web Config, and then select the **Device Management** tab > **Export and Import Setting Value** > **Export**.
2. Select the **Contacts** checkbox under the **Scan** category.
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**.

Export and Bulk Registration of Contacts Using Tool

If you use Epson Device Admin, you can back up just the contacts and edit the exported files, then register them all at once.

It is useful if you want to back up only the contacts or when you replace the scanner and you want to transfer the contacts from the old one to new one.

Exporting Contacts

Save the contacts information to the file.

You can edit files saved in SYLK format or csv format by using a spreadsheet application or text editor. You can register all at once after deleting or adding the information.

Information that includes security items such as password and personal information can be saved in binary format with a password. You cannot edit the file. This can be used as the backup file of the information including the security items.

1. Start Epson Device Admin.
2. Select **Devices** on the side bar task menu.
3. Select the device you want to configure from the device list.
4. Click **Device Configuration** on the **Home** tab on the ribbon menu.

   When the administrator password has been set, enter the password and click **OK**.
5. Click **Common** > **Contacts**.
6. Select the export format from **Export** > **Export items**.
   - ❏ All Items

     Export the encrypted binary file. Select when you want to include the security items such as password and personal information. You cannot edit the file. If you select it, you have to set the password. Click **Configuration** and set a password between 8 and 63 characters long in ASCII. This password is required when importing the binary file.
   - ❏ Items except Security Information

     Export the SYLK format or csv format files. Select when you want to edit the information of the exported file.
7. Click **Export**.
8. Specify the place to save the file, select the file type, and then click **Save**.

   The completion message is displayed.
9. Click **OK**.

   Check that the file is saved to the specified place.

Importing Contacts

Import the contacts information from the file.

You can import the files saved in SYLK format or csv format or the backed-up binary file that includes the security items.

1. Start Epson Device Admin.
2. Select **Devices** on the side bar task menu.
3. Select the device you want to configure from the device list.
4. Click **Device Configuration** on the **Home** tab on the ribbon menu.

   When the administrator password has been set, enter the password and click **OK**.
5. Click **Common** > **Contacts**.
6. Click **Browse** on **Import**.
7. Select the file you want to import and then click **Open**.

   When you select the binary file, in **Password** enter the password you set when exporting the file.
8. Click **Import**.

   The confirmation screen is displayed.
9. Click **OK**.

   The validation result is displayed.

   ❏ Edit the information read

   Click when you want to edit the information individually.

   ❏ Read more file

   Click when you want to import multiple files.
10. Click **Import**, and then click **OK** on the import completion screen.

    Return to the device's property screen.
11. Click **Transmit**.
12. Click **OK** on the confirmation message.

    The settings are sent to the scanner.
13. On the sending completion screen, click **OK**.

    The scanner's information is updated.

    Open the contacts from Web Config or scanner's control panel, and then check that the contact is updated.

Cooperation between the LDAP Server and Users

When cooperating with the LDAP server, you can use the address information registered to the LDAP server as the destination of an email.

Configuring the LDAP Server

To use LDAP server information, register it on the scanner.

1. Access the Web Config and select the **Network** tab > **LDAP Server** > **Basic**.
2. Enter a value for each item.
3. Select **OK**.

   The settings you have selected are displayed.

LDAP Server Settings

Items	Settings and Explanation
Use LDAP Server	Select **Use** or **Do Not Use**.
LDAP Server Address	Enter the address of the LDAP server. Enter between 1 and 255 characters of either IPv4, IPv6, or FQDN format. For the FQDN format, you can use alphanumeric characters in ASCII (0x20-0x7E) and "- " except for the beginning and end of the address.
LDAP server Port Number	Enter the LDAP server port number between 1 and 65535.
Secure Connection	Specify the authentication method when the scanner accesses the LDAP server.
Certificate Validation	When this is enabled, the certificate of the LDAP sever is validated. We recommend this is set to **Enable**. To set up, the **CA Certificate** needs to be imported to the scanner.
Search Timeout (sec)	Set the length of time for searching before timeout occurs between 5 and 300.
Authentication Method	Select one of the methods. If you select **Kerberos Authentication**, select **Kerberos Settings** to configure settings for Kerberos. To perform Kerberos Authentication, the following environment is required. ❏ The scanner and the DNS server can communicate. ❏ The time of the scanner, KDC server, and the server that is required for authentication (LDAP server, SMTP server, File server) are synced. ❏ When the service server is assigned as the IP address, the FQDN of the service server is registered on the DNS server reverse lookup zone.
Kerberos Realm to be Used	If you select **Kerberos Authentication** for **Authentication Method**, select the Kerberos realm that you want to use.
Administrator DN / User Name	Enter the user name for the LDAP server in 128 characters or less in Unicode (UTF-8). You cannot use control characters, such as 0x00-0x1F and 0X7F. This setting is not used when **Anonymous Authentication** is selected as the **Authentication Method**. If you do not specify this, leave it blank.
Password	Enter the password for the LDAP server authentication in 128 characters or less in Unicode (UTF-8). You cannot use control characters, such as 0x00-0x1F and 0X7F. This setting is not used when **Anonymous Authentication** is selected as the **Authentication Method**. If you do not specify this, leave it blank.

Kerberos Settings

If you select **Kerberos Authentication** for **Authentication Method** of **LDAP Server** > **Basic**, configure the following Kerberos settings from the **Network** tab > **Kerberos Settings**. You can register up to 10 settings for the Kerberos settings.

Items	Settings and Explanation
Realm (Domain)	Enter the realm of the Kerberos authentication in 255 characters or less in ASCII (0x20-0x7E). If you do not register this, leave it blank.
KDC Address	Enter the address of the Kerberos authentication server. Enter 255 characters or less in either IPv4, IPv6 or FQDN format. If you do not register this, leave it blank.
Port Number (Kerberos)	Enter the Kerberos server port number between 1 and 65535.

Configuring the LDAP Server Search Settings

When you set up the search settings, you can use the email address registered to the LDAP server.

1. Access Web Config and select the **Network** tab > **LDAP Server** > **Search Settings**.
2. Enter a value for each item.
3. Click **OK** to display the setting result.

   The settings you have selected are displayed.

LDAP Server Search Settings

Items	Settings and Explanation
Search Base (Distinguished Name)	If you want to search an arbitrary domain, specify the domain name of the LDAP server. Enter between 0 and 128 characters in Unicode (UTF-8). If you do not search for arbitrary attribute, leave this blank. Example for the local server directory: dc=server,dc=local
Number of search entries	Specify the maximum number of search results to return (between 5 and 500). If the number of search results returned exceeds the maximum value specified, a warning message is displayed and some server entries may be excluded from the search. Refine your search criteria to reduce the number of search results and ensure that all server entries are included in the search.
User name Attribute	Specify the attribute name to display when searching for user names. Enter between 1 and 255 characters in Unicode (UTF-8). The first character should be a-z or A-Z. Example: cn, uid
User name Display Attribute	Specify the attribute name to display as the user name. Enter between 0 and 255 characters in Unicode (UTF-8). The first character should be a-z or A-Z. Example: cn, sn

Items	Settings and Explanation
Email Address Attribute	Specify the attribute name to display when searching for email addresses. Enter a combination of between 1 and 255 characters using A-Z, a-z, 0-9, and -. The first character should be a-z or A-Z. Example: mail
Arbitrary Attribute 1 - Arbitrary Attribute 4	You can specify other arbitrary attributes to search for. Enter between 0 and 255 characters in Unicode (UTF-8). The first character should be a-z or A-Z. If you do not want to search for arbitrary attributes, leave this blank. Example: o, ou

Checking the LDAP Server Connection

You can perform an LDAP server connection test using the values entered in **LDAP Server** > **Search Settings**.

1. Access Web Config and select the **Network** tab > **LDAP Server** > **Connection Test**.
2. Select **Start**.

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

LDAP Server Connection Test References

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

Using Document Capture Pro Server

By using Document Capture Pro Server, you can manage the sorting method, saving format, and forwarding destination of a scanning result executed from the scanner's control panel. You can call and execute a job previously registered on the server from the scanner's control panel.

Install it on the server computer.

For more information on Document Capture Pro Server, contact your local Epson office.

Setting Server Mode

To use Document Capture Pro Server, set up as follows.

1. Access Web Config and select the **Scan** tab > **Document Capture Pro**.
2. Select **Server Mode** for **Mode**.
3. Enter the address of the server with Document Capture Pro Server installed on it for **Server Address**.

   Enter between 2 and 255 characters in either IPv4, IPv6, host name or FQDN format. For FQDN format, you can use alphanumeric characters in ASCII (0x20-0x7E) and "- " except for at the beginning and end of the address.
4. Click **OK**.

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

Setting Up AirPrint

Access Web Config, select the **Network** tab, then select **AirPrint Setup**.

Items	Explanation
Bonjour Service Name	Enter a Bonjour service name, using ASCII text (0x20-0x7E) and up to 41 characters.
Bonjour Location	Enter a description of the scanner's location, using Unicode (UTF-8) text and up to 127 bytes.
Wide-Area Bonjour	Set whether or not to use Wide-Area Bonjour. If you use it, the scanner must be registered on the DNS server in order to search for the scanner over the segment.
Enable AirPrint	Bonjour and AirPrint (Scan service) are enabled.

Problems when Preparing Network Scanning

Hints to Solving Problems

❏ Checking the error message

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

❏ Checking the communication status

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

❏ Connection test

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

❏ Initializing the settings

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

Cannot Access Web Config

The IP address is not assigned to the scanner.

Solutions

A valid IP address may not be assigned to the scanner. Configure the IP address using the scanner's control panel. You can confirm the current setting information from the scanner's control panel.

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

Solutions

SSL/TLS has the Encryption Strength. You can open Web Config by using a web browser that supports bulk encryptions as indicated below. Check you are using a supported browser.

❏ 80bit: AES256/AES128/3DES

❏ 112bit: AES256/AES128/3DES

❏ 128bit: AES256/AES128

❏ 192bit: AES256

❏ 256bit: AES256

CA-signed Certificate is expired.

Solutions

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

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

Solutions

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

- ❏ The scanner's IP address entered to common name for creating a Self-signed Certificate or CSR
- ❏ IP address entered to web browser when running Web Config

For Self-signed Certificate, update the certificate.

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

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

Solutions

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

- ❏ Windows:

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

- ❏ Mac OS:

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

  Example:

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

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

DHCP is disabled in the computer's settings.

Solutions

If the DHCP for obtaining an IP address automatically is disabled on the computer, you may not be able to access Web Config. Enable DHCP.

Example for Windows 10:

Open the Control Panel and then click **Network and Internet** > **Network and Sharing Center** > **Change adapter settings**. Open the Properties screen of the connection you are using, and then open the properties screen for **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**. Check that **Obtain an IP address automatically** is selected on the displayed screen.

Cannot Send Scanned Images to an Email when Using Microsoft Exchange Online

Cannot sign in or users cannot sign in

Your Entra ID may be blocked by a conditional access policy.

Solution:

Check your conditional access policies with Entra ID.

For detailed instructions, see the "Microsoft Learn" site.

Cannot send email

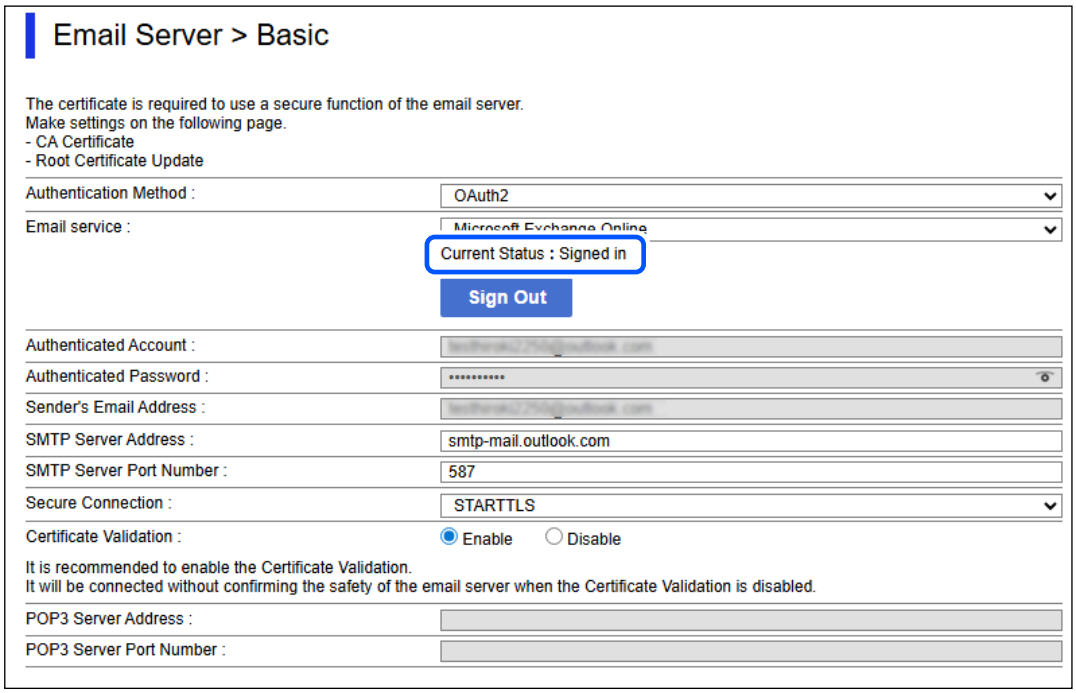
Status:

"To use this function, you must sign in to your email service. Please contact your administrator." is displayed.

Solution:

Check Web Config for the current status.

Select the **Network** tab > **Email Server** > **Basic**



If the **Current Status** is **Signed in**, the sign-in information may not have been saved to the scanner. Click **OK** to send the setting information to the scanner.

If there is no **Current Status** and the **Sign In** button is displayed, sign in.

"Setting Up OAuth2.0 Authentication for the Email Server" on page 45

Status:

The cloud service or email service is not connected, or the connection has expired.

Solution:

Connect to cloud service or email service.

Status:

You need to sign in to cloud service again.

Solution:

Sign in to cloud service.

Expiration message is displayed

A certain period of time has passed since signing in without using the email sending function.

If a scanner using OAuth 2.0 authentication has not been used for an extended period, or the email-sending function has not been used, the access token and refresh token will become invalid.

Solution:

The administrator should perform the sign-in operation again.

"Setting Up OAuth2.0 Authentication for the Email Server" on page 45

Customizing the Control Panel Display

Registering Presets. 80

Editing the Home Screen of the Control Panel. 82

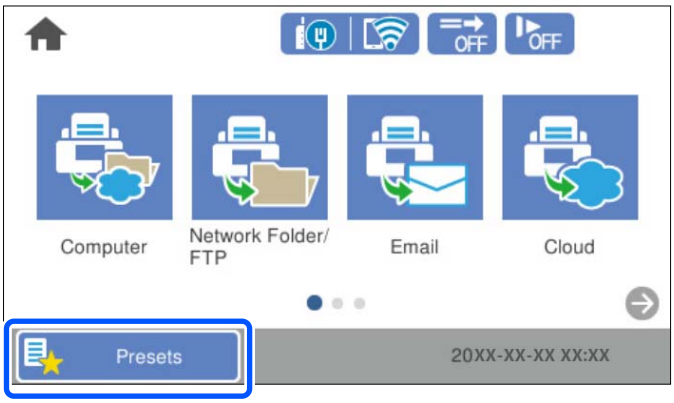
Registering Presets

You can register frequently used scanning setting as **Presets**. You can register up to 48 presets.

