EPSON
EXCEED YOUR VISION

Administrator's Guide

NPD6411-00 EN

Contents

Appendix

Copyright and Trademarks

- ❏ EPSON is a registered trademark, and EPSON EXCEED YOUR VISION or EXCEED YOUR VISION is a trademark of Seiko Epson Corporation.
- ❏ Microsoft, Windows, and Windows Vista are registered trademarks of Microsoft Corporation.
- ❏ Mac OS, OS X, Bonjour, and Safari are registered trademarks of Apple Inc, registered in the U.S. and other countries.
- ❏ General Notice: Other product names used herein are for identification purposes only and may be trademarks of their respective owners. Epson disclaims any and all rights in those marks.

About this Manual

Marks and Symbols

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

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

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

Related Information

➡ Clicking this icon takes you to related information.

Artworks

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

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

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

Operating System References

Windows

In this manual, terms such as "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Vista", "Windows XP", "Windows Server 2012 R2", "Windows Server 2012","Windows Server 2008 R2", "Windows Server 2008", "Windows Server 2003 R2" and "Windows Server 2003" refer to the following operating systems. Additionally, "Windows" refers to all versions.

❏ Microsoft® Windows® 10 operating system

❏ Microsoft® Windows® 8.1 operating system

❏ Microsoft® Windows® 8 operating system

❏ Microsoft® Windows® 7 operating system

❏ Microsoft® Windows Vista® operating system

❏ Microsoft® Windows® XP operating system

❏ Microsoft® Windows® XP Professional x64 Edition operating system

❏ Microsoft® Windows Server® 2012 R2 operating system

- ❏ Microsoft® Windows Server® 2012 operating system
- ❏ Microsoft® Windows Server® 2008 R2 operating system
- ❏ Microsoft® Windows Server® 2008 operating system
- ❏ Microsoft® Windows Server® 2003 R2 operating system
- ❏ Microsoft® Windows Server® 2003 operating system

Mac OS X

In this manual, “Mac OS X v10.11.x” refers to OS X El Capitan“, Mac OS X v10.10.x” refers to OS X Yosemite, “Mac OS X v10.9.x” refers to OS X Mavericks, and “Mac OS X v10.8.x” refers to OS X Mountain Lion. Additionally, “Mac OS X” refers to “Mac OS X v10.11.x” , “Mac OS X v10.10.x” , “Mac OS X v10.9.x” , “Mac OS X v10.8.x” , “Mac OS X v10.7.x” , and “Mac OS X v10.6.8”.

Notices

- ❏ Reproduction of information in this manual is prohibited.
- ❏ All information in this manual is subject to change without notice.
- ❏ If you find inaccuracies or have concerns about this manual, contact Epson.
- ❏ Notwithstanding the preceding article, Epson cannot be held responsible for any effects resulting from the use of the product.
- ❏ Epson cannot be held responsible for any failures caused by the improper use of the product and the improper repair of the product by a third party.

Introduction

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

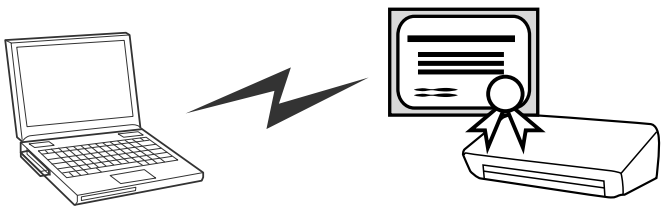
There are two pieces of software to configure the scanner's advanced network settings, Web Config and EpsonNet Config. In this manual, instructions for configuring each feature are basically from Web Config. For information on operations of EpsonNet Config, see the documentation or help of EpsonNet Config. Descriptions of the OS menu items are based on Windows 7 and Mac OS X 10.10.x.

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

Epson products support the following system administration functions. The available functions vary depending on the product. (Unavailable functions are not displayed on the scanner's control panel or software settings screen.) See the documentation to confirm what functions are available for your product.

SSL/TLS Communication

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



Related Information

➡ "Configuring SSL/TLS Communication" on page 15

Controlling Protocols

Scanners use many different protocols to communicate during scanning. By adding permissions or restrictions to individual protocols, you can control the protocols and prevent security risks from occurring due to unintended use.

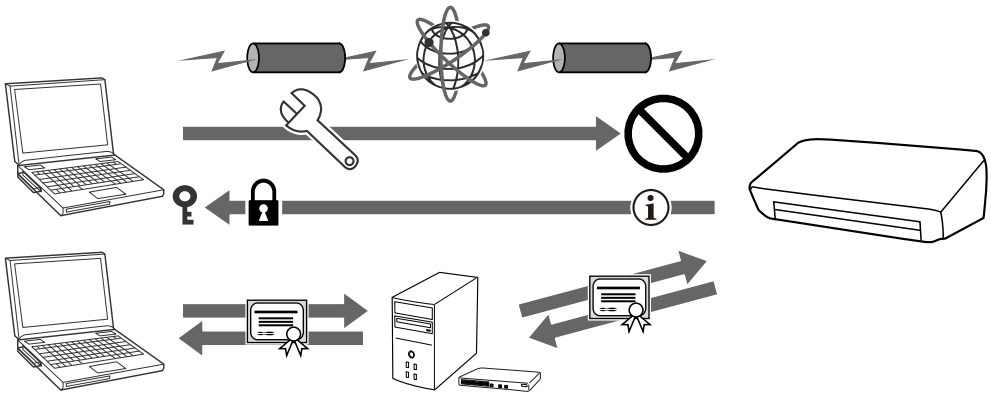
Related Information

➡ "Controlling Protocols and Services" on page 17

➡ "Configuring Protocols" on page 51

Encryption of IP Communication and Connection to an Authentication Network

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



Related Information

➡ “Configuring IPsec/IP Filtering” on page 18

➡ “Using SNMPv3 Protocol” on page 25

➡ “Connecting the Scanner to an IEEE802.1X Network” on page 27

Importing and Exporting the Scanner Settings

You can import and export the scanner settings. Use this feature when you want to copy the scanner settings to another scanner or when you replace the scanner.