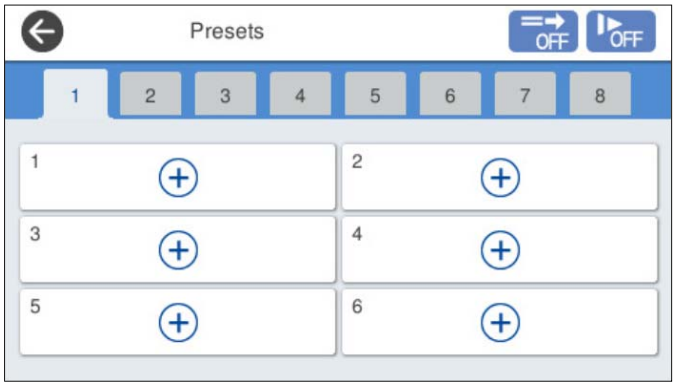
Note:

- *You can register the current settings by selecting ☆ on the start scanning screen.*
- *You can also register **Presets** in Web Config.*
  *Select the **Scan** tab > **Presets**.*
- *If you select **Scan to Computer** when registering, you can register the job created in Document Capture Pro as **Presets**. This is available only for computers connected over a network. Register the job in Document Capture Pro in advance.*
- *If the **Lock Setting** on the control panel is enabled, only the administrator can register **Presets**.*

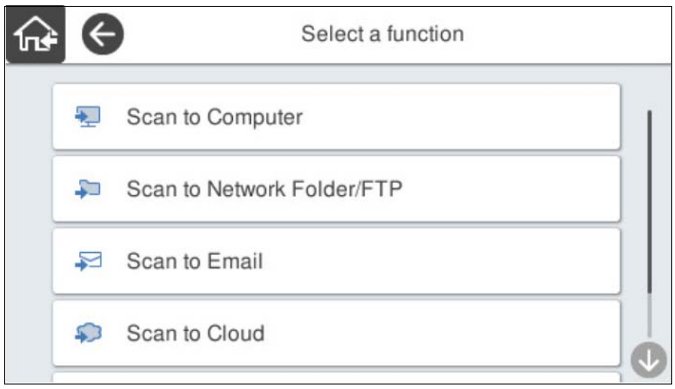
1. Select **Presets** on the home screen on the scanner's control panel.



2. Select ⊕.



3. Select the menu you want to use to register a preset.



4. Set each item, and then select ☆+.

   Note:
   *When you select **Scan to Computer**, select the computer on which Document Capture Pro is installed, and then select a registered job. This is available only for computers connected over a network.*

5. Make the preset settings.

   ❏ **Name**: Set the name.

   ❏ **Set Icon**: Set the image and color of the icon to display.

   ❏ **Quick Send Setting**: Immediately starts scanning without confirmation when the preset is selected.

   When you are using Document Capture Pro Server, even if you set the software to confirm a job's contents before scanning, the **Quick Send Setting** on the scanner's preset takes priority over the software.

   ❏ **Contents**: Check scan settings.

6. Select **OK**.

Menu Options of Presets

You can change the settings of a preset by selecting > in each preset.

Change Name:

Changes the preset name.

Change Icon:

Changes the icon image and color of the preset.

Quick Send Setting:

Immediately starts scanning without confirmation when the preset is selected.

Change Position:

Changes the display order of the presets.

Delete:

Deletes the preset.

Add or Remove Icon on Home:

Adds or deletes the preset icon from the home screen.

Confirm Details:

View the settings of a preset. You can load the preset by selecting **Use This Setting**.

Editing the Home Screen of the Control Panel

You can customize the home screen by selecting **Settings** > **Edit Home** on the scanner's control panel.

- Layout : Changes the display method of the menu icons.
  "Changing the Layout of the Home Screen" on page 82
- Add Icon: Adds icons to the **Presets** settings you have made, or restores icons that have been removed from the screen.
  "Add Icon" on page 83
- Remove Icon : Removes icons from the home screen.
  "Remove Icon" on page 84
- Move Icon : Changes the display order of the icons.
  "Move Icon" on page 85
- Restore Default Icon Display : Restores the default display settings for the home screen.
- Wall Paper : Change the wallpaper color for the home screen.

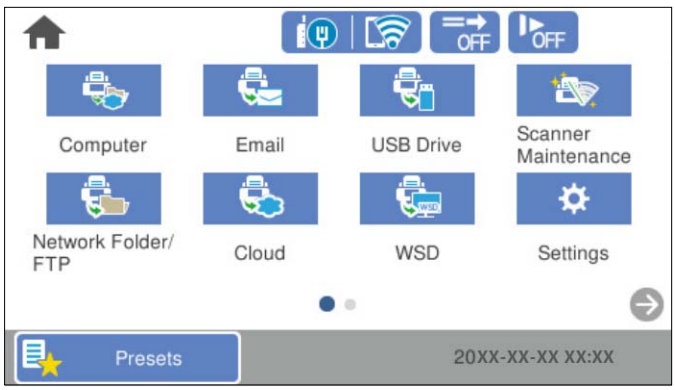
Changing the Layout of the Home Screen

1. Select **Settings** > **Edit Home** > **Layout** on the scanner's control panel.

2. Select **Line** or **Matrix**.

   Line:

   Matrix:



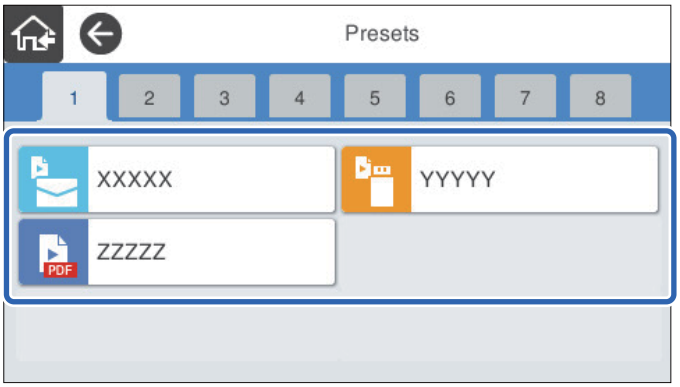
3. Select to return and check the home screen.

Add Icon

1. Select **Settings** > **Edit Home** > **Add Icon** on the scanner's control panel.
2. Select **Function** or **Presets**.
   - ❏ Function: Displays the default functions shown on the home screen.

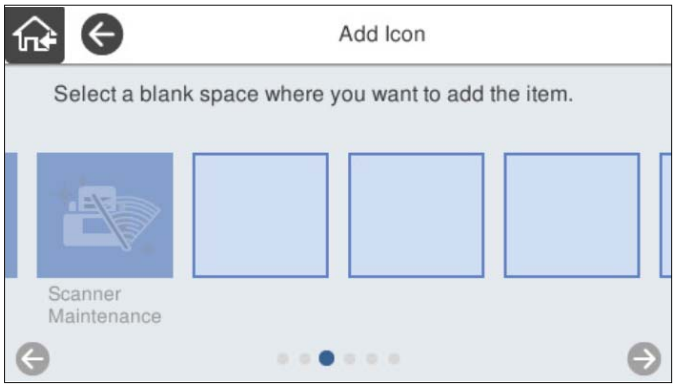
❏ Presets: Displays registered presets.

3. Select the item you want to add to the home screen.



4. Select the blank space where you want to add the item.

   If you want to add multiple icons, repeat steps 3 to 4.

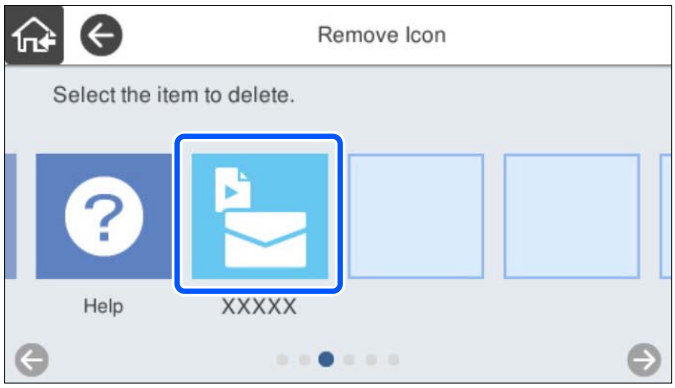


5. Select to return and check the home screen.

Remove Icon

1. Select **Settings** > **Edit Home** > **Remove Icon** on the scanner's control panel.

2. Select the icon you want to remove.



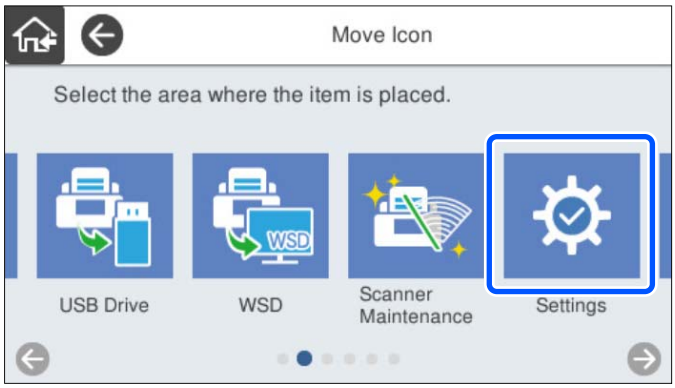
3. Select **Yes** to finish.

   If you want to remove multiple icons, repeat procedure 2 to 3.

4. Select to return and check the home screen.

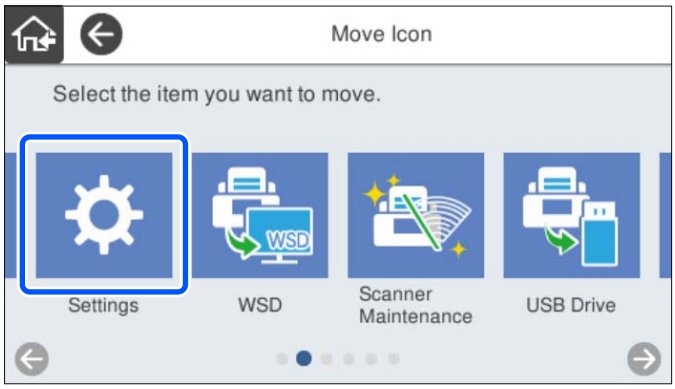
Move Icon

1. Select **Settings** > **Edit Home** > **Move Icon** on the scanner's control panel.
2. Select the icon you want to move.



3. Select the destination frame.

   If another icon is already set in the destination frame, the icons are replaced.



4. Select to return and check the home screen.

Basic Security Settings

Introduction of Product Security Features. 88

Administrator Settings. 88

Disabling the External Interface. 94

Monitoring a Remote Scanner. 95

Solving Problems. 96

Introduction of Product Security Features

This section introduces the security function of the Epson Devices.

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

Related Information

➡ "Configuring the Administrator Password" on page 88
➡ "Disabling the External Interface" on page 94

Administrator Settings

Configuring the Administrator Password

When you set an administrator password, you can prevent users from changing system management settings. The default values are set at the time of purchase. Change them as necessary.

Note:
The following provides the default values for the administrator information.

- *User name (used for Web Config only): None (blank)*
- *Password: Depends on the label attached to the back of the product.*

  If there is a "PASSWORD" label attached to the back, enter the 8-digit number shown on the label.

  If there is no "PASSWORD" label attached, enter the serial number on the label attached to the back of the product for the initial administrator password.

You can change the administrator password using either Web Config, the scanner's control panel, or Epson Device Admin. When using Epson Device Admin, see the Epson Device Admin guide or help.

Changing the Administrator Password Using Web Config

Change the administrator password in Web Config.

1. Access Web Config and select the **Product Security** tab > **Change Administrator Password**.
2. Enter the necessary information in **Current password**, **User Name**, **New Password**, and **Confirm New Password**.

   The new password must be 8 to 20 characters long and only contain single-byte alphanumeric characters and symbols.

   Note:
   The following provides the default values for the administrator information.

   - *User name: none (blank)*
   - *Password: Depends on the label attached to the back of the product.*

     If there is a "PASSWORD" label attached to the back, enter the 8-digit number shown on the label.

     If there is no "PASSWORD" label attached, enter the serial number on the label attached to the back of the product for the initial administrator password.

   Important:
   Be sure to remember the administrator password you set. If you forget your password, you will not be able to reset it and you will need to request help from service personnel.
3. Select **OK**.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Changing the Administrator Password from the Control Panel

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

1. Select **Settings** on the scanner's control panel.
2. Select **System Administration** > **Admin Settings**.
3. Select **Admin Password** > **Change**.
4. Enter your current password.

   Note:
   The initial administrator password (default) at the time of purchase varies depending on the label attached to the back of the product.

   If there is a "PASSWORD" label attached to the back, enter the 8-digit number shown on the label.

   If there is no "PASSWORD" label attached, enter the serial number on the label attached to the back of the product for the initial administrator password.
5. Enter your new password.

   The new password must be 8 to 20 characters long and only contain single-byte alphanumeric characters and symbols.

> ***Important:***
> *Be sure to remember the administrator password you set. If you forget your password, you will not be able to reset it and you will need to request help from service personnel.*

6. Enter the new password again for confirmation.

A completion message is displayed.

Using Lock Setting for the Control Panel

You can use Lock Setting to lock the control panel to prevent users from changing items related to system settings.

Note:
If you enable Authentication Settings on the scanner, Lock Setting is also enabled for the control panel. The control panel cannot be unlocked when Authentication Settings is enabled.

Even if you disable Authentication Settings, Lock Setting remains enabled. If you want to disable it, you can make settings from the control panel or Web Config.

Setting Lock Setting from the Control Panel

1. If you want to cancel the **Lock Setting** once it has been enabled, tap at the top right corner of the Home screen to log in as an administrator.

   is not displayed when **Lock Setting** is disabled. If you want to enable this setting, go to the next step.

2. Select **Settings**.

3. Select **System Administration** > **Admin Settings**.

4. Select **On** or **Off** as the **Lock Setting**.

Setting Lock Setting from Web Config

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

2. Select **ON** or **OFF** for **Panel Lock**.

3. Click **OK**.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Lock Setting items on the Settings Menu

This is a list of items that are locked in the **Settings** menu on the control panel by Lock Setting.

✓: To be locked.

- : Not to be locked.

Settings menu		Lock Setting
Basic Settings		-
	LCD Brightness	-
	Sounds	-
	Sleep Timer	✓
	Power Off Timer	✓
	Date/Time Settings	✓
	Language	✓/-*
	Keyboard (This feature may not be available depending on your region.)	-
	Operation Time Out	✓
	PC Connection via USB	✓
	Direct power on	✓
Scanner Settings		-
	Slow	-
	Double Feed Stop Timing	✓
	DFDS Function	-
	Paper Protection	✓
	Glass Dirt Detection	✓
	Ultrasonic Double Feed Detection	✓
	Automatic Feeding Mode Timeout	✓
	Confirm Recipient	✓
Edit Home		✓
	Layout	✓
	Add Icon	✓
	Remove Icon	✓
	Move Icon	✓
	Restore Default Icon Display	✓
	Wall Paper	✓
User Settings		✓

Settings menu		Lock Setting
	Network Folder/FTP	✓
	Email	✓
	Cloud	✓
	USB Drive	✓
Network Settings		✓
	Wi-Fi Setup	✓
	Wired LAN Setup	✓
	Network Status	✓
	Advanced	✓
Web Service Settings		✓
	Epson Connect Services	✓
Document Capture Pro		-
	Change Settings	✓
Contacts Manager		-
	Register/Delete	✓/-*
	Frequent	-
	View Options	-
	Search Options	-
System Administration		✓
	Contacts Manager	✓
	Admin Settings	✓
	Restrictions	✓
	Password Encryption	✓
	Customer Research	✓
	WSD Settings	✓
	Restore Default Settings	✓
	Firmware Update	✓
Device Information		-

Settings menu			Lock Setting
	Serial Number		-
	Current Version		-
	Total Number of Scans		-
	Number of 1-Sided Scans		-
	Number of 2-Sided Scans		-
	Number of Scans of Carrier Sheet		-
	Number of Scans After Replacing Roller		-
	Number of Scans After Regular Cleaning		-
	Reset the Number of Scans		✓
Scanner Maintenance			-
	Roller Cleaning		-
	Roller Replacement		-
		Reset the Number of Scans	✓
		How to Replace	-
	Regular Cleaning		-
		Reset the Number of Scans	✓
		How to Clean	-
	Glass Cleaning		-
Roller Replacement Alert Setting			✓
	Count Alert Setting		✓
Regular Cleaning Alert Settings			✓
	Warning Alert Setting		✓
	Count Alert Setting		✓

* You can set whether or not to allow changes in **System Administration** > **Restrictions**.

Logging in as an Administrator from the Control Panel

You can use any of the following methods to log in as an administrator from the scanner's control panel.

1. Tap at the top right of the screen.
   - ❏ When Authentication Settings is enabled, the icon is displayed on the **Welcome** screen (the authentication standby screen).
   - ❏ When Authentication Settings is disabled, the icon is displayed on the Home screen.

2. Tap **Yes** when the confirmation screen is displayed.
3. Enter the administrator's password.

   A login complete message is displayed, and then the Home screen on the control panel is displayed.

To logout, tap at the top right of the Home screen.

Disabling the External Interface

You can disable the interface that is used to connect the device to the scanner. Make the restriction settings to restrict scanning other than via network.

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

*PC Connection via USB : **Settings** > **Basic Settings** > **PC Connection via USB***

1. Access Web Config and select the **Product Security** tab > **External Interface**.
2. Select **Disable** on the functions you want to set.

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

   PC Connection via USB

   You can restrict the usage of the USB connection from the computer. If you want to restrict it, select **Disable**.
3. Click **OK**.
4. Check that the disabled port cannot be used.

   PC Connection via USB

   If the driver was installed on the computer

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

   If the driver was not installed on the computer

   Windows:

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

   Mac OS:

   Connect the scanner to the computer using a USB cable, and then confirm that you cannot add the scanner from **Printers & Scanners**.

Related Information

➡ “Running Web Config on a Web Browser” on page 37

Monitoring a Remote Scanner

Checking Information for a Remote Scanner

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

❏ Product Status

Check the status, cloud service, product number, MAC address, etc.

❏ Network Status

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

❏ Usage Status

Check the first day of scanning, scanning count, etc.

❏ Hardware Status

Check the status of each function of the scanner.

❏ Panel Snapshot

Displays a snapshot of the screen displayed on the scanner's control panel.

Receiving Email Notifications When Events Occur

About Email Notifications

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

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

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

Related Information

➡ "Registering an Email Server" on page 44

Configuring Email Notification

Configure email notification by using Web Config.

1. Access Web Config and select the **Device Management** tab > **Email Notification**.
2. Set the subject of email notification.

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

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

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

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

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

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

4. Select the language for the email notifications.

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

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

   Example :

   If you want to send a notification to the email address set for number 1 in **Email Address Settings** when the admin password is changed, select the check box for column **1** on the line **Administrator password changed**.

6. Click **OK**.

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

   Example : The administrator password has been changed.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Items for Email Notification

Items	Settings and Explanation
Administrator password changed	Notice when administrator password has been changed.
Scanner error	Notice when the scanner error has occurred.
Wi-Fi failure	Notice when the error of the wireless LAN interface has occurred.

Solving Problems

Forgot Your Administrator's Password

You need help from service personnel. Contact your local dealer.

Note:
The following provides the initial values for the Web Config administrator.

- *User name: none (blank)*
- *Password: Depends on the label attached to the back of the product.*

  If there is a "PASSWORD" label attached to the back, enter the 8-digit number shown on the label.

  If there is no "PASSWORD" label attached, enter the serial number on the label attached to the back of the product for the initial administrator password.

If you restore the administrator password, it is reset to the initial value at the time of purchase.

Advanced Security Settings

Security Settings and Prevention of Danger. 98

Controlling Using Protocols. 99

Using a Digital Certificate. 102

SSL/TLS Communication with the Scanner. 107

Encrypted Communication Using IPsec/IP Filtering. 108

Connecting the Scanner to an IEEE802.1X Network. 119

Solving Problems for Advanced Security. 121

Security Settings and Prevention of Danger

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

For scanners that do not have access protection from the outside, it will be possible to read the contacts that are stored in the scanner from the Internet.

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

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

Related Information

- "Controlling Using Protocols" on page 99
- "SSL/TLS Communication with the Scanner" on page 107
- "Encrypted Communication Using IPsec/IP Filtering" on page 108
- "Connecting the Scanner to an IEEE802.1X Network" on page 119

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.

Make sure you configure the administrator password before setting IPsec/IP filtering or IEEE802.1X.

Controlling Using Protocols

You can scan using a variety of pathways and protocols. Also, you can use network scanning from an unspecified number of network computers.

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

Controlling protocols

Configure the protocol settings supported by the scanner.

1. Access Web Config and then select the **Network Security** tab > **Protocol**.
2. Configure each item.
3. Click **Next**.
4. Click **OK**.

   The settings are applied to the scanner.

Related Information

➡ "Running Web Config on a Web Browser" 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, etc.
SLP Settings	You can enable or disable the SLP function. SLP is used for push scanning 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, and 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, etc.

Protocol	Description
SNMPv3 Settings	You can specify whether or not to enable SNMPv3. This is used to set up encrypted devices, monitoring, etc.

Protocol Setting Items

Bonjour Settings

Items	Setting value and Description
Use Bonjour	Select this to search for or use devices through Bonjour.
Bonjour Name	Displays the Bonjour name.
Bonjour Service Name	Displays the Bonjour service name.
Location	Displays the Bonjour location name.
Wide-Area Bonjour	Set whether to use Wide-Area Bonjour.

SLP Settings

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

WSD Settings

Items	Setting value and Description
Enable WSD	Select this to enable adding devices using WSD 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

Items	Setting value and Description
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

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

SNMPv1/v2c Settings

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

SNMPv3 Settings

Items		Setting value and Description
Enable SNMPv3		SNMPv3 is enabled when the box is checked.
User Name		Enter between 1 and 32 characters using 1 byte characters.
Authentication Settings		
	Algorithm	Select an algorithm for an authentication for SNMPv3.
	Password	Enter the password for an authentication for SNMPv3. Enter between 8 and 32 characters in ASCII (0x20-0x7E). If you do not specify this, leave it blank.
	Confirm Password	Enter the password you configured for confirmation.
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.

Using a Digital Certificate

About Digital Certification

❏ CA-signed Certificate

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

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

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

❏ CA Certificate

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

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

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

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

❏ Self-signed Certificate

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

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

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

Related Information

➡ "Configuring a CA-signed Certificate" on page 102

➡ "Updating a Self-signed Certificate" on page 106

➡ "Configuring a CA Certificate" on page 106

Configuring a CA-signed Certificate

Obtaining a CA-signed Certificate

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

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

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

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

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

   A CSR creating page is opened.

3. Enter a value for each item.

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

4. Click **OK**.

   A completion message is displayed.

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

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

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

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

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

8. Save the issued CA-signed Certificate to a computer connected to the scanner.

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

Related Information

➡ "Running Web Config on a Web Browser" on page 37

CSR Setting Items

Items	Settings and Explanation
Key Length	Select a key length for a CSR.
Common Name	You can enter between 1 and 128 characters. If this is an IP address, it should be a static IP address. You can enter 1 to 5 IPv4 addresses, IPv6 addresses, host names, FQDNs by separating them with commas. The first element is stored to the common name, and other elements are stored to the alias field of the certificate subject. Example: Scanner's IP address : 192.0.2.123, Scanner name : EPSONA1B2C3 Common Name : EPSONA1B2C3, EPSONA1B2C3.local, 192.0.2.123

Items	Settings and Explanation
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.
Sender's Email Address	You can enter the sender's email address for the mail server setting. Enter the same email address as the **Sender's Email Address** for the **Network** tab > **Email Server** > **Basic**.

Importing a CA-signed Certificate

Import the obtained CA-signed Certificate to the scanner.

Important:

- ❏ *Make sure that the scanner's date and time is set correctly or the certificate may be invalid.*
- ❏ *If you obtain a certificate using a CSR created from Web Config, you can import a certificate one time.*

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

   A certificate importing page is opened.
3. Enter a value for each item. Set **CA Certificate 1** and **CA Certificate 2** when verifying the path of the certificate on the web browser that accesses the scanner.

   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

➡ "Running Web Config on a Web Browser" on page 37

CA-signed Certificate Importing Setting Items

Items	Settings and Explanation
Server Certificate or Client Certificate	Select a certificate's format. For SSL/TLS connection, the Server Certificate is displayed. For IPsec/IP Filtering or IEEE802.1x, the Client Certificate is displayed.
Private Key	If you obtain a certificate of the PEM/DER format by using a CSR created from a computer, specify a private key file that matches a certificate.
Password	If the file format is **Certificate with Private Key (PKCS#12)**, enter the password for encrypting the private key that is set when you obtain the certificate.
CA Certificate 1	If your certificate's format is **Certificate (PEM/DER)**, import a certificate of a certificate authority that issues a CA-signed Certificate used as server certificate. Specify a file if you need.
CA Certificate 2	If your certificate's format is **Certificate (PEM/DER)**, import a certificate of a certificate authority that issues CA Certificate 1. Specify a file if you need.

Deleting a CA-signed Certificate

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

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

1. Access Web Config, and then select the **Network Security** tab. Next, select **SSL/TLS** > **Certificate** or **IPsec/IP Filtering** > **Client Certificate** or **IEEE802.1X** > **Client Certificate**.
2. Click **Delete**.
3. Confirm that you want to delete the certificate in the message displayed.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Updating a Self-signed Certificate

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

1. Access Web Config and select the **Network Security** tab > **SSL/TLS** > **Certificate**.
2. Click **Update**.
3. Enter **Common Name**.

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

   Example:

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

   Common name : EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. Specify a validity period for the certificate.
5. Click **Next**.

   A confirmation message is displayed.
6. Click **OK**.

   The scanner is updated.

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

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Configuring a CA Certificate

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

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

Importing a CA Certificate

Import the CA Certificate to the scanner.

1. Access Web Config and then select the **Network Security** tab > **CA Certificate**.
2. Click **Import**.
3. Specify the CA Certificate you want to import.
4. Click **OK**.

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

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Deleting a CA Certificate

You can delete the imported CA Certificate.

1. Access Web Config and then select the **Network Security** tab > **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.
4. Click **Reboot Network**, and then check that the deleted CA Certificate is not listed on the updated screen.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

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.

Configuring Basic SSL/TLS Settings

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

Configure encryption strength and redirect feature.

1. Access Web Config and select the **Network Security** tab > **SSL/TLS** > **Basic**.
2. Select a value for each item.
   - ❏ Encryption Strength
     Select the level of encryption strength.
   - ❏ Redirect HTTP to HTTPS
     Redirect to HTTPS when HTTP is accessed.
3. Click **Next**.
   A confirmation message is displayed.

4. Click **OK**.

   The scanner is updated.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Configuring a Server Certificate for the Scanner

1. Access Web Config and select the **Network Security** tab > **SSL/TLS** > **Certificate**.
2. Specify a certificate to use on **Server Certificate**.
   - ❏ Self-signed Certificate

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

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

   A confirmation message is displayed.
4. Click **OK**.

   The scanner is updated.

Related Information

➡ "Running Web Config on a Web Browser" on page 37
➡ "Configuring a CA-signed Certificate" on page 102
➡ "Configuring a CA Certificate" on page 106

Encrypted Communication Using IPsec/IP Filtering

About IPsec/IP Filtering

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

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

Configuring Default Policy

To filter traffic, configure the default policy. The default policy applies to every user or group connecting to the scanner. For more fine-grained control over users and groups of users, configure group policies.

1. Access Web Config and then select the **Network Security** tab > **IPsec/IP Filtering** > **Basic**.
2. Enter a value for each item.
3. Click **Next**.

   A confirmation message is displayed.
4. Click **OK**.

   The scanner is updated.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Default Policy Setting Items

Default Policy

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

❏ **Access Control**

Configure a control method for traffic of IP packets.

Items	Settings and Explanation
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**.

Items	Settings and Explanation
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**.

Items		Settings and Explanation
Local	Authentication Method	To select **Certificate**, you need to obtain and import a CA-signed certificate in advance.
	ID Type	If you select **Pre-Shared Key** for **Authentication Method**, select the type of ID for the 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 255 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 255 1-byte ASCII (0x20 to 0x7E) characters. You need to include "@". **Key ID** : Enter 1 to 255 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.

Items		Settings and Explanation
Remote	Authentication Method	To select **Certificate**, you need to obtain and import a CA-signed certificate in advance.
	ID Type	If you select **Pre-Shared Key** for **Authentication Method**, select the type of ID for the device that you want to authenticate.
	ID	Enter the scanner's ID that matches the type of ID. You cannot use "@", "#", and "=" for the first character. **Distinguished Name** : Enter 1 to 255 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 255 1-byte ASCII (0x20 to 0x7E) characters. You need to include "@". **Key ID** : Enter 1 to 255 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.

Items	Settings and Explanation
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

If you select **IPsec** for **Access Control**, select an option.

Items	Settings and Explanation
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**

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

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

Configuring Group Policy

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.

1. Access Web Config and then select the **Network Security** tab > **IPsec/IP Filtering** > **Basic**.
2. Click a numbered tab you want to configure.
3. Enter a value for each item.
4. Click **Next**.

   A confirmation message is displayed.
5. Click **OK**.

   The scanner is updated.

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.

Items	Settings and Explanation
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**.

Note:
If an IPv6 address is assigned automatically, the connection may be unavailable. Configure a static IPv6 address.

Remote Address(Host)

Enter a device's IP address to control access. The IP address must be 43 characters or less. If you do not enter an IP address, all addresses are controlled.

Note:
If an IP address is assigned automatically (e.g., assigned by DHCP), the connection may be unavailable. Configure a static IP address.

Method of Choosing Port

Select a method to specify ports.

❏ Service Name

If you select **Service Name** for **Method of Choosing Port**, select an option.

❏ Transport Protocol

If you select **Port Number** for **Method of Choosing Port**, you need to configure an encapsulation mode.

Items	Settings and Explanation
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**.

Items	Settings and Explanation
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**.

Items		Settings and Explanation
Local	Authentication Method	If you select **IPsec** for **Access Control**, select an option. Used certificate is common with a default policy.
	ID Type	If you select **Pre-Shared Key** for **Authentication Method**, select the type of ID for the 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 255 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 255 1-byte ASCII (0x20 to 0x7E) characters. You need to include "@". **Key ID** : Enter 1 to 255 1-byte ASCII (0x20 to 0x7E) characters.
	Pre-Shared Key	If you select **Pre-Shared Key** for **Authentication Method**, enter a pre-shared key between 1 and 127 characters.
	Confirm Pre-Shared Key	Enter the key you configured for confirmation.
Remote	Authentication Method	If you select **IPsec** for **Access Control**, select an option. Used certificate is common with a default policy.
	ID Type	If you select **Pre-Shared Key** for **Authentication Method**, select the type of ID for the device that you want to authenticate.
	ID	Enter the scanner's ID that matches the type of ID. You cannot use "@", "#", and "=" for the first character. **Distinguished Name** : Enter 1 to 255 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 255 1-byte ASCII (0x20 to 0x7E) characters. You need to include "@". **Key ID** : Enter 1 to 255 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.

Items	Settings and Explanation
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

If you select **IPsec** for **Access Control**, select an option.

Items	Settings and Explanation
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

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

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

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.

*3 Except IPv6 link local addresses.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

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 Epson Device Admin and the a scanner driver
SNMP	UDP	161	Any port	Acquiring and configuring MIB from applications such as Epson Device Admin and the Epson scanner driver
WSD	TCP	Any port	5357	Controlling WSD
WS-Discovery	UDP	3702	Any port	Searching for WSD scanners
Network Scan	TCP	1865	Any port	Forwarding scanned data from Document Capture Pro
Network Push Scan	TCP	Any port	2968	Acquiring job information for push scanning from Document Capture Pro
Network Push Scan Discovery	UDP	2968	Any port	Searching for a computer from scanner
FTP Data (Remote)	TCP	Any port	20	FTP client (forwarding scanned data) However this can control only an FTP server that uses remote port number 20.
FTP Control (Remote)	TCP	Any port	21	FTP client (controlling forwarded scanned data)
CIFS (Remote)	TCP	Any port	445	CIFS client (forwarding scanned data to a folder)

Service name	Protocol type	Local port number	Remote port number	Features controlled
NetBIOS Name Service (Remote)	UDP	Any port	137	CIFS client (forwarding scanned data to a folder)
NetBIOS Datagram Service (Remote)	UDP	Any port	138	
NetBIOS Session Service (Remote)	TCP	Any port	139	
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 (updating the firmware and the root certificate)
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: Do not configure.

Receiving scanning data 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**, **HTTP (Local)**, **HTTPS (Local)** and **Network Scan**.

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

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

   If you have already imported a certificate published by a Certification Authority, 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

➡ "Running Web Config on a Web Browser" on page 37
➡ "Configuring a CA-signed Certificate" on page 102
➡ "Configuring a CA Certificate" on page 106

Connecting the Scanner to an IEEE802.1X Network

Configuring an IEEE802.1X Network

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

1. Access Web Config and then select the **Network Security** tab > **IEEE802.1X** > **Basic**.
2. Enter a value for each item.

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

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

3. Click **Next**.

   A confirmation message is displayed.

4. Click **OK**.

   The scanner is updated.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

IEEE802.1X Network Setting Items

Items	Settings and Explanation	
IEEE802.1X (Wired LAN)	You can enable or disable settings of the page (**IEEE802.1X** > **Basic**) for IEEE802.1X (Wired LAN).	
IEEE802.1X (Wi-Fi)	The connection status of IEEE802.1X (Wi-Fi) is displayed.	
Connection Method	The connection method of a current network is displayed.	
EAP Type	Select an option for an authentication method between the 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.
	EAP-TTLS	
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**.	
Anonymous Name	If you select **PEAP-TLS** or **PEAP/MSCHAPv2** for **EAP Type**, 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

Configuring a Certificate for IEEE802.1X

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

1. Access Web Config and then select the **Network Security** tab > **IEEE802.1X** > **Client Certificate**.
2. Enter a certificate in the **Client Certificate**.