Related Information

➡ “Exporting and Importing the Web Config Settings” on page 52

Using Network Configuration Software

About Web Config

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

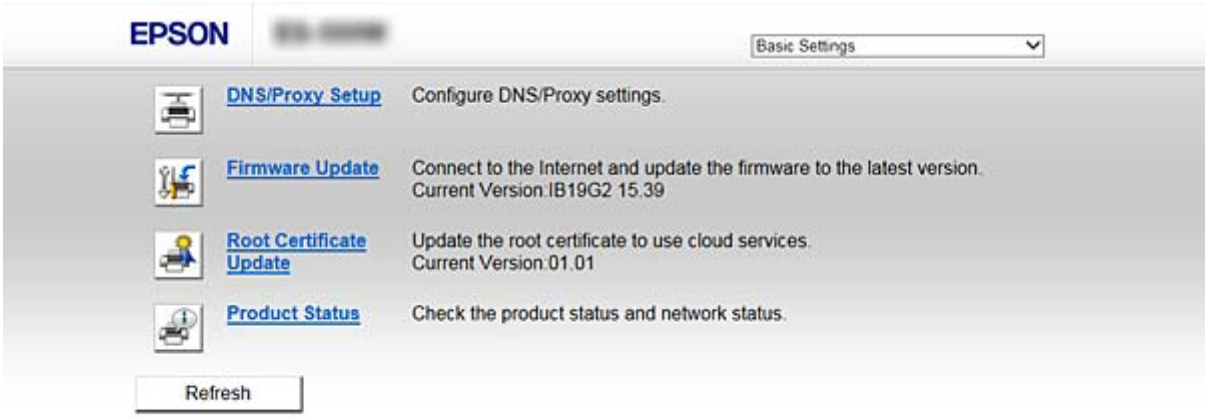
To access Web Config, you need to have first assigned an IP address to the scanner.

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

There are two setting pages as below.

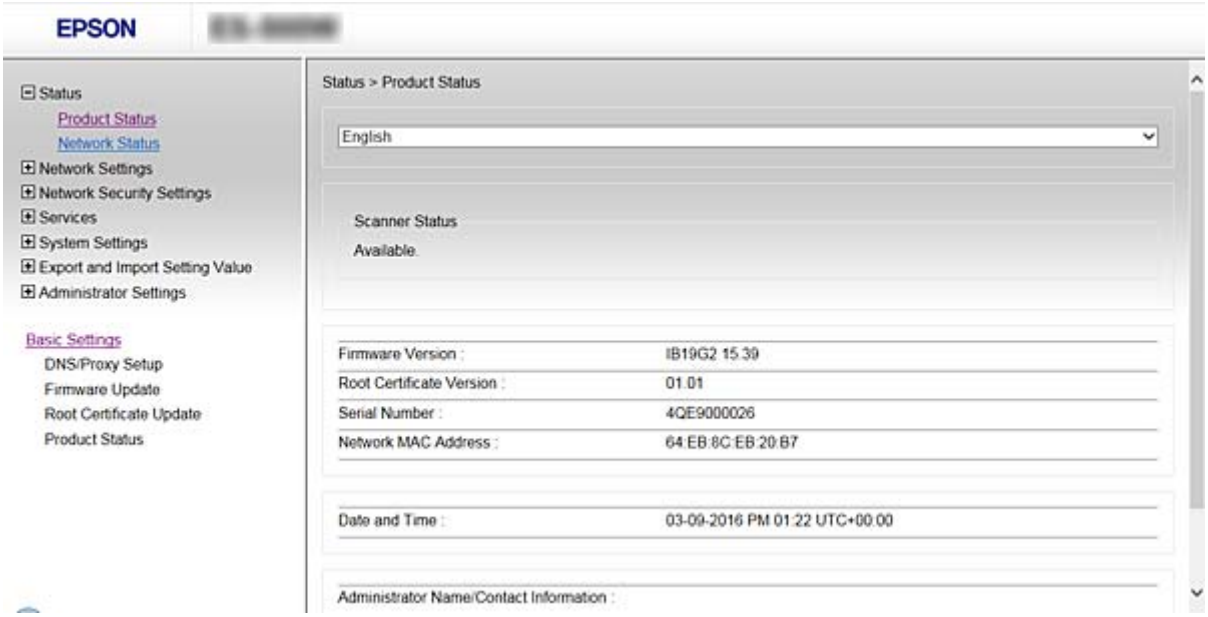
❏ **Basic Settings**

You can configure the basic settings for the scanner.



❏ **Advanced Settings**

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



Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 13

Accessing Web Config

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

❏ Accessing via HTTPS

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

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

❏ Accessing via HTTP

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

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

Note:

❏ *Examples*

IPv4:

https://192.168.100.201/

http://192.168.100.201/

IPv6:

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

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

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

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

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

Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 13

➡ "Configuring SSL/TLS Communication" on page 15

➡ "Using a Digital Certificate" on page 29

About EpsonNet Config

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

Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 13

Using EpsonNet Config – Windows

Installing EpsonNet Config – Windows

Download EpsonNet Config from Epson support website, and then install it by following the on-screen instructions.

Running EpsonNet Config - Windows

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

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

Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 13

Uninstalling EpsonNet Config - Windows

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

Using EpsonNet Config – Mac OS X

Installing EpsonNet Config – Mac OS X

Download EpsonNet Config from Epson support website, and then install it by following the on-screen instructions.

Running EpsonNet Config - Mac OS X

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

Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 13

Uninstalling EpsonNet Config – Mac OS X

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

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

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

Web Config and EpsonNet Config Feature Comparison

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

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

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

Related Information

➡ "About Web Config" on page 9
➡ "Accessing Web Config" on page 10
➡ "About EpsonNet Config" on page 11
➡ "Running EpsonNet Config - Windows" on page 12
➡ "Running EpsonNet Config - Mac OS X" on page 12
➡ "Configuring Basic SSL/TLS Settings" on page 15
➡ "Configuring a Server Certificate for the Scanner" on page 16
➡ "Configuring IPsec/IP Filtering" on page 18
➡ "Using SNMPv3 Protocol" on page 25
➡ "Connecting the Scanner to an IEEE802.1X Network" on page 27

➡ “Obtaining and Importing a CA-signed Certificate” on page 30
➡ “Updating a Self-signed Certificate” on page 34
➡ “Using an Email Server” on page 45
➡ “Configuring the Administrator Password” on page 50
➡ “Configuring Email Notification” on page 49
➡ “Exporting and Importing the Web Config Settings” on page 52

Other Network Software

About Epson Device Admin

Epson Device Admin is an application that allows you to install devices on the network, and then configure and manage the devices. You can make a template containing setting items and apply it to other devices as shared settings. You can download Epson Device Admin from Epson support website. For more information, see the documentation or help of Epson Device Admin.