   If you have already imported a certificate published by a Certification Authority, you can copy the certificate and use it in IEEE802.1X. To copy, select the certificate from **Copy From**, and then click **Copy**.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Solving Problems for Advanced Security

Restoring the Security Settings

When you establish a highly secure environment such as IPsec/IP Filtering, 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 Web Config

You can disable IPsec/IP Filtering using Web Config.

1. Access Web Config and select the **Network Security** tab > **IPsec/IP Filtering** > **Basic**.
2. Disable the **IPsec/IP Filtering**.

Problems Using Network Security Features

Forgot a Pre–shared Key

Re-configure a pre-shared key.

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

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

Related Information

➡ "Running Web Config on a Web Browser" on page 37
➡ "Encrypted Communication Using IPsec/IP Filtering" on page 108

Cannot Communicate with IPsec Communication

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

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

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

*available for IKEv2 only

Related Information

➡ "Encrypted Communication Using IPsec/IP Filtering" on page 108

Cannot Communicate Suddenly

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

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

Use a static IP address.

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

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

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

Use a static IP address.

Related Information

➡ "Running Web Config on a Web Browser" on page 37
➡ "Encrypted Communication Using IPsec/IP Filtering" on page 108

Cannot Connect After Configuring IPsec/IP Filtering

The settings of IPsec/IP Filtering are 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 108

Cannot Access the Scanner after Configuring IEEE802.1X

The settings of IEEE802.1X are incorrect.

Disable IEEE802.1X and Wi-Fi 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 119

Problems on Using a Digital Certificate

Cannot Import a CA-signed Certificate

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

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

❏ Are you trying to import the certificate to a device that does not have the same information?
Check the information of the CSR and then import the certificate to a device that has the same information.

❏ Did you overwrite the CSR saved into the scanner after sending the CSR to a certificate authority?
Obtain the CA-signed certificate again with the CSR.

CA-signed Certificate is more than 5KB.

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

The password for importing the certificate is incorrect.

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

Related Information

➡ "Importing a CA-signed Certificate" on page 104

Cannot Update a Self-Signed Certificate

The Common Name has not been entered.

Common Name must be entered.

Unsupported characters have been entered to Common Name.

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

A comma or space is included in the common name.

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

Related Information

➡ "Updating a Self-signed Certificate" on page 106

Cannot Create a CSR

The Common Name has not been entered.

The **Common Name** must be entered.

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

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

A comma or space is included in the Common Name.

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

Related Information

➡ "Obtaining a CA-signed Certificate" on page 102

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**.

Messages	Cause/What to do
CA Certificate 1 is not entered.	**Cause:** CA certificate 1 is not entered and only CA certificate 2 is entered. **What to do:** Import CA certificate 1 first.
Invalid value below.	**Cause:** Unsupported characters are contained in the file path and/or password. **What to do:** Make sure that the characters are entered correctly for the item.
Invalid date and time.	**Cause:** Date and time for the 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.
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.

Messages	Cause/What to do
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.
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

➡ "About Digital Certification" on page 102

Delete a CA-signed Certificate by Mistake

There is no backup file for the CA-signed certificate.

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

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

Related Information

➡ "Importing a CA-signed Certificate" on page 104
➡ "Deleting a CA-signed Certificate" on page 105

Authentication Settings

About Authentication Settings. 128

About Authentication Method. 129

Software for Setting Up. 131

Updating the Scanner's Firmware. 131

Connecting and Configuring an Authentication Device. 131

Registering and Setting Information. 136

Job History Reports Using Epson Device Admin. 151

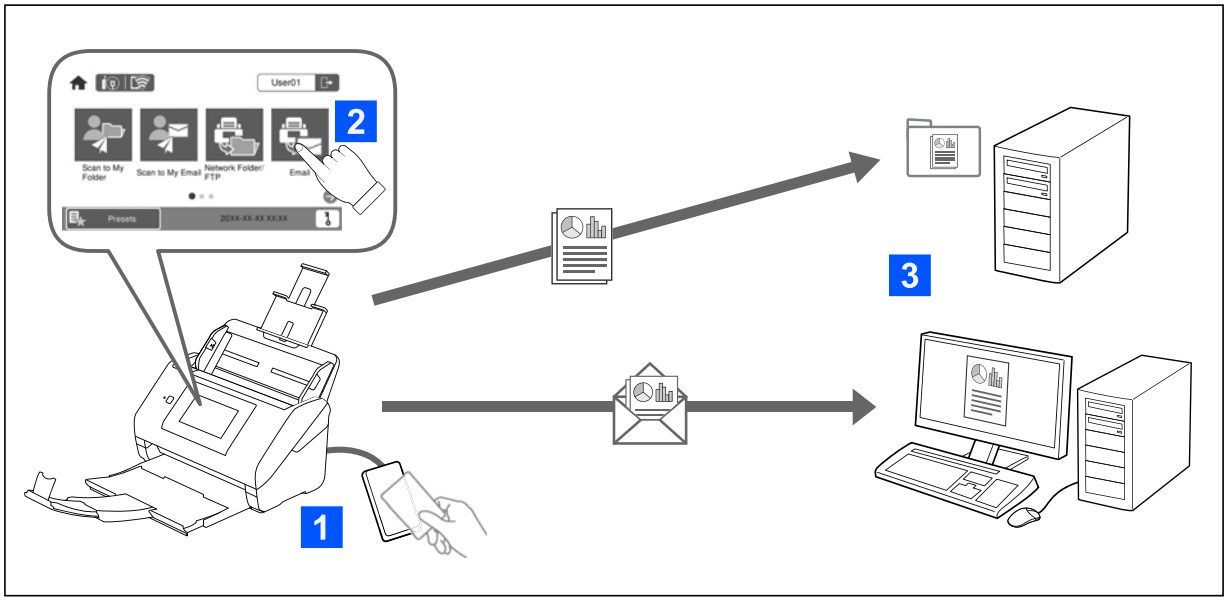
Logging in as an Administrator from the Control Panel. 151

Disabling Authentication Settings. 152

Deleting Authentication Settings Information (Restore Default Settings). 152

Solving Problems. 153

About Authentication Settings



When Authentication Settings is enabled, user authentication is required to start scanning. You can set the scanning methods that can be used by each user, and prevent accidental operations.

You can specify the authenticated user's email address as the scanning destination (Scan to My Email), or save each user's data to a personal folder (Scan to My Folder). You can also specify other scanning methods.

Note:

❏ *You cannot scan from a computer or a smart device when Authentication Settings is enabled.*

❏ *In addition to the Authentication Settings introduced in this manual, you can also build an authentication system using an authentication server. To build a system, use Document Capture Pro Server Authentication Edition (the abbreviated name is Document Capture Pro Server AE). For further information, contact your local Epson office.*

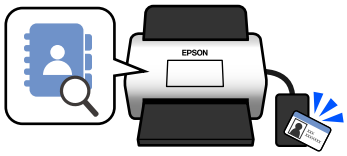
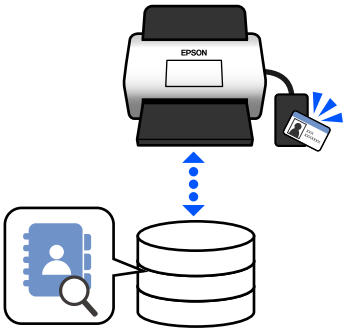
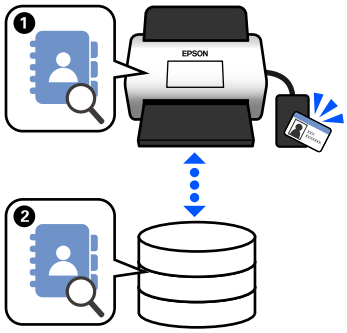
Available Functions for Authentication Settings

Scanning Function on the Control Panel	Authentication Settings	
	When enabled	When disabled
Scan to My Folder Saves images to the folder assigned to the authenticated user.	✓	-
Scan to My Email Sends images to the email address of the authenticated user.	✓	-
Scan to Network Folder/FTP Saves images to a folder on the network.	✓	✓
Scan to Computer Saves images to a connected computer using jobs created in Document Capture Pro (Windows)/Document Capture (Mac OS). *When Authentication Settings is enabled, you can only use jobs registered in **Presets**.	✓*	✓

Scanning Function on the Control Panel	Authentication Settings	
	When enabled	When disabled
Scan to Email Sends images to the email address you set.	✓	✓
Scan to Cloud Sends images to the cloud service you set.	✓	✓
Scan to USB Drive Saves images to a USB drive connected to the scanner. This is available only when no authentication device is connected to the scanner.	✓	✓
Scan to WSD Saves images to a connected computer using the WSD feature.	-	✓
Presets You can register up to 48 preset scanning functions. You can allocate up to five Presets to users registered in the Local DB. Allocated Presets are available only for that user. Presets that have not been allocated to any user can be used by all users.	✓	✓

About Authentication Method

This scanner can provide authentication using the following methods without having to build an authentication server.

	Local DB	LDAP	Local DB and LDAP
User information location	**Scanner's memory** This authentication method checks the user information registered to the scanner and compares it with the user who is using the scanning function.	**LDAP server*** This authentication method checks the user information of the LDAP server synchronized with the scanner. Since up to 300 items of user information from the LDAP server can be temporarily stored in the scanner as a cache, authentication can be performed using the cache if the LDAP server goes down. *A server that provides a directory service that can communicate with LDAP.	**Scanner's memory and LDAP server** Check the user information registered in the scanner first (❶), and if there is no match, check the user information against the LDAP server (❷).
			
Number of registered users	50 (scanner's memory)	Unlimited (LDAP server)	50 (scanner's memory) Unlimited (LDAP server)
Scanner's memory cache	-	300	Max 300 (50 of the cache slots are shared with User Settings in Local DB)
Login methods	You can use any of the following methods. ❏ Hold up an authentication card, or enter a **User ID** and **Password** ❏ Hold up an authentication card, or enter an **ID Number** ❏ Enter a **User ID** and **Password** ❏ Enter a **User ID** ❏ Enter an **ID Number**		
Limits of the "Scan to" feature	Set individually for each user	Same settings for all LDAP users	Local DB users: Set individually LDAP users: Same settings for all users
Allocating Presets to users	Up to 5 per user	- (Cannot be set individually)	Local DB users: Up to 5 per user LDAP users: -

Software for Setting Up

Set up using Web Config or Epson Device Admin.

❏ When you use Web Config, you can set up the scanner only by using a web browser.
"Web Config" on page 37

❏ When you use Epson Device Admin, you can set up multiple scanners at once using a configuration template.
"Epson Device Admin" on page 38

Updating the Scanner's Firmware

Before enabling Authentication Settings, update the scanner's firmware to the latest version. Connect the scanner to the Internet in advance.

> ***Important:***
> *Do not turn off the computer or the scanner while updating.*

When setting up from Web Config:

Select the **Device Management** tab > **Firmware Update**, and then follow the on-screen instructions to update the firmware.

When setting up from Epson Device Admin:

Select **Home** > **Firmware** > **Update** on the device list screen, and then follow the on-screen instructions to update the firmware.

Note:
If the latest firmware is already installed, you do not need to update.

Connecting and Configuring an Authentication Device

If you want to connect and use an authentication device such as an IC card reader, you first need to configure the device. This is not necessary if you are not using an authentication device.

Related Information

➡ "Connecting Authentication Device" on page 134
➡ "Authentication Device Settings" on page 135

Card Reader Compatible List

This list does not guarantee operations for the card readers in the list.

Yes: Supported (The ID information can be read with standard card reader settings.)

No: Not Compatible

Maker	Model	Model Number	Authentication card							Mode
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Yes	Yes*1	Yes*1	Yes*1	No	No	No	Keyboard
RF IDEAS	pcProx	RDR-7081BKU	Yes*1	No	Yes	Yes	No	No	No	Keyboard
RF IDEAS	pcProx	RDR-7581AKU	Yes	No	Yes*1	Yes*1	No	No	No	Keyboard
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	No	No	Yes	Yes	No	No	No	Keyboard
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Yes	No	Yes	Yes	Yes	Yes	Yes	Keyboard
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Keyboard
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Keyboard
ELATEC	TWN4 Slim	T4QC-FC3B7	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Keyboard
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Yes	Yes	Yes	Yes	Yes	No	Yes	Keyboard*1
ACS	ACR122U	ACR122U	No	No	Yes*2	Yes*2	Yes	No	Yes*2	PC/SC

Maker	Model	Model Number	Authentication card							Mode
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ACS	ACR1252	ACR1252	No	No	Yes*2	Yes*2	Yes	Yes	Yes*2	PC/SC
Sony	PaSoRi	RC-S330/S	No	No	Yes*2	Yes*2	Yes*2	Yes*2	Yes*2	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	No	No	Yes*2	Yes*2	Yes*2	Yes*2	Yes*2	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Keyboard
DMZ	Leitor RFID Multi-125	DMZ087	No	Yes	No	No	No	No	No	Keyboard
DMZ	Leitor RFID Mifare	DMZ088	No	No	Yes	Yes	No	No	No	Keyboard
DMZ	Biometric & RFID Reader	DMZ073	No	Yes	No	No	No	No	No	Keyboard
inepro	SCR708	SCR708	Yes*1	Yes*1	Yes*1	Yes*1	Yes*1	Yes*1	Yes*1	Keyboard
Y Soft	YU030888 001	MU0388	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Keyboard
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	No	No	Yes	Yes	No	No	Yes	Keyboard
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	No	No	Yes	Yes	No	No	Yes	Keyboard

Maker	Model	Model Number	Authentication card							Mode
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (Type B) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
NT-ware	MiCard Multi-Tech4-PI	T4DT-FB4WUF-PI	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Keyboard
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Yes*1	Yes*1	Yes*1	Yes*1	No	No	No	Keyboard
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Yes	Yes	Yes	Yes	Yes	Yes	No	Keyboard

*1 You need to change the settings of the card reader by using the proprietary software provided by the card reader maker.

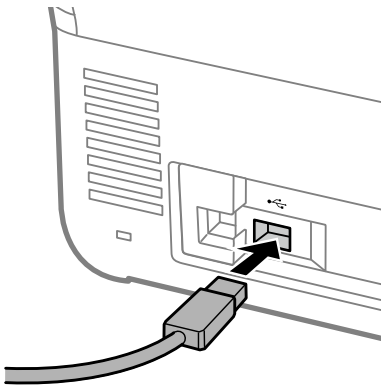
*2 If you need to use data in a particular area in the card other than the standard ID of the card as an authentication ID by configuring product settings, please contact your Epson partner or local representative for more information about a way to set up the product.

Connecting Authentication Device

Important:

When you connect the authentication device to multiple scanners, use a product with the same model number.

Connect the card reader's USB cable to the external interface USB port on the scanner.



Operation Check for Authentication Device

You can check the connection status and authentication card recognition for the authentication device from the scanner's control panel.

Information is displayed if you select **Settings** > **Device Information** > **Authentication Device Status**.

Authentication Device Settings

Set the reading format for authentication information received from an authenticate card.

You can set the following reading method for the authentication device.

❏ Read the particular area of the authentication card, such as employee number or personal ID.

❏ Use the authentication card information except for the UID (authentication card information such as the serial number.)

You can use a tool to generate the operational parameters. Ask your dealer for details.

Note:
Using authentication cards from different manufacturers:

When using UID card information (card ID information such as the serial number), you can use a mix of different types of authentication cards. This cannot be mixed when using other card information.

When setting up from Web Config:

Select the **Device Management** tab > **Card Reader**.

When setting up from Epson Device Admin:

Select **Administrator Settings** > **Authentication Settings** > **Card Reader** from the configuration template.

Item	Explanation
Vendor ID	Set the vendor ID of the authentication device that limits use from 0000 to FFFF by using 4 alphanumeric characters. If you do not want to limit it, set to 0000.
Product ID	Set the product ID of the authentication device that limits use from 0000 to FFFF by using 4 alphanumeric characters. If you do not want to limit it, set to 0000.
Operational parameter	Set the operation parameter of the authentication device between 0 and 8192 characters. A~Z, a~z, 0~9, +, /, =,space, and line feed are available.
Card Reader	Select the conversion format for authentication device. You can check the format details. See the link provided in the item description.
Authentication Card ID save format	Select the conversion format for authentication information of an ID card. You can check the format details. See the link provided in the item description.
Set card ID range	Enable specification of the reading position.
Text Start Position	Specify the text start position for reading the ID information. You can specify between 1 and 4096.
Number of Characters	Specify the number of characters to be read from the start position of the ID information. You can specify between 1 and 4096.