About EpsonNet SetupManager

EpsonNet SetupManager is a software to create a package for a simple scanner installation, such as installing and configuring the scanner software.

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

For more information, visit your regional Epson website.

Using the Scanner in a Secure Network

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

Configuring SSL/TLS Communication

Configuring Basic SSL/TLS Settings

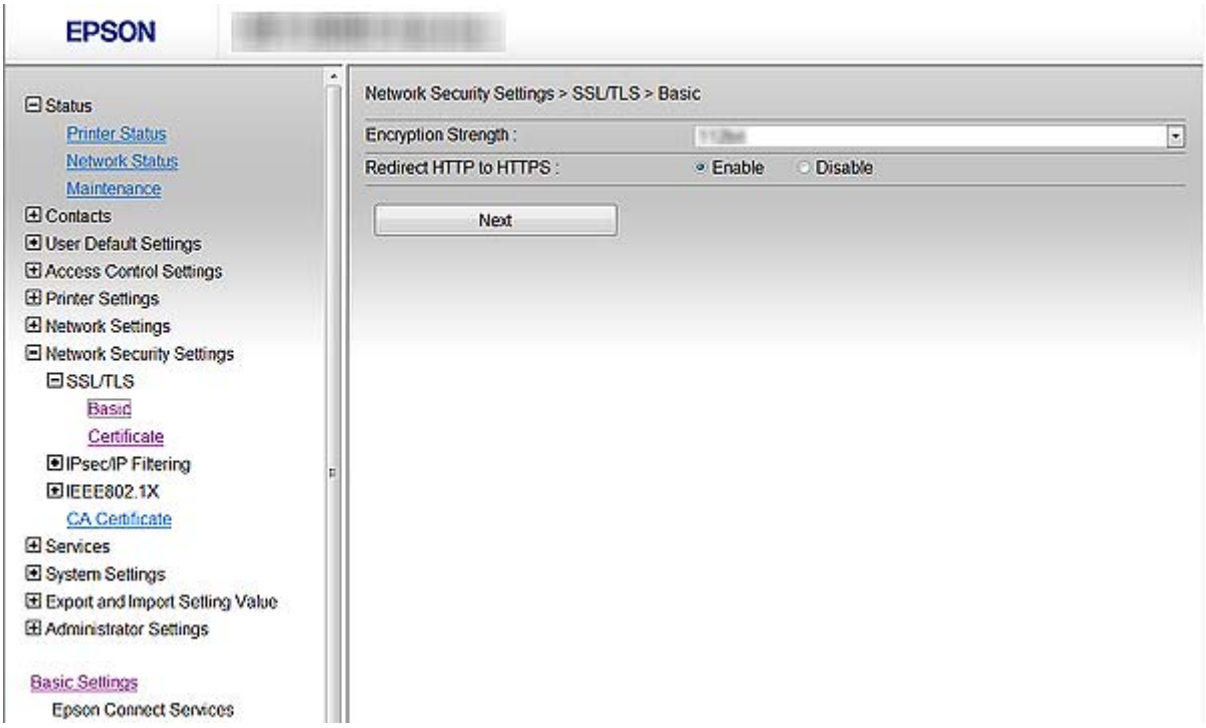
If the scanner supports the HTTPS server feature, you can use an SSL/TLS communication to encrypt communications. You can configure and manage the scanner using Web Config while ensuring security.

Configure encryption strength and redirect feature.

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

➡ "Accessing Web Config" on page 10

Configuring a Server Certificate for the Scanner

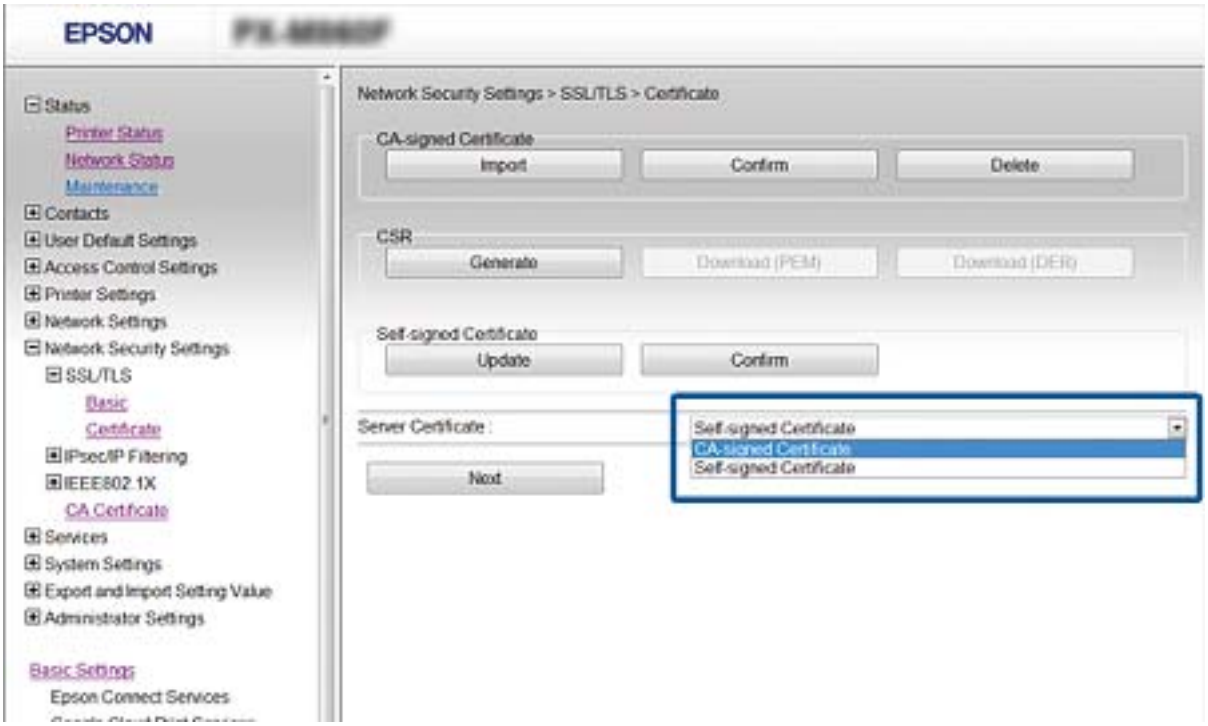
1. Access Web Config and select **Network Security Settings** >**SSL/TLS**> **Certificate**.
2. Specify a certificate to use on **Server Certificate**.