Registering and Setting Information

Setting Up

Make the necessary settings depending on the Authentication Method and the scanning method you use.

Important:

Before starting the setup, check that the time setting for the scanner is correct.

If the time setting is incorrect, the error message "License is expired" is displayed, which may lead to failure to set up the scanner. Also, in order to use a security function such as SSL/ TLS communication or IPsec, the correct time must be set. You can set the time as follows.

- ❏ *Web Config:* ***Device Management*** *tab >* ***Date and Time*** *>* ***Date and Time****.*
- ❏ *Scanner's control panel:* ***Settings*** *>* ***Basic Settings*** *>* ***Date/Time Settings****.*

Settings	Local DB	LDAP	Local DB and LDAP
Enabling authentication You need to enable authentication before making authentication settings. "Enabling Authentication" on page 137	✓	✓	✓
Authentication Settings Setting the Authentication Method and how to authenticate the user. "Authentication Settings" on page 137	✓	✓	✓
Registering User Settings Register the settings for each user. You can also register users in bulk by using a CSV file. "Registering User Settings" on page 139	✓	–	✓
Synchronizing with the LDAP Server Make the LDAP server synchronization settings. "Synchronizing with the LDAP Server" on page 145	–	✓	✓
Setting the Email Server Set the email server settings. Set this when using functions that requires email server settings such as Scan to My Email. "Setting the Email Server" on page 148	✓	✓	✓
Setting Scan to My Folder Set the destination folders. Set this when using the Scan to My Folder function. "Setting Scan to My Folder" on page 149	✓	✓	✓

Settings	Local DB	LDAP	Local DB and LDAP
Customize One-touch Functions Set this when changing the items displayed on the scanner's control panel. You can display only the icons you need on the control panel, or change the order of the icons. "Customize One-touch Functions" on page 151	✓	✓	✓

Enabling Authentication

You need to enable authentication before making authentication settings.

When setting up from Web Config:

Select **On (Device/LDAP Server)** from the **Product Security** tab > **Basic** > **Authentication**.

When setting up from Epson Device Admin:

On the configuration template, select **On (Device/LDAP Server)** from **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Note:
If you enable Authentication Settings on the scanner, Lock Setting is also enabled for the control panel. The control panel cannot be unlocked when Authentication Settings is enabled.

Even if you disable Authentication Settings, Lock Setting remains enabled. If you want to disable it, you can make settings from the control panel or Web Config.

Related Information

➡ "Setting Lock Setting from the Control Panel" on page 90
➡ "Setting Lock Setting from Web Config" on page 90

Authentication Settings

Setting the Authentication Method and how to authenticate the user.

When setting up from Web Config:

Select the **Product Security** tab > **Authentication Settings**.

When setting up from Epson Device Admin:

Select **Administrator Settings** > **Authentication Settings** > **Authentication Settings** from the configuration template.

Item	Explanation
Authentication Method	Select the Authentication Method. ❏ Local DB Authenticate using the User Settings registered to the scanner. It is necessary to register the user to the scanner. ❏ LDAP Authenticate using the user information on the LDAP server synchronized with the scanner. You need to configure the LDAP server settings beforehand. ❏ Local DB and LDAP Authenticate using the user information registered to the scanner or the LDAP server synchronized with the scanner. You need to register the user to the scanner and set up the LDAP server.
How to Authenticate User	Select how to authenticate a user. ❏ Card or User ID and Password Use an authenticate card to authenticate users. You can also use a user ID and password to authenticate. ❏ User ID and Password Use a user ID and password to authenticate users. You cannot use an authenticate card to authenticate when you select this function. ❏ User ID Use only a user ID to authenticate users. You do not need to set a password. ❏ Card or ID Number Use an authenticate card to authenticate users. You can also use an ID Number. ❏ ID Number Use only an ID Number to authenticate users.
Allow users to register authentication cards	Enable it if you allow users to register the authentication card to the system. If you select **LDAP** for **Authentication Method**, you cannot set it. For more information on how users can register their authentication cards, see "Registering an Authentication Card" in the *User's Guide*.
The Minimum Digit Number of ID Number	Select the minimum number of digits for the ID number.
Minimum Number of Bytes for User ID (UTF-8)	Select the minimum bytes for the User ID. Supported in Europe, the Middle East, and Africa only.
Caching for LDAP authenticated users	When using LDAP server authentication, you can set whether or not to use caching for user information.
Use user information in SMTP authentication	When using a user ID and password for authentication, you can set whether or not to use user information for SMTP authentication. The system uses the last user ID and password that were logged in.
Restrictions for LDAP authenticated users	If you are using LDAP, you can set the functions that are available to the user.

Registering User Settings

Register the User Settings used for user authentication. You can register using any of the following methods.

❏ Registering User Settings One by One (Web Config)

❏ Registering Multiple User Settings as a Batch Using a CSV File (Web Config)

❏ Registering User Settings to Multiple Scanners as a Batch Using a Configuration Template (Epson Device Admin)

Related Information

➡ "Registering User Settings Individually (Web Config)" on page 139

➡ "Registering Multiple User Settings Using a CSV file (Web Config)" on page 140

➡ "Registering User Settings to Multiple Scanners as a Batch (Epson Device Admin)" on page 143

Registering User Settings Individually (Web Config)

Access Web Config and select the **Product Security** tab > **User Settings** > **Add**, and then enter the User Settings.

Item	Explanation
User ID	Enter the user ID you want to use for authentication within a range of 1 to 83 bytes that can be expressed in Unicode (UTF-8). Since the user ID is not case sensitive, you can login using upper or lower case letters.
User name Display	Enter the user name displayed on the scanner's control panel within 32 characters that can be expressed in Unicode (UTF-16). You can leave this blank.
Password	Enter the password you want to use for authentication within 32 characters in ASCII. The password is case sensitive. Leave this blank if you select **User ID** for **How to Authenticate User**.
Authentication Card ID	Enter the authentication card ID within 116 characters in ASCII. You can leave this blank. When you permit **Allow users to register authentication cards** for **Authentication Settings**, the result registered by users is reflected.
ID Number	This item is displayed when **Card or ID Number** or **ID Number** is selected in **Authentication Settings** > **How to Authenticate User**. Enter a number that falls somewhere between the number set in **Authentication Settings** > **The Minimum Digit Number of ID Number** and is up to 8 digits.
Auto Generate	This item is displayed when **Card or ID Number** or **ID Number** is selected in **Authentication Settings** > **How to Authenticate User**. Click to automatically generate an ID number with the same number of digits you selected in **The Minimum Digit Number of ID Number**.
Department	Enter the department name and so on that identifies the user within 40 characters that can be expressed in Unicode (UTF-16). You can leave this blank.

Item	Explanation
Email Address	Enter the user's email address within 200 characters in ASCII. This is used as the destination for **Scan to My Email**. You can leave this blank.
Scan to My Folder	Set the save destinations individually when you select **Individual** in **Scan to My Folder** > **Setting Type**. See the following for more information on the setting items. "Setting Scan to My Folder" on page 149
Restrictions	You can restrict the functions for each user. Select the function that you permit to use.
Presets	You can set up to five presets that are only available to the selected user from the Presets registered in the scanner. ❏ Presets that have been allocated to a user can only be used by that user. Presets that have not been allocated to any user can be used by all users. ❏ If a user only has one Presets available, that is automatically loaded after authentication. If multiple Presets are available, a list of Presets is displayed after authentication. ❏ You cannot create or display Presets that use functions that have been restricted in **Restrictions**.

Registering Multiple User Settings Using a CSV file (Web Config)

Enter the settings for each user in a CSV file and register them as a batch.

Creating a CSV File

Create a CSV file to import User Settings.

Note:
If you register one or more User Settings in advance and then export a formatted file (CSV file), you can use the registered setting as a reference for entering setting items.

1. Access Web Config and select the **Product Security** tab > **User Settings**.
2. Click **Export**.
3. Select the file format for **File Format**.

   Select it by referring below.

Item	Explanation
CSV UTF-16 (Tab delimited)	Select when you edit the file using Microsoft Excel. Each parameter is enclosed by "[ ]"(brackets). Enter the parameters in "[ ]". When you update the file, we recommend overwriting the file. If you newly save the file, select Unicode text(*.txt) for the file format.
CSV UTF-8 (Comma delimited)	Select when you edit the file using a text editor or macro without Microsoft Excel.
CSV UTF-8 (Semicolon delimited)	

4. Click **Export**.

5. Edit and save this CSV file in a spreadsheet application such as Microsoft Excel or in a text editor.

> ***Important:***
> *When editing the file, do not change the encoding and header information.*

CSV File Setting Items

Item	Settings and Explanation
UserID	Enter the user ID to use authentication between 1 and 83 bytes in Unicode.
UserName	Enter the user name displayed on the scanner's control panel within 32 characters in Unicode. You can leave this blank.
Password	Enter the password to use for authentication within 32 characters in ASCII. When importing, this is set as the password instead of **EncPassword**. Leave this blank if you select **User ID** for **How to Authenticate User**. When exporting, this is always blank.
AuthenticationCardID	Set the reading result of Authenticate card. When you permit **Allow users to register authentication cards** in **Authentication Settings**, the result registered by users is reflected. Enter within 116 characters in ASCII. You can leave this blank.
IDNumber	This item is displayed when **Card or ID Number** or **ID Number** is selected in **Authentication Settings** > **How to Authenticate User**. Enter a number that falls somewhere between the number set in **Authentication Settings** > **The Minimum Digit Number of ID Number** and is up to 8 digits. An ID Number cannot be duplicated. If it is duplicated, you will be alerted to the error when importing the file. When left blank, it is automatically assigned a number.
Department	Enter the department name arbitrary to distinguish the users. Enter within 40 characters in Unicode. You can leave this blank.
MailAddress	Set the email address for the users. This is used as the destination for **Scan to My Email**. You can use A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Enter 200 characters or less. You cannot use "," (comma) for the first character. You can leave this blank.
FolderProtocol	Set the type of Scan to My Folder function. Network Folder/FTP (SMB): 0, FTP: 1
FolderPath	Set the saving destination for the Scan to My Folder function.
FolderUserName	Set the user name for the Scan to My Folder function.
FolderPassword	Set a password to authenticate the destination folder for the Scan to My Folder function within 32 ASCII characters. When importing, this is set as the password instead of **EncPassword**. When exporting, this is always blank.

Item	Settings and Explanation
FtpPassive	Set the connection mode for the FTP server when **FTP** is selected as the **Type** for the Scan to My Folder function. Active mode: 0, Passive mode: 1
FtpPort	Set the port number for sending scanned data to the FTP server from 0 to 65535 when **FTP** is selected as the **Type** for the Scan to My Folder function.
ScanToMemory	Set the restrictions for Scan to USB Drive. Not Allowed: 0, Allowed: 1
ScanToMail	Set the restrictions for Scan to Email. You can set **Scan to My Email** only when **Scan to Email** has been enabled. Not Allowed: 0, Allowed: 1
ScanToFolder	Set the restrictions for Scan to Network Folder/FTP. You can set **Scan to My Folder** only when **Scan to Network Folder/FTP** has been enabled. Not Allowed: 0, Allowed: 1
ScanToCloud	Set the restrictions for Scan to Cloud. Not Allowed: 0, Allowed: 1
ScanToComputer	Set the restrictions for Scan to Computer. Not Allowed: 0, Allowed: 1
PresetIndex	Set the Presets that you want to associate with the user. You can set up to five Presets registration numbers separated by commas.
EncPassword	When exporting user settings, the parameter set for **Password** is encrypted, then the value is encoded by BASE64 and output. When importing with the new password for **Password**, this value is ignored. If **Password** is blank, this value is used and the password remains as it was before exporting.
EncFolderPassword	When exporting the parameter set for **FolderPassword** is encrypted, then the value is encoded by BASE64 and output. When importing with the new password for **FolderPassword**, this value is ignored. If **FolderPassword** is blank, this value is used and the password remains as it was before exporting.

Importing a CSV File

1. Access Web Config and select the **Product Security** tab > **User Settings**.
2. Click **Import**.
3. Select the file you want to import.
4. Click **Import**.
5. After checking the displayed information, click **OK**.

Registering User Settings to Multiple Scanners as a Batch (Epson Device Admin)

You can register User Settings used in Local DB as a batch by using an LDAP server or a CSV/ENE file.

Note:
*An ENE file is a binary file provided by Epson that encrypts and saves information for **Contacts** such as personal information and User Settings. It can be exported from Epson Device Admin and you can set a password. It is useful when you want to import the User Settings from a backup file.*

Importing from CSV / ENE File

1. Select **Administrator Settings** > **Authentication Settings** > **User Settings** from the configuration template.
2. Click **Import**.
3. Select **CSV or ENE File** from **Import Source**.
4. Click **Browse**.

   The file selection screen is displayed.
5. Select the file you want to import to open it.
6. Select an import method.
   - ❏ Overwrite and Add: Overwrites if the same user ID exists; adds a new ID if it does not exist.
   - ❏ Replace All: Replaces everything with the user settings you want to import.
7. Click **Import**.

   The setting confirmation screen is displayed.
8. Click **OK**.

   The validation result is displayed.

   Note:
   - ❏ *If the number of imported user settings exceeds the number that can be imported, a message will prompt you to delete some user settings. Delete any excess user settings before importing.*
   - ❏ *Select the user settings you want to delete before importing, and then click **Delete**.*
9. Click **Import**.

   The user settings are imported into the configuration template.

Importing from the LDAP Server

1. Select **Administrator Settings** > **Authentication Settings** > **User Settings** from the configuration template.
2. Click **Import**.
3. Select **LDAP** from **Import Source**.

4. Click **Settings**.

   The **LDAP Server** settings are displayed.

   Note:
   This LDAP server setting is for importing the user settings from the LDAP server. The imported (copied) user settings are used to authenticate users by using the scanner itself.

   *On the other hand, when you select **LDAP** or **Local DB and LDAP** as the authentication method, users are authenticated by communicating with the LDAP server.*

5. Set each item.

   When importing user settings from an LDAP server, you can also configure the following settings in addition to the LDAP settings.

   For other items, see Related Information.

Item			Explanation
LDAP Server Settings	LDAP Server Type		Allows you to select the type of LDAP server.
Search Settings	Search Filter		You can set the text used for the LDAP search filter. Select **Custom** to edit the search text.
	Options	Type	You can set the type of save destination for **Scan To My Folder**.
		Connection Mode	When the **Type** is set to **FTP**, you can set the FTP connection mode.
		Port Number	When the **Type** is set to **FTP**, you can set the port number you want to use.

6. Perform the connection test as necessary by clicking **Connection Test**.

   Acquires and displays 10 user settings from the LDAP server.

7. Click **OK**.

8. Select an import method.

   ❏ Overwrite and Add: Overwrites if the same user ID exists; adds a new ID if it does not exist.

   ❏ Replace All: Replaces everything with the user settings you want to import.

9. Click **Import**.

   The setting confirmation screen is displayed.

10. Click **OK**.

    The validation result is displayed.

11. Click **Import**.

    The user settings are imported into the configuration template.

Related Information

➡ "Configuring an LDAP Server" on page 145

➡ "Configuring the LDAP Server Search Settings" on page 146

Synchronizing with the LDAP Server

Make the LDAP Server settings for the scanner.

Make settings for both primary server and secondary server as necessary.

Note:
*The **LDAP Server** settings are shared with **Contacts**.*

Available Services

The following directory services are supported.

Service Name	Version
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Configuring an LDAP Server

To use an LDAP server, you first need to configure the LDAP server.

When setting up from Web Config:

Select the **Network** tab > **LDAP Server** > **Basic (Primary Server)** or **Basic (Secondary Server)**.

If you select **Kerberos Authentication** as the **Authentication Method**, select **Network** > **Kerberos Settings** to make settings for Kerberos.

When setting up from Epson Device Admin:

Select **Network** > **LDAP server** > **Server Settings (Primary Server)** or **Server Settings (Secondary Server)** from the configuration template.

If you select **Kerberos Authentication** as the **Authentication Method**, select **Network** - **Security** > **Kerberos Settings** to make settings for Kerberos.