   ❏ **Self-signed Certificate**

   A self-signed certificate has been generated by the 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

➡ "Accessing Web Config" on page 10

➡ “Obtaining and Importing a CA-signed Certificate” on page 30

Controlling Protocols and Services

You can scan using a variety of pathways and protocols, and 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.

1. Access Web Config and select **Services** > **Protocol**.
2. Configure each item.
3. Click **Next**.
4. Click **OK**

   The settings are applied to the scanner.

Protocols you can Enable or Disable

Protocol	Description
Bonjour Settings	You can specify whether to use Bonjour. Bonjour is used to search for devices, scan, and so on.
SLP Settings	You can enable or disable the 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 or scan from the WSD port.
LLTD Settings	You can enable or disable the LLTD function. When this is enabled, it is displayed on the Windows network map.
LLMNR Settings	You can enable or disable the LLMNR function. When this is enabled, you can use name resolution without NetBIOS even if you cannot use DNS.
SNMPv1/v2c Settings	You can specify whether or not to enable SNMPv1/v2c. This is used to set up devices, monitoring, and so on.

Controlling the Services

Enable or disable the services such as network scanning.

1. Access Web Config and select **Services**.
2. Enable or disable the items.

   Configurable items differ depending on the scanner.

3. Click **Next**.
4. Click **OK**.

Services you can Enable or Disable

Service	Description
Network Scan	You can specify whether or not to use Network Scan. When this is enabled, you can use the scanning function from networked computers.
AP mode	You can specify whether or not to enable AP mode. When this is enabled, you can connect devices using AP mode.

Configuring IPsec/IP Filtering

About IPsec/IP Filtering

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

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

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

Configuring Default Policy

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

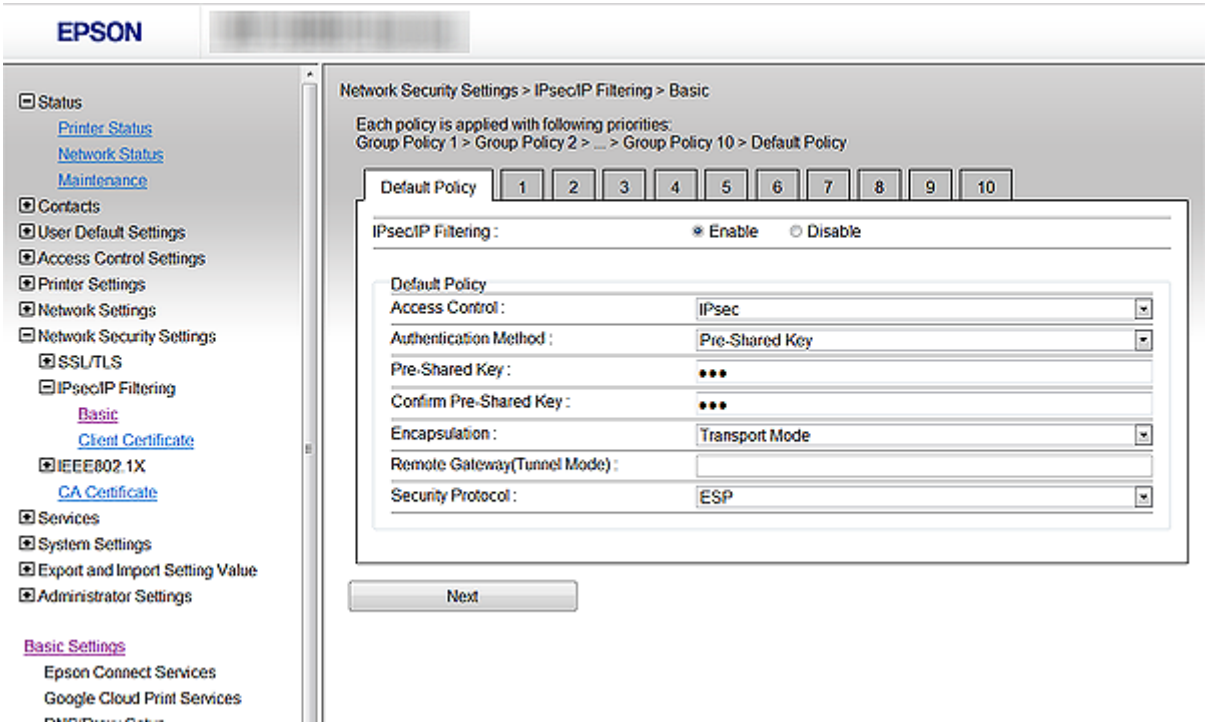
   A confirmation message is displayed.
4. Click **OK**.

   The scanner is updated.

Related Information

➡ “Accessing Web Config” on page 10
➡ “Default Policy Setting Items” on page 19

Default Policy Setting Items



Items	Settings and Explanation	
IPsec/IP Filtering	You can enable or disable an IPsec/IP Filtering feature.	
Access Control	Configure a control method for traffic of IP packets.	
	Permit Access	Select this to permit configured IP packets to pass through.
	Refuse Access	Select this to refuse configured IP packets to pass through.
	IPsec	Select this to permit configured IPsec packets to pass through.
Authentication Method	To select **Certificate**, you need to obtain and import a CA-signed certificate in advance.	
Pre-Shared Key	If you select **Pre-Shared Key** for **Authentication Method**, enter a pre-shared key between 1 and 127 characters.	
Confirm Pre-Shared Key	Enter the key you configured for confirmation.	
Encapsulation	If you select **IPsec** for **Access Control**, you need to configure an encapsulation mode.	
	Transport Mode	If you only use the 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.	

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

Related Information

➡ "Configuring Default Policy" on page 18

Configuring Group Policy

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

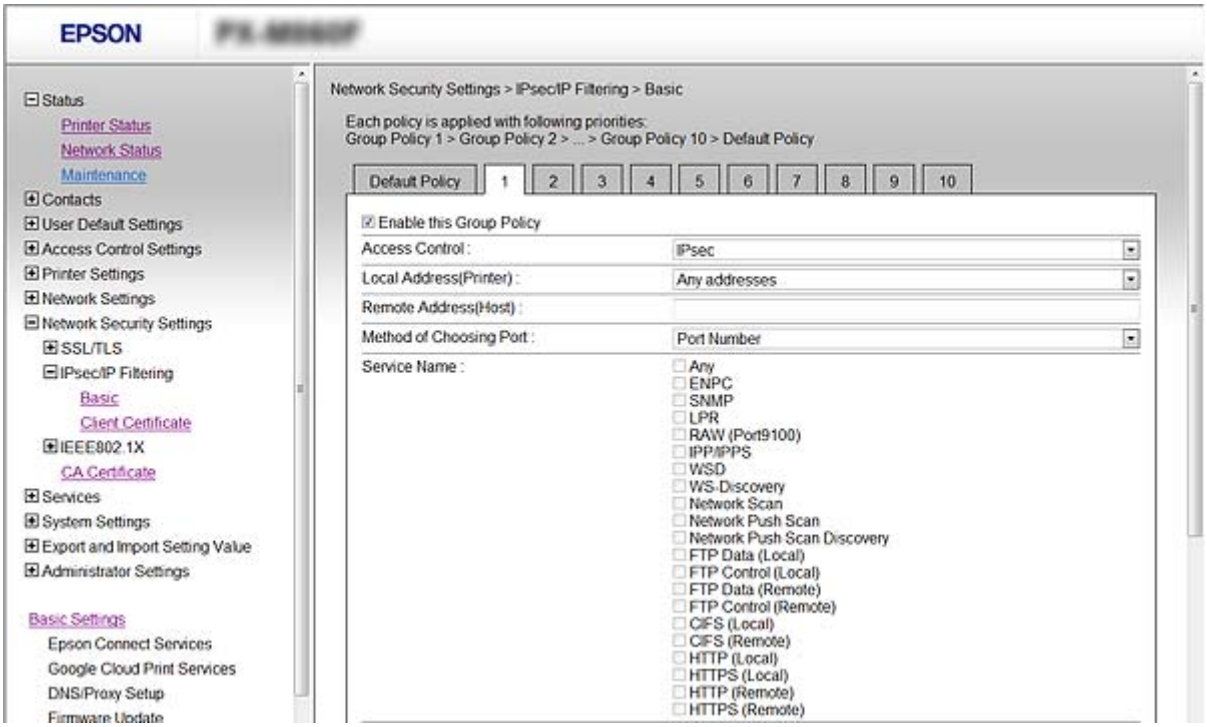
   A confirmation message is displayed.
5. Click **OK**.

   The scanner is updated.

Related Information

➡ "Accessing Web Config" on page 10
➡ "Group Policy Setting Items" on page 21

Group Policy Setting Items



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

Items	Settings and Explanation	
Transport Protocol	If you select **Port Number** for **Method of Choosing Port**, you need to configure an encapsulation mode.	
	Any Protocol	Select this to control all protocol types.
	TCP	Select this to control data for unicast.
	UDP	Select this to control data for broadcast and multicast.
	ICMPv4	Select this to control ping command.
Local Port	If you select **Port Number** for **Method of Choosing Port** and if you select **TCP** or **UDP** for **Transport Protocol**, enter port numbers to control receiving packets, separating them with commas. You can enter 10 port numbers at the maximum. Example: 20,80,119,5220 If you do not enter a port number, all ports are controlled.	
Remote Port	If you select **Port Number** for **Method of Choosing Port** and if you select **TCP** or **UDP** for **Transport Protocol**, enter port numbers to control sending packets, separating them with commas. You can enter 10 port numbers at the maximum. Example: 25,80,143,5220 If you do not enter a port number, all ports are controlled.	
Authentication Method	If you select **IPsec** for **Access Control**, select an option. Used certificate is common with a default policy.	
Pre-Shared Key	If you select **Pre-Shared Key** for **Authentication Method**, enter a pre-shared key between 1 and 127 characters.	
Confirm Pre-Shared Key	Enter the key you configured for confirmation.	
Encapsulation	If you select **IPsec** for **Access Control**, you need to configure an encapsulation mode.	
	Transport Mode	If you only use the 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.	
	ESP	Select this to ensure the integrity of an authentication and data, and encrypt data.
	AH	Select this to ensure the integrity of an authentication and data. Even if encrypting data is prohibited, you can use IPsec.

Related Information

➡ “Configuring Group Policy” on page 20

➡ “Combination of Local Address (Scanner) and Remote Address(Host) on Group Policy” on page 23

➡ “References of Service Name on Group Policy” on page 23

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	✓	✓	✓

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

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

*3Except IPv6 link local addresses.

References of Service Name on Group Policy

Note:
Unavailable services are displayed but cannot be selected.

Service Name	Protocol type	Local port number	Remote port number	Features controlled
Any	–	–	–	All services
ENPC	UDP	3289	Any port	Searching for a scanner from applications such as EpsonNet Config and the a scanner driver
SNMP	UDP	161	Any port	Acquiring and configuring of MIB from applications such as EpsonNet Config and the Epson scanner driver
WSD	TCP	Any port	5357	Controlling WSD
WS-Discovery	UDP	3702	Any port	Searching for a scanner from WSD
Network Scan	TCP	1865	Any port	Forwarding scan data from the scanner software
HTTP (Local)	TCP	80	Any port	HTTP(S) server (forwarding data of Web Config and WSD)
HTTPS (Local)	TCP	443	Any port	
HTTP (Remote)	TCP	Any port	80	HTTP(S) client (communicating between firmware updating and root certificate updating)
HTTPS (Remote)	TCP	Any port	443	

Configuration Examples of IPsec/IP Filtering

Receiving IPsec packets only

This example is to configure a default policy only.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

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

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

Group Policy: 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.