Item	Settings and Explanation
Use LDAP Server	Select **Use** or **Do Not Use**.
LDAP Server Address	Enter the LDAP server address. Enter between 1 and 255 characters of either IPv4, IPv6, or FQDN format. For the FQDN format, you can use alphanumeric characters in ASCII (0x20 - 0x7E) and hyphens, except at the beginning and end of the address.
LDAP server Port Number (Port number)	Enter the LDAP server port number between 1 and 65535.
Secure Connection	Specify the authentication method for the scanner to access the LDAP server. If you select **None**, communications are not encrypted. We recommend setting this to something other than **None**.
Certificate Validation	The LDAP server's certificate is authenticated when this is enabled. We recommend setting this to **Enable**. To set up, the **CA Certificate** needs to be imported to the scanner.

Item	Settings and Explanation
Search Timeout (sec)	Set the length of time for searching before timeout occurs between 5 and 300 seconds.
Authentication Method	Select the authentication method. When you select **Simple Authentication**, we recommend setting **Secure Connection** to something other than **None**. If you select **Kerberos Authentication**, make settings for Kerberos in advance. To perform Kerberos Authentication, the following environment is required. ❏ The scanner and the DNS server can communicate. ❏ The time for the scanner, KDC server, and the server that is required for authentication (LDAP server, SMTP server, File server) are synchronized. ❏ When the service server is assigned as the IP address, the FQDN for the service server is registered to the DNS server reverse lookup zone.
Kerberos Realm to be Used	If you select **Kerberos Authentication** for **Authentication Method**, select the Kerberos realm that you want to use.
Administrator DN / User Name	Enter the user name for the LDAP server in 128 characters or less in Unicode (UTF-8). You cannot use control characters, such as 0x00 to 0x1F and 0X7F. This setting is not used when **Anonymous Authentication** is selected as the **Authentication Method**. If you do not want to specify this, leave it blank.
Password	Enter the password for the LDAP server authentication in 128 characters or less in Unicode (UTF-8). You cannot use control characters, such as 0x00 to 0x1F and 0X7F. This setting is not used when **Anonymous Authentication** is selected as the **Authentication Method**. If you do not want to specify this, leave it blank.

Kerberos Settings

If you select **Kerberos Authentication** as the **Authentication Method**, you need to make Kerberos settings. You can register up to 10 Kerberos settings.

When setting up from Web Config:

Select the **Network** tab > **Kerberos Settings**.

When setting up from Epson Device Admin:

Select **Network** > **Security** > **Kerberos Settings** from the configuration template.

Item	Settings and Explanation
Realm (Domain)	Enter the realm of the Kerberos authentication in 255 characters or less in ASCII (0x20-0x7E). If you do not want to register this, leave it blank.
KDC Address	Enter the address of the Kerberos authentication server. Enter 255 characters or less in either IPv4, IPv6 or FQDN format. If you do not want to register this, leave it blank.
Port Number (Kerberos)	Enter the Kerberos server port number between 1 and 65535.

Configuring the LDAP Server Search Settings

Sets the search attributes for user settings.

When setting up from Web Config:

Select the **Network** tab > **LDAP Server** > **Search Settings (Authentication)**.

When setting up from Epson Device Admin:

Select **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)** from the configuration template.

Item	Settings and Explanation
Search Base (Distinguished Name)	Specify the start position when searching for user information from the LDAP server. Enter between 0 and 128 characters in Unicode (UTF-8). If you do not search for arbitrary attribute, leave this blank. Example for the local server directory: dc=server,dc=local
User ID Attribute	Specify the attribute name to display when searching for the ID number. Enter between 1 and 255 characters in ASCII. The first character should be a-z or A-Z. Example: cn, uid
User name Display Attribute	Specify the attribute name to display as the user name. Enter between 0 and 255 characters in ASCII. The first character should be a-z or A-Z. You can leave this blank. Example: cn, name
Authentication Card ID Attribute	Specify the attribute name to display as the authentication card ID. Enter between 0 and 255 characters in ASCII. The first character should be a-z or A-Z. You can leave this blank. Example: cn, sn
ID Number Attribute	Specify the attribute name to display when searching for the ID number. Enter between 1 and 255 characters in ASCII. The first character should be a-z or A-Z. Example: cn, id
Department Attribute	Specify the attribute name to display as the department name. Enter between 0 and 255 characters in ASCII. The first character should be a-z or A-Z. You can leave this blank. Example: ou, ou-cl
Email Address Attribute	Specify the attribute name to display when searching for email addresses. Enter between 1 and 255 characters in ASCII. The first character should be a-z or A-Z. Example: mail
Save To Attribute	Specify the attribute name that points to the destination for Scan To My Folder. Enter between 0 and 255 characters in ASCII. Example: homeDirectory

Checking the LDAP Server Connection

You can perform an LDAP server connection test using the values entered in **LDAP Server** > **Search Settings**.

1. Access Web Config and select the **Network** tab > **LDAP Server** > **Connection Test**.
2. Select **Start**.

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

LDAP Server Connection Test References

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

Setting the Email Server

When you use **Scan to My Email**, set Email Server.

Note:
*You can set **Scan to My Email** only when **Scan to Email** has been enabled.*

When setting up from Web Config:

Select the **Network** tab > **Email Server** > **Basic**.

When setting up from Epson Device Admin:

Select **Common** > **Email Server** > **Mail Server Settings** from the configuration template.

Item	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	The email server needs to support SMTP authentication.
	POP before SMTP	When you select this item, set a POP3 server.
Authenticated Account	If you select **SMTP AUTH** or **POP before SMTP** as the **Authentication Method**, enter the authenticated account name. Enter 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. Enter between 0 and 20 characters in ASCII (0x20 - 0x7E).	

Item	Settings and Explanation	
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.	
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 authenticated when this is enabled. We recommend setting this to **Enable**.	
POP3 Server Address	If you select **POP before SMTP** as the **Authentication Method**, enter the POP3 server address. You can enter 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**, specify the port number. Enter a number between 1 and 65535.	

Setting Scan to My Folder

Saves scanned images to the folder assigned to each user. You can set the following as a dedicated folder.

Note:
*You can set **Scan To My Folder** only when **Scan to Network Folder/FTP** has been enabled.*

Save To Setting	Authentication Method	Folder Path Setting Location
Specify one network folder for the entire Authentication Settings to automatically create a personal folder below the specified folder using the name of the user ID.	❏ Local DB ❏ LDAP ❏ Local DB and LDAP	Scanner (Scan to My Folder setting)
Assign different network folders individually to each user.	Local DB	Scanner (User Settings)
	LDAP	LDAP Attributes
	Local DB and LDAP	Scanner (User Settings) or LDAP attributes

When setting up from Web Config:

Select the **Product Security** tab > **Scan to Network Folder/FTP**.

When setting up from Epson Device Admin:

Select **Administrator Settings** > **Authentication Settings** > **Scan to Network Folder/FTP** > **Scan to My Folder** from the configuration template.

Item		Explanation
Save To Setting	Setting Type	❏ **Shared**: Automatically creates a folder named after the user's ID below the folder path or URL specified in **Save to**, and saves the scanned images to this folder. ❏ **Individual**: Set the save destination for scan results for each user. Local DB users can be set in the user settings. LDAP users use the storage location acquired from the LDAP server's search attributes.
	Type	Select the transmission protocol according to the scanning output destination. For a network folder: **Network Folder (SMB)** For an FTP server: **FTP**
	Save to	Specify the path or URL of the output path. Enter within 160 characters in Unicode (UTF-16).
	Connection Mode	Set when you select **FTP** in **Type**. Select a connection mode to the FTP server.
	Port Number	Set when you select **FTP** in **Type**. Enter the port number to send the scanned data to an FTP server between 0 and 65535.
Authentication Settings	Setting Type	Set when you select **Individual** as the **Setting Type** in **Save To Setting**. Set the "User Name" and "Password" to access the folder. ❏ **Shared**: Use a common **User Name** and **Password** for all users. ❏ **Individual**: For Local DB users, set the **User Name** and **Password** individually in **User Settings**. LDAP users cannot be configured individually. The **User Name** and **Password** set by this item are used as a batch.
	User Name	Enter the user name to access the scan output destination folder. Enter within 30 characters in Unicode (UTF-16). Set this when you are using a **Shared** or LDAP server.
	Password	Enter the password corresponding to the **User Name**. Enter within 20 characters in Unicode (UTF-16). Set this when you are using a **Shared** or LDAP server.

Prohibit Changing the Destination for Scan to Network Folder/FTP

Item	Explanation
Prohibit manual entry of destination	When enabled, the user cannot change the default destination.

Customize One-touch Functions

You can display only necessary icons by editing the icon layout displayed on the home screen for the control panel.

When setting up from Web Config:

Select the **Product Security** tab > **Customize One-touch Functions**.

When setting up from Epson Device Admin:

Select **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** from the configuration template.

Note:
In the following cases, icons for the specified functions are not displayed on the home screen.

- ❏ *When you select functions that are not permitted due to **Restrictions**.*
- ❏ *When the email address for a logged in user is not registered. (Scan to My Email)*
- ❏ *When the destination folder is not set. (Scan to My Folder)*

Item	Explanation
Maximum functions per screen	Select the layout of the icons displayed on the control panel. The image changes according to the selected layout.
Screen(s)	Select the number of pages.
Number	Select the functions you want to display for each numbered position.

Job History Reports Using Epson Device Admin

You can create a Job History report for each group and each user by using Epson Device Admin. You can save up to 3,000 instances of usage histories to the scanner. You can create the report by specifying a period or setting a regular schedule.

To output the Job History as a report, select **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices** from the ribbon menu on the Device List screen.

For details on how to create a user report, see the documentation for Epson Device Admin.

Items that can be Included in the Report

You can output the following items in the user report.

Date/Job ID/Operation/User ID/Department/Result/Result details/Scan: Destination type/Scan: Destination/Scan: Paper Size/Scan: 2-Sided/Scan: Color/Scan: Pages/Devices: Model/Devices: IP Address/Devices: Serial Number/ Devices: Department/Devices: Location/Devices: Remark/Devices: Note

Logging in as an Administrator from the Control Panel

You can use any of the following methods to log in as an administrator from the scanner's control panel.

1. Tap at the top right of the screen.
   - ❏ When Authentication Settings is enabled, the icon is displayed on the **Welcome** screen (the authentication standby screen).
   - ❏ When Authentication Settings is disabled, the icon is displayed on the Home screen.
2. Tap **Yes** when the confirmation screen is displayed.
3. Enter the administrator's password.

   A login complete message is displayed, and then the Home screen on the control panel is displayed.

To logout, tap at the top right of the Home screen.

Disabling Authentication Settings

You can disable Authentication Settings using Web Config.

Note:
The User Settings registered to the scanner will be saved even if Authentication Settings is disabled. You can remove them by restoring the scanner to its default settings.

1. Access Web Config.
2. Select the **Product Security** tab > **Basic** > **Authentication**.
3. Select **OFF**.
4. Click **Next**.
5. Click **OK**.

Note:
Even if you disable Authentication Settings, Lock Setting remains enabled. If you want to disable it, you can make settings from the control panel or Web Config.

Related Information

➡ "Setting Lock Setting from the Control Panel" on page 90
➡ "Setting Lock Setting from Web Config" on page 90

Deleting Authentication Settings Information (Restore Default Settings)

To delete all Authentication Settings information (Card Reader, Authentication Method, User Settings, and so on), restore all of the scanner settings to the default settings at the time of purchase.

Select **Settings** > **System Administration** > **Restore Default Settings** > **All Settings** on the control panel.

> ***Important:***
> *All contacts and other network settings will also be deleted. Deleted settings cannot be restored.*

Solving Problems

Cannot Read the Authentication Card

Check the following.

❏ Check if the authentication device is connected to the scanner correctly.
Connect the authentication device to the external interface USB port on the back of the scanner.

❏ Check that the authentication device and the authentication card are supported.

Maintenance

Cleaning Outside the Scanner. 155

Cleaning Inside the Scanner. 155

Replacing the Roller Assembly Kit. 160

Resetting the Number of Scans. 165

Energy Saving. 165

Transporting the Scanner. 166

Backing Up the Settings. 167

Restore Default Settings. 168

Updating Applications and Firmware. 169

Cleaning Outside the Scanner

Wipe off any stains on the outer case with a dry cloth or a cloth dampened with mild detergent and water.

Important:

- ❏ *Never use alcohol, thinner, or any corrosive solvent to clean the scanner. Deformation or discoloration may occur.*
- ❏ *Do not let water get inside the product. This could cause a malfunction to occur.*
- ❏ *Never open the scanner case.*

1. Press the ⏻ button to turn off the scanner.
2. Unplug the AC adapter from the scanner.
3. Clean the outer case with a cloth dampened with mild detergent and water.

   Note:
   Wipe the touchscreen by using a soft, dry cloth.

Cleaning Inside the Scanner

After using the scanner for a while, paper and room dust on the roller or the glass part inside the scanner may cause paper feed or scanned image quality problems. Clean the inside of the scanner every 5,000 scans.

You can check the latest number of scans on the control panel or in the Epson Scan 2 Utility.

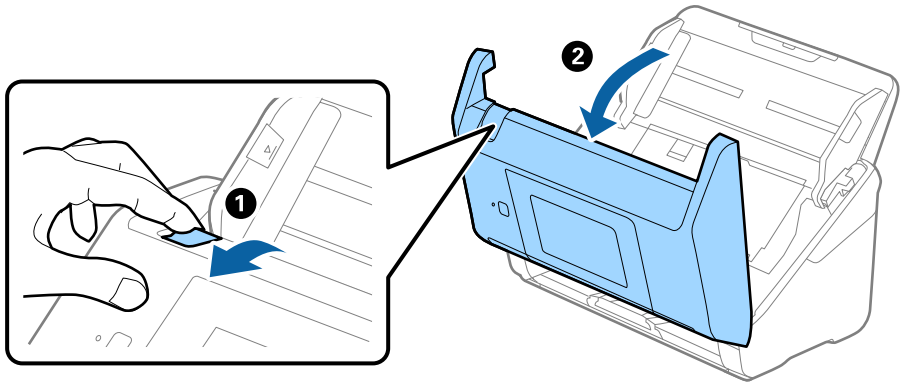
If a surface is stained with a hard-to-remove material, use a genuine Epson cleaning kit to remove the stains. Use a small amount of cleaner on the cleaning cloth to remove the stains.

Important:

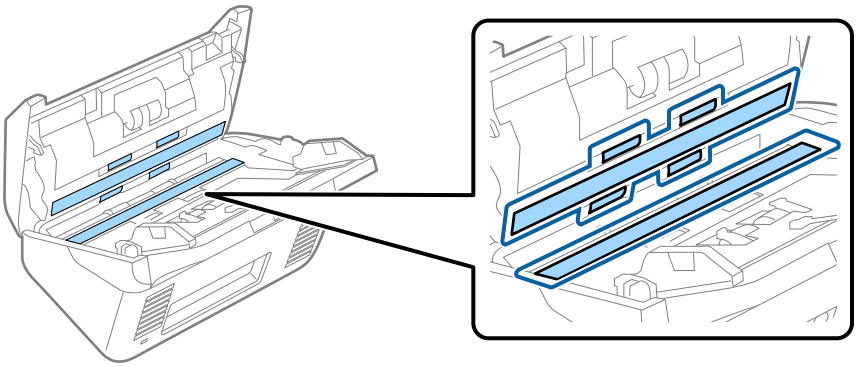
- ❏ *Never use alcohol, thinner, or any corrosive solvent to clean the scanner. Deformation or discoloration may occur.*
- ❏ *Never spray any liquid or lubricant on the scanner. Damage to equipment or circuits may cause abnormal operations.*
- ❏ *Never open the scanner case.*

1. Press the ⏻ button to turn off the scanner.
2. Unplug the AC adapter from the scanner.

3. Pull the lever and open the scanner cover.



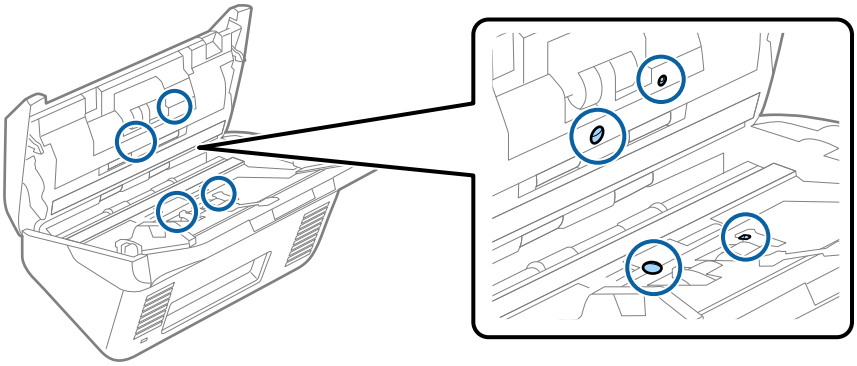
4. Wipe off any stains on the plastic roller and glass surface at the bottom inside of the scanner cover using a soft cloth or a genuine Epson cleaning kit.