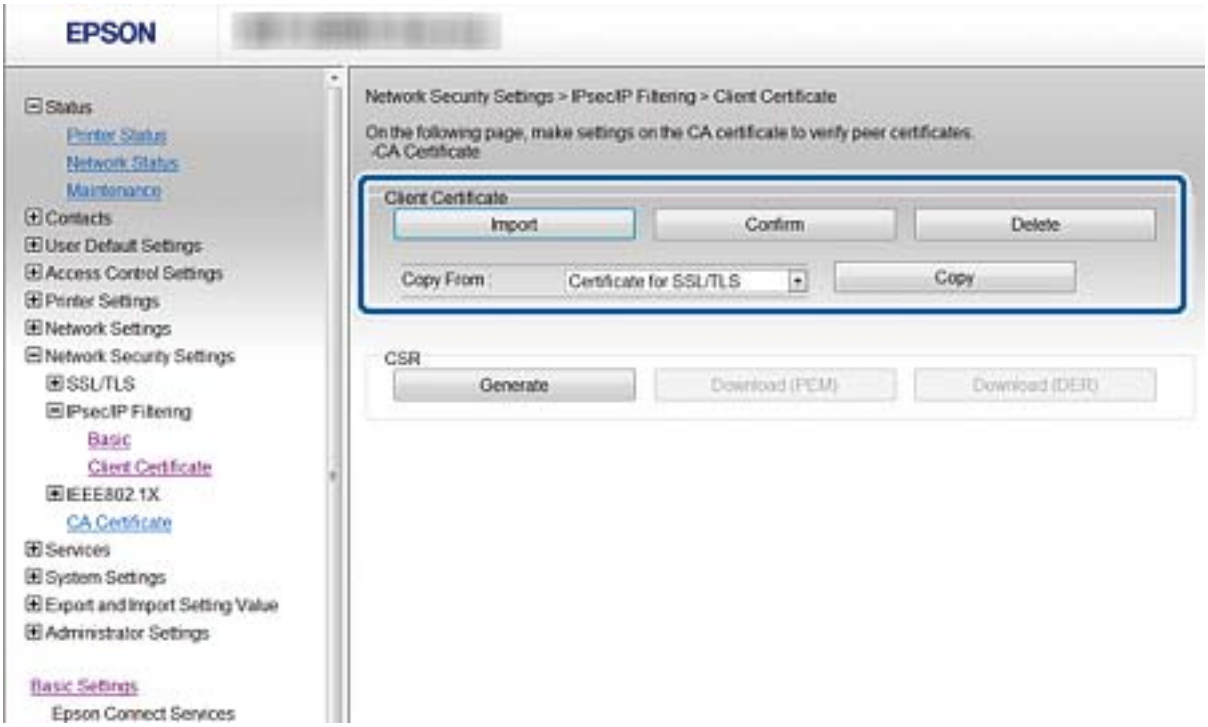
Configuring a Certificate for IPsec/IP Filtering

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

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

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

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



Related Information

➡ "Accessing Web Config" on page 10

➡ "Obtaining and Importing a CA-signed Certificate" on page 30

Using SNMPv3 Protocol

Configuring SNMPv3

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

1. Access Web Config and select **Services** > **Protocol** .
2. Enter a value for each item of **SNMPv3 Settings**.
3. Click **Next**.

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

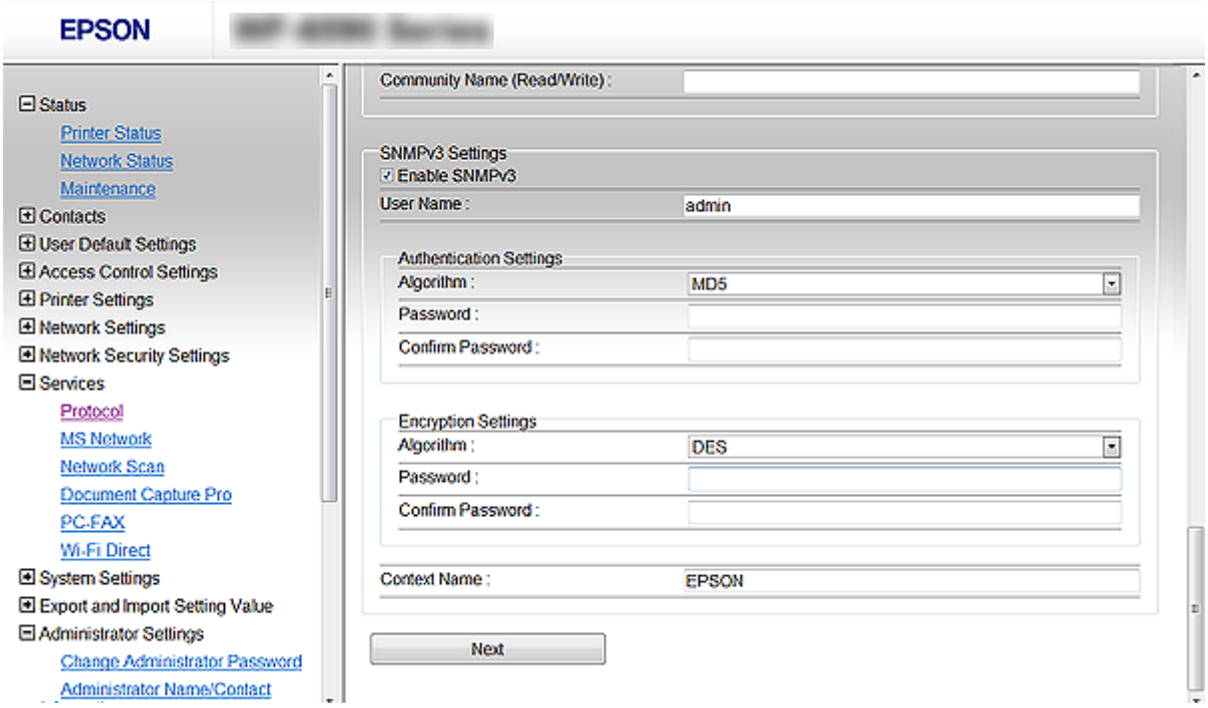
   The scanner is updated.

Related Information

➡ “Accessing Web Config” on page 10

➡ “SNMPv3 Setting Items” on page 26

SNMPv3 Setting Items



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

Related Information

➡ “Configuring SNMPv3” on page 25

Connecting the Scanner to an IEEE802.1X Network

Configuring an IEEE802.1X Network

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

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

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

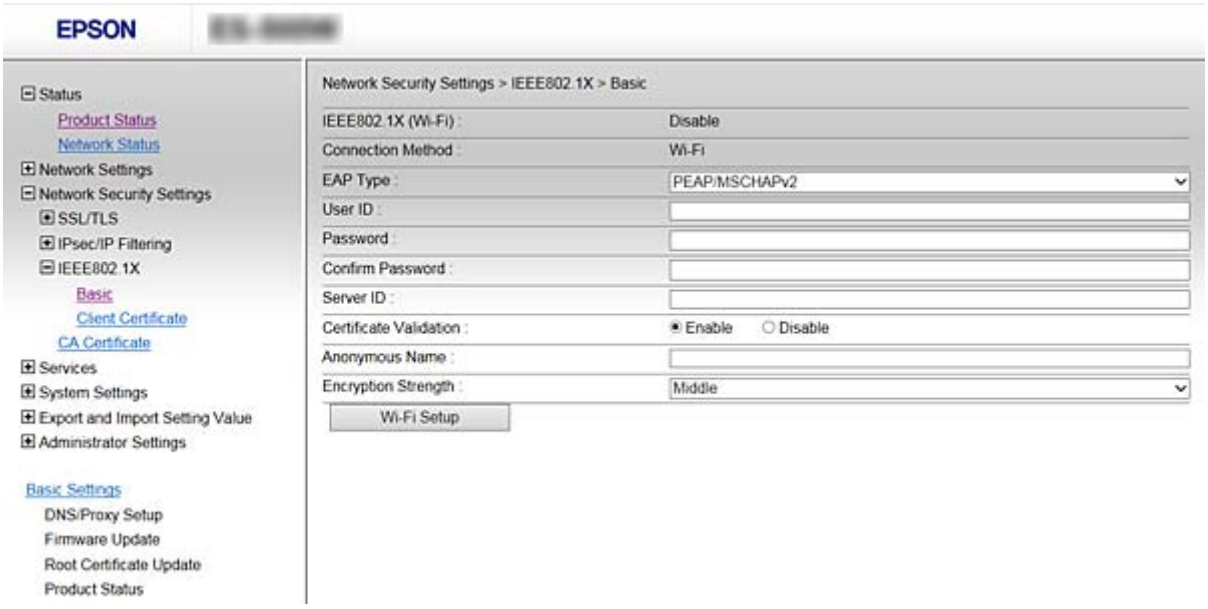
   A confirmation message is displayed.
4. Click **OK**.

   The scanner is updated.

Related Information

➡ "Accessing Web Config" on page 10
➡ "IEEE802.1X Network Setting Items" on page 27
➡ "Cannot Access the Scanner after Configuring IEEE802.1X" on page 40

IEEE802.1X Network Setting Items



Items	Settings and Explanation
IEEE802.1X (Wi-Fi)	The connection status of IEEE802.1X (Wi-Fi) is displayed.

Items	Settings and Explanation	
Connection Method	The connection method of a current network is displayed.	
EAP Type	Select an option for an authentication method between the scanner and a RADIUS server.	
	EAP-TLS	You need to obtain and import a CA-signed certificate.
	PEAP-TLS	
	PEAP/MSCHAPv2	You need to configure a password.
User ID	Configure an ID to use for an authentication of a RADIUS server. Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters.	
Password	Configure a password to authenticate the scanner. Enter 1 to 128 1-byte ASCII (0x20 to 0x7E) characters. If you are using a Windows server as a RADIUS server, you can enter up to 127 characters.	
Confirm Password	Enter the password you configured for confirmation.	
Server ID	You can configure a server ID to authenticate with a specified RADIUS server. Authenticator verifies whether a server ID is contained in the subject/subjectAltName field of a server certificate that is sent from a RADIUS server or not. Enter 0 to 128 1-byte ASCII (0x20 to 0x7E) characters.	
Certificate Validation	You can set certificate validation regardless of the authentication method. Import the certificate in **CA Certificate**.	
Anonymous Name	If you select **PEAP-TLS** or **PEAP/MSCHAPv2** for **Authentication Method**, you can configure an anonymous name instead of a user ID for a phase 1 of a PEAP authentication. Enter 0 to 128 1-byte ASCII (0x20 to 0x7E) characters.	
Encryption Strength	You can select one of the followings.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Related Information

➡ "Configuring an IEEE802.1X Network" on page 27

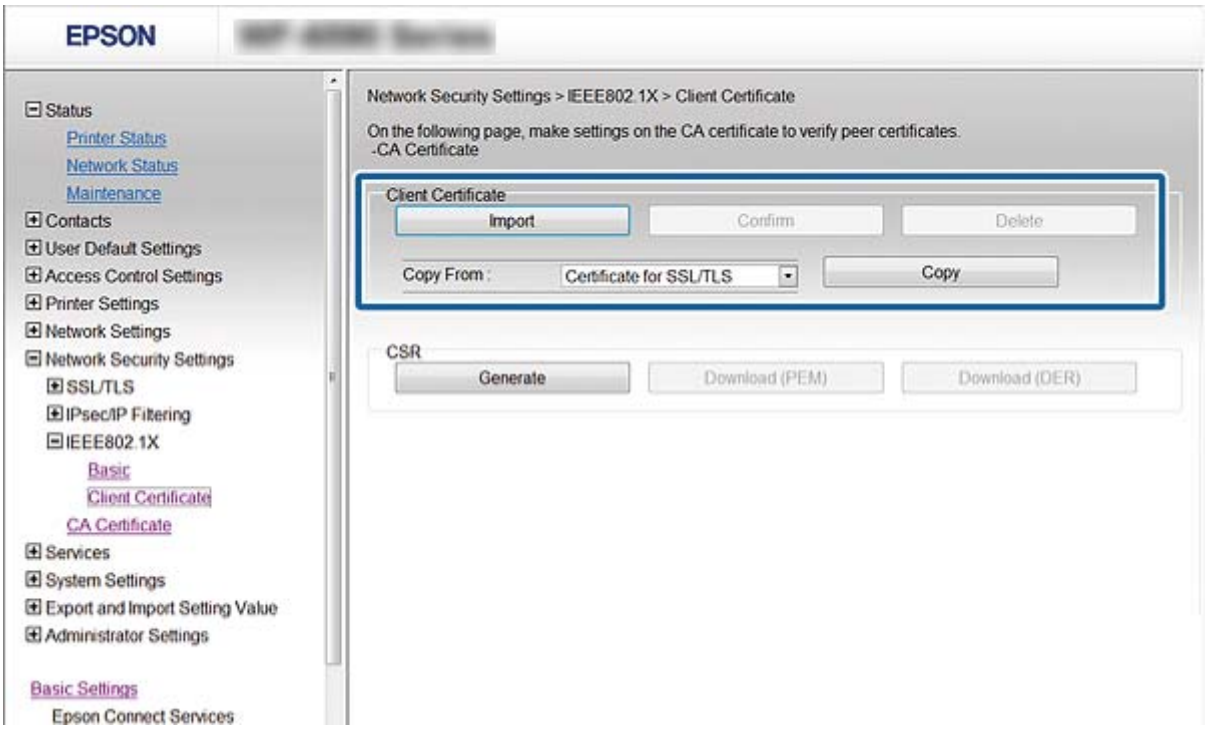
Configuring a Certificate for IEEE802.1X