Important:

- *Do not place too much force on the glass surface.*
- *Do not use a brush or a hard tool. Any scratches on the glass may affect the scan quality.*
- *Do not spray cleaner directly onto the glass surface.*

5. Wipe off any stains on the sensors with a cotton swab.

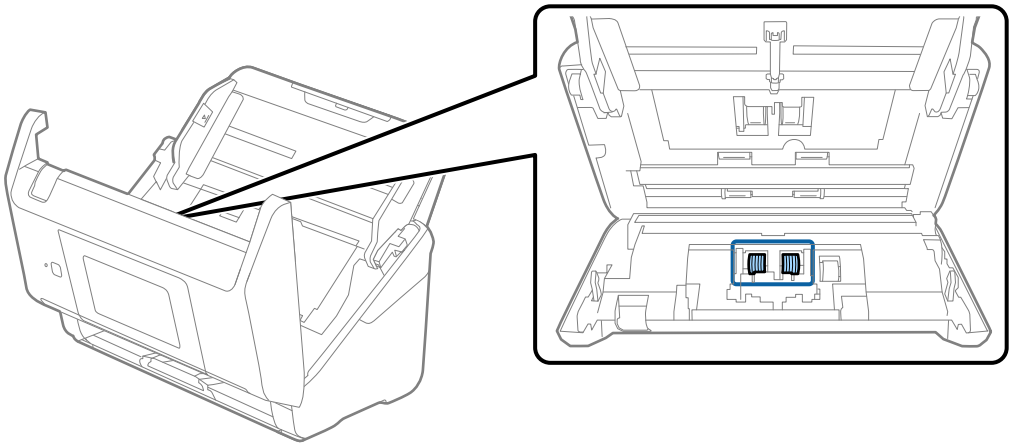


Important:

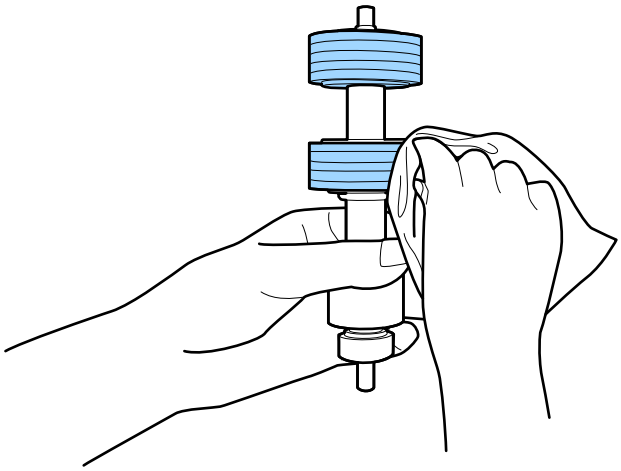
Do not use liquid such as a cleaner on a cotton swab.

6. Open the cover, and then remove the separation roller.

   See “Replacing the Roller Assembly Kit” for more details.



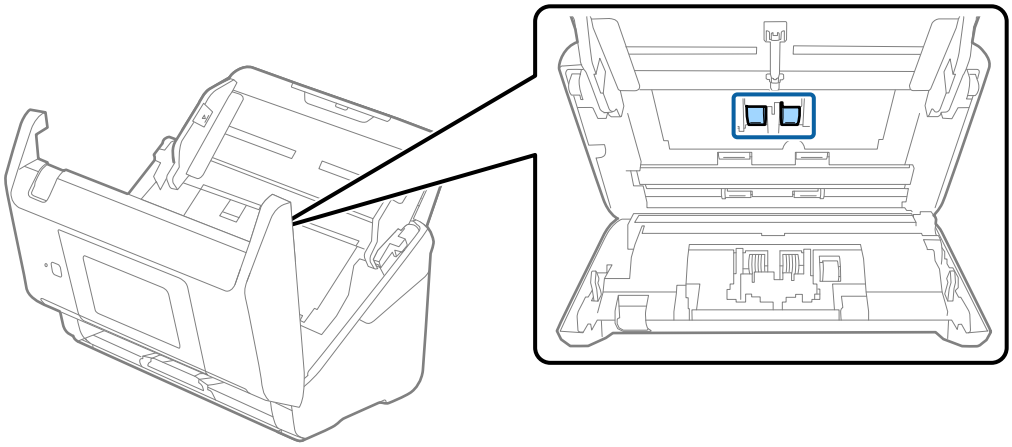
7. Wipe off any dust or dirt on the separation roller using a genuine Epson cleaning kit or a soft, moist cloth.



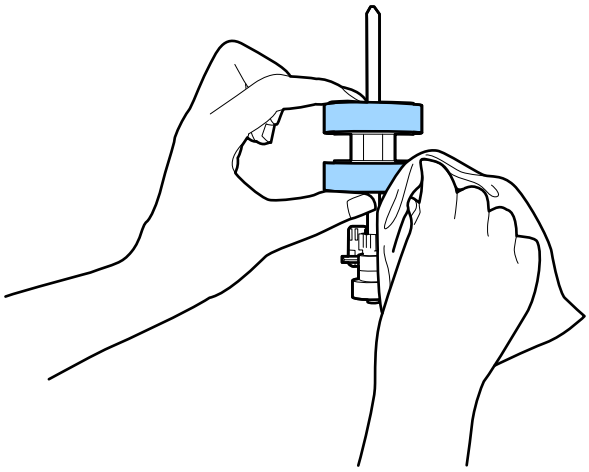
> ***Important:***
>
> *Use only a genuine Epson cleaning kit or a soft, moist cloth to clean the roller. Using a dry cloth may damage the surface of the roller.*

8. Open the cover, and then remove the pickup roller.

   See “Replacing the Roller Assembly Kit” for more details.



9. Wipe off any dust or dirt on the pickup roller using a genuine Epson cleaning kit or a soft, moist cloth.

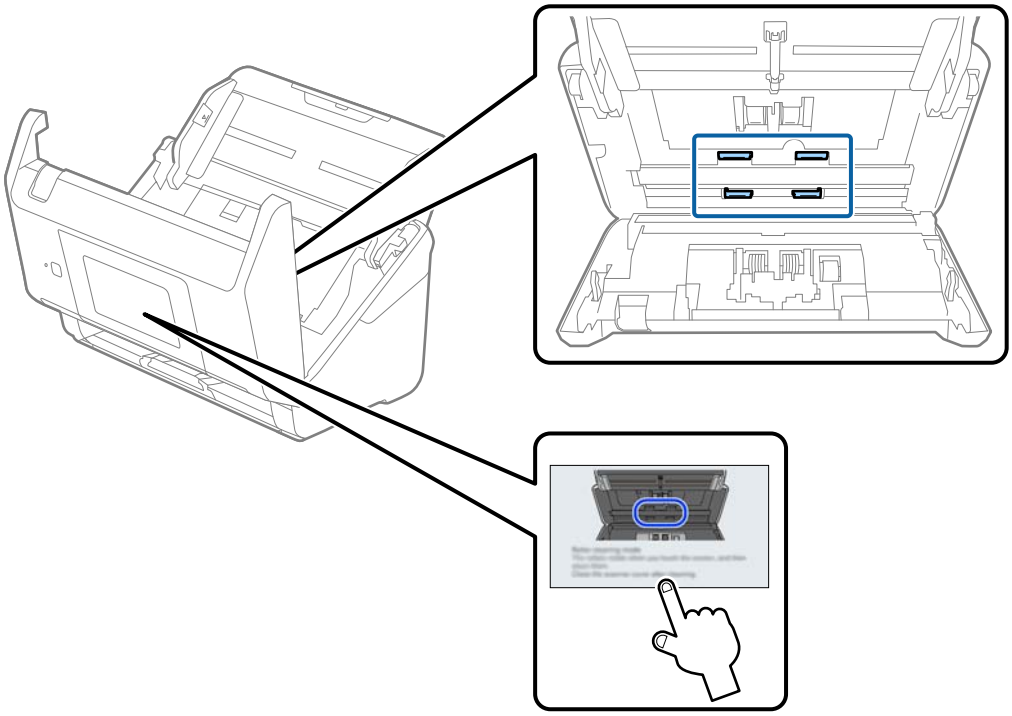


> ***Important:***
>
> *Use only a genuine Epson cleaning kit or a soft, moist cloth to clean the roller. Using a dry cloth may damage the surface of the roller.*

10. Close the scanner cover.
11. Plug in the AC adapter, and then turn on the scanner.
12. Select **Scanner Maintenance** from the home screen.
13. On the **Scanner Maintenance** screen, select **Roller Cleaning**.
14. Pull the lever to open the scanner cover.

    The scanner enters roller cleaning mode.

15. Slowly rotate the rollers at the bottom by tapping anywhere on the LCD. Wipe the surface of the rollers using a genuine Epson cleaning kit or a soft cloth dampened with water. Repeat this until the rollers are clean.



> ***Caution:***
>
> *Be careful not to get your hands or hair caught in the mechanism when operating the roller. This could cause an injury.*

16. Close the scanner cover.

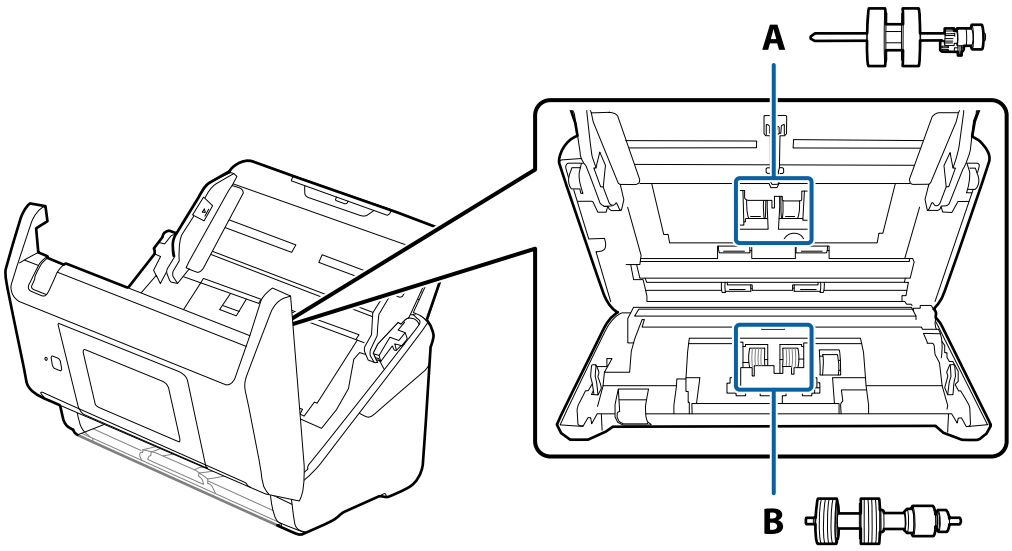
    The scanner exits roller cleaning mode.

Related Information

➡ "Replacing the Roller Assembly Kit" on page 160

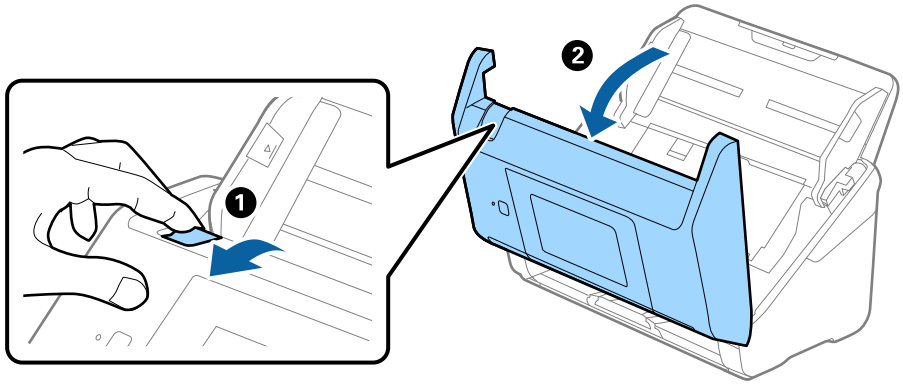
Replacing the Roller Assembly Kit

The roller assembly kit (the pickup roller and the separation roller) needs to be replaced when the number of scans exceeds the life cycle of the rollers. When a replacement message is displayed on the control panel or your computer screen, follow the steps below to replace it.

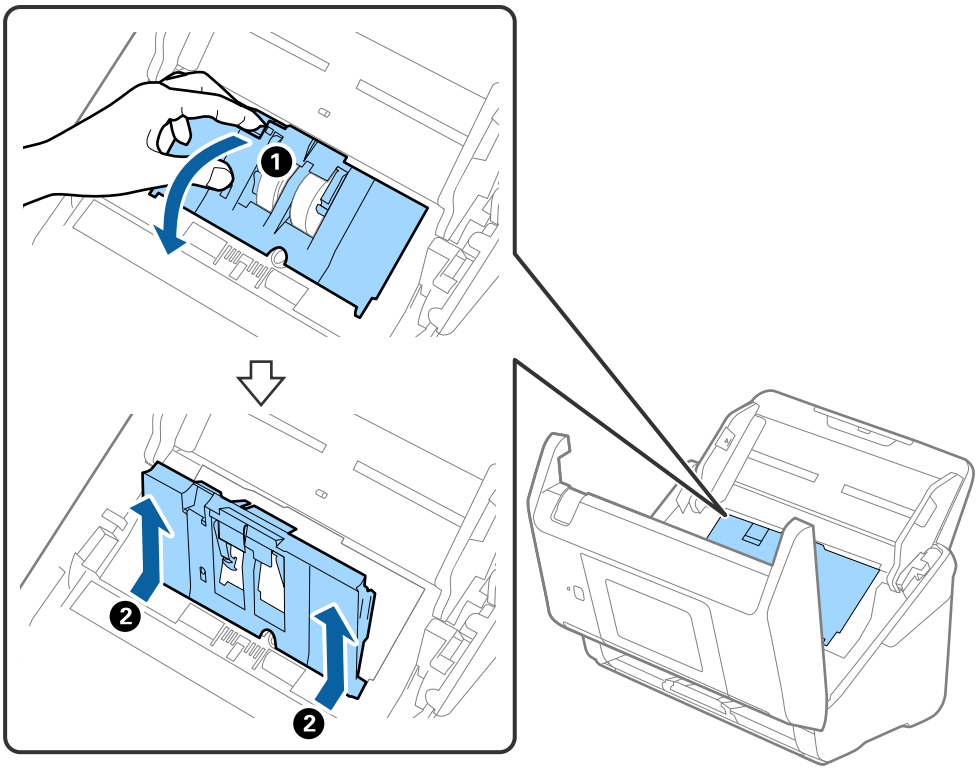


A: pickup roller, B: separation roller

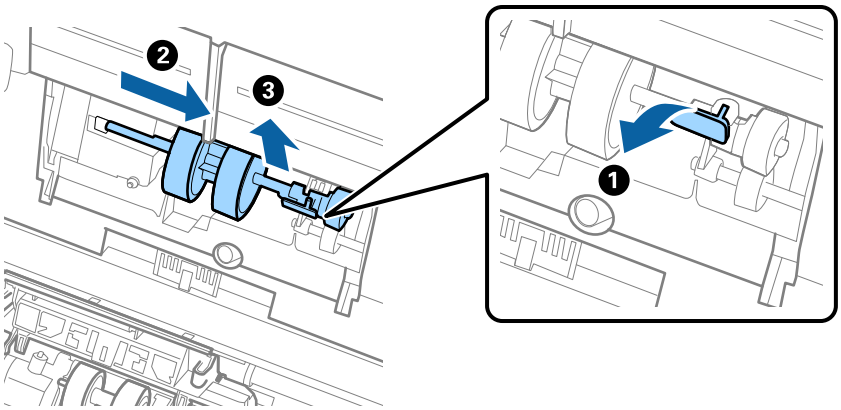
1. Press the ⏻ button to turn off the scanner.
2. Unplug the AC adapter from the scanner.
3. Pull the lever and open the scanner cover.



4. Open the cover of the pickup roller, and then slide and remove it.

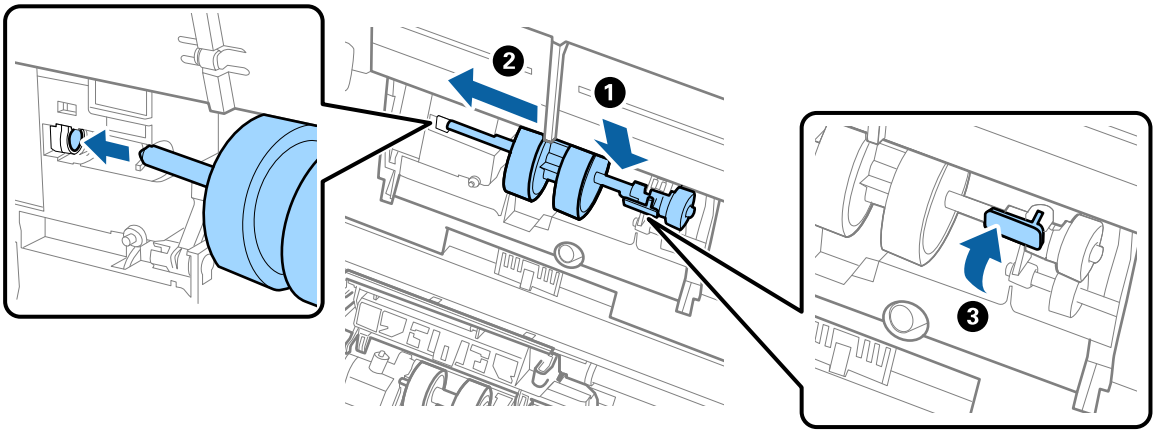


5. Pull down the fixture of the roller axis, and then slide and remove the installed pickup rollers.

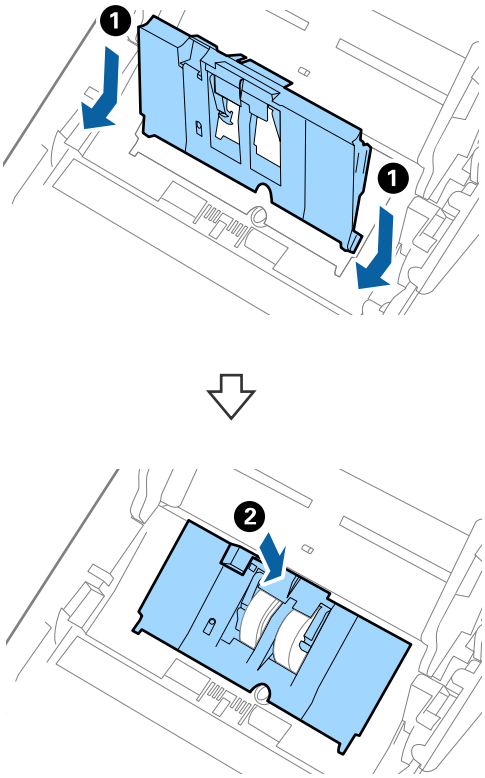


> **Important:**
> *Do not pull out the pickup roller forcibly. This could damage the inside of the scanner.*

6. While holding down the fixture, slide the new pickup roller to the left and insert it into the hole in the scanner. Press the fixture to secure it.

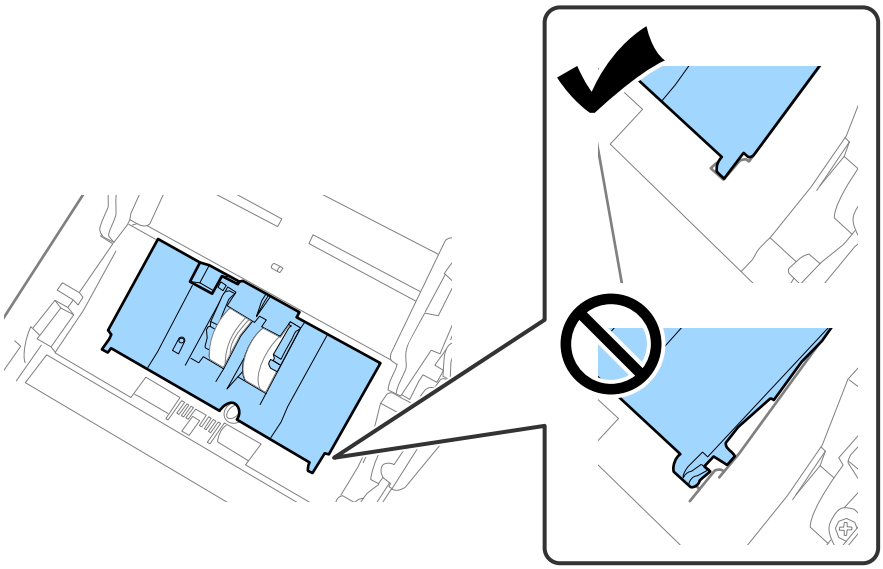


7. Put the edge of the cover of the pickup roller into the groove and slide it. Close the cover firmly.

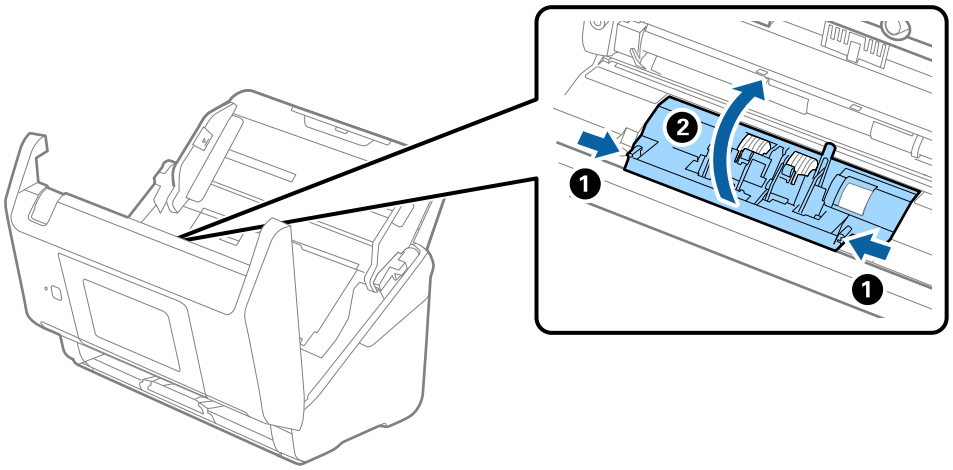


Important:

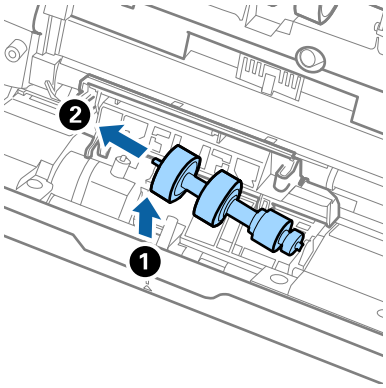
- ❏ *Make sure the pickup cover is closed correctly.*
- ❏ *Make sure the pickup rollers are installed correctly if the cover is hard to close.*
- ❏ *Do not install the cover while it is raised.*



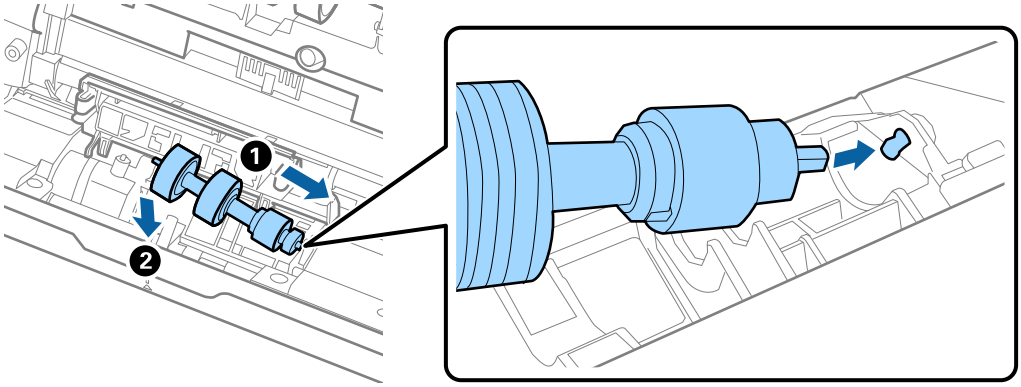
8. Push the hooks on both ends of the separation roller cover to open the cover.



9. Lift the left side of the separation roller, and then slide and remove the installed separation rollers.



10. Insert the new separation roller axis into the hole on the right side, and then lower the roller.



11. Close the separation roller cover.

> ***Important:***
> *If the cover is hard to close, make sure the separation rollers are installed correctly.*

12. Close the scanner cover.

13. Plug in the AC adapter, and then turn on the scanner.

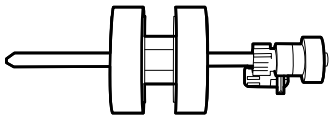
14. Reset the scan number on the control panel.

Note:
Dispose of the pickup roller and the separation roller following the rules and regulations of your local authority. Do not disassemble them.

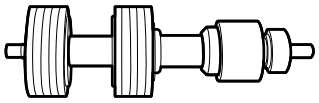
Roller Assembly Kit Codes

Parts (the pickup roller and separation roller) should be replaced when the number of scans exceeds the service number. You can check the latest number of scans on the control panel or in the Epson Scan 2 Utility.

A



B



A: pickup roller, B: separation roller

Part name	Codes	Life cycle
Roller Assembly Kit	B12B819671 B12B819681 (India only)	200,000*

* This number was reached by consecutively scanning using Epson test original papers, and is a guide to the replacement cycle. The replacement cycle may vary depending on different paper types, such as paper that generates a lot of paper dust or paper with a rough surface that may shorten the life cycle.

Resetting the Number of Scans

Reset the number of scans after replacing the roller assembly kit.

1. Select **Settings** > **Device Information** > **Reset the Number of Scans** > **Number of Scans After Replacing Roller** from the home screen.
2. Tap **Yes**.

Related Information

➡ "Replacing the Roller Assembly Kit" on page 160

Energy Saving

You can save energy by using sleep mode or auto power off mode when no operations are performed by the scanner. You can set the time period before the scanner enters sleep mode and turns off automatically. Any increase will affect the product's energy efficiency. Consider the environment before making any changes.

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

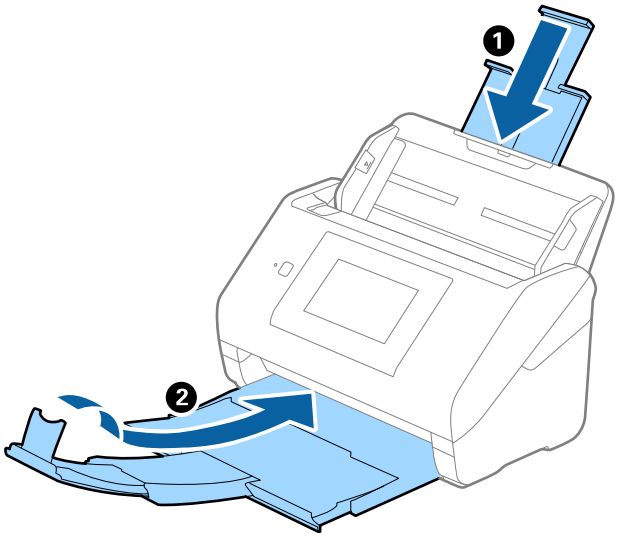
3. Select **Power Off Settings**, and then make settings.

   Note:
   Available features may vary depending on the location of purchase.

Transporting the Scanner

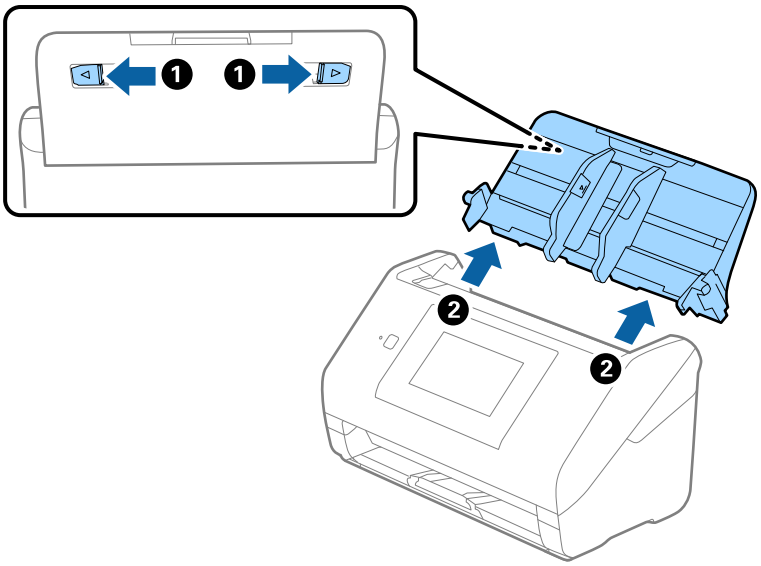
When you need to transport the scanner to move or for repairs, follow the steps below to pack the scanner.

1. Press the ⏻ button to turn off the scanner.
2. Unplug the AC adapter.
3. Remove the cables and the devices.
4. Close the input tray extension and output tray.



> ***Important:***
> *Make sure you close the output tray securely; otherwise it may be damaged during transport.*

5. Remove the input tray.



6. Attach the packing materials that came with the scanner, and then repack the scanner in its original box or a sturdy box.

Backing Up the Settings

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

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

Export the settings

Export the setting from the scanner.

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

2. Select the settings that you want to export.

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

3. Enter a password to encrypt the exported file.

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

4. Click **Export**.

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

Related Information

➡ "Running Web Config on a Web Browser" on page 37

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.*

1. Access Web Config, and then select the **Device Management** tab > **Export and Import Setting Value** > **Import**.
2. Select the exported file, and then enter the encrypted password.
3. Click **Next**.
4. Select the settings that you want to import, and then click **Next**.
5. Click **OK**.

The settings are applied to the scanner.

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Restore Default Settings

On the control panel, select **Settings** > **System Administration** > **Restore Default Settings**, and then select the items you want to restore to their defaults.

- ❏ Network Settings: Restore network related settings to their initial status.
- ❏ All Except Network Settings: Restore other settings to their initial status except for network related settings.
- ❏ All Settings: Restore all settings to their initial status when purchased.

> ***Important:***
> *If you select and run **All Settings**, all setting data registered to the scanner including the contacts and the authentication user settings will be deleted. Deleted settings cannot be restored.*

Updating Applications and Firmware

You may be able to clear certain problems and improve or add functions by updating the applications and the firmware. Make sure you use the latest version of the applications and firmware.

Important:

❏ *Do not turn off the computer or the scanner while updating.*

Note:
When the scanner can connect to the Internet, you can update the firmware from Web Config. Select the ***Device Management*** *tab > **Firmware Update**, check the displayed message, and then click **Start**.*

1. Make sure that the scanner and the computer are connected, and the computer is connected to the internet.
2. Start EPSON Software Updater, and update the applications or the firmware.

   Note:
   Windows Server operating systems are not supported.

   ❏ Windows 10

   Click the start button, and then select **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Enter the application name in the search charm, and then select the displayed icon.

   ❏ Windows 7

   Click the start button, and then select **All Programs** or **Programs** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Select **Finder** > **Go** > **Applications** > **Epson Software** > **EPSON Software Updater**.

Note:
If you cannot find the application you want to update in the list, you cannot update using the EPSON Software Updater. Check for the latest versions of the applications on your local Epson website.

http://www.epson.com

Updating the Scanner's Firmware using the Control Panel

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

1. Select **Settings** on the home screen.
2. Select **System Administration** > **Firmware Update** > **Update**.

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

3. Check the message displayed on the screen and start searching for available updates.

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

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

Updating Firmware Using Web Config

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

1. Access Web Config and select the **Device Management** tab > **Firmware Update**.
2. Click **Start**, and then follow the on-screen instructions.

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

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

Related Information

➡ "Running Web Config on a Web Browser" on page 37

Updating Firmware without Connecting to the Internet

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

Note:
Before updating, make sure that the scanner driver Epson Scan 2 is installed on your computer. If Epson Scan 2 is not installed, install it again.

1. Check the Epson website for the latest firmware update releases.

   http://www.epson.com

   ❏ If there is the firmware for your scanner, download it and go to the next step.

   ❏ If there is no firmware information on the website, you are already using the latest firmware.
2. Connect the computer that contains the downloaded firmware to the scanner by USB cable.
3. Double-click the downloaded .exe file.

   Epson Firmware Updater starts.
4. Follow the on-screen instructions.