Configure the Client Certificate for IEEE802.1X. If you want to configure the certification authority certificate, go to **CA Certificate**.

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

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

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



Related Information

➡ "Accessing Web Config" on page 10

➡ "Obtaining and Importing a CA-signed Certificate" on page 30

Using a Digital Certificate

About Digital Certification

❏ Certificate signed by a CA

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

❏ CA certificate

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

❏ Self-signed certificate

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

Related Information

➡ "Web Config and EpsonNet Config Feature Comparison" on page 13
➡ "Obtaining and Importing a CA-signed Certificate" on page 30
➡ "Deleting a CA-signed Certificate" on page 33
➡ "Updating a Self-signed Certificate" on page 34

Obtaining and Importing a CA-signed Certificate

Obtaining a CA-signed Certificate

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

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

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

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

   A CSR creating page is opened.

3. Enter a value for each item.

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

4. Click **OK**.

   A completion message is displayed.

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

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

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

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

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

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

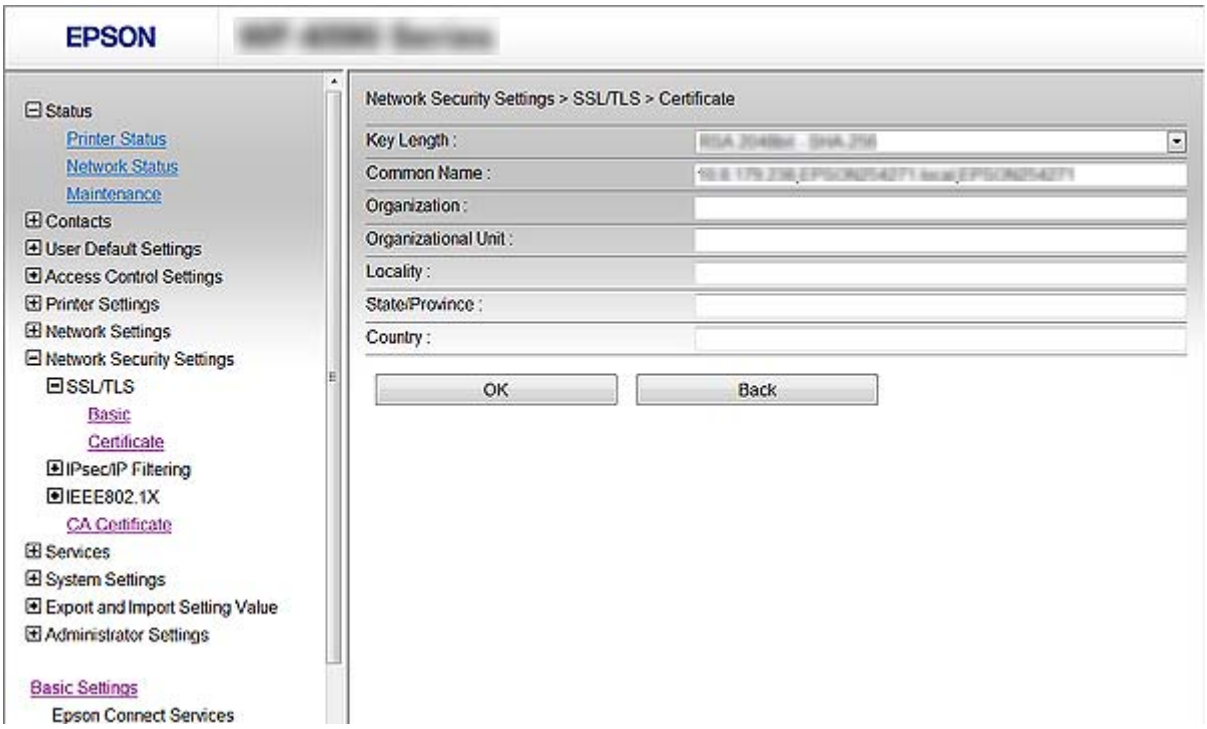
   Obtaining a CA-signed Certificate is complete when you save a certificate to a destination.

Related Information

➡ "Accessing Web Config" on page 10

➡ "CSR Setting Items" on page 31
➡ "Importing a CA-signed Certificate" on page 32

CSR Setting Items



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

Related Information

➡ "Obtaining a CA-signed Certificate" on page 30

Importing a CA-signed Certificate

Important:

❏ *Make sure that the scanner's date and time is set correctly.*

❏ *If you obtain a certificate using a CSR created from Web Config, you can import a certificate one time.*

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

2. Click **Import**.

   A certificate importing page is opened.

3. Enter a value for each item.

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

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

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

      ❏ **Password**: Do not configure.

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

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

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

      ❏ **Password**: Do not configure.

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

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

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

      ❏ **Password**: Optional

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

4. Click **OK**.

   A completion message is displayed.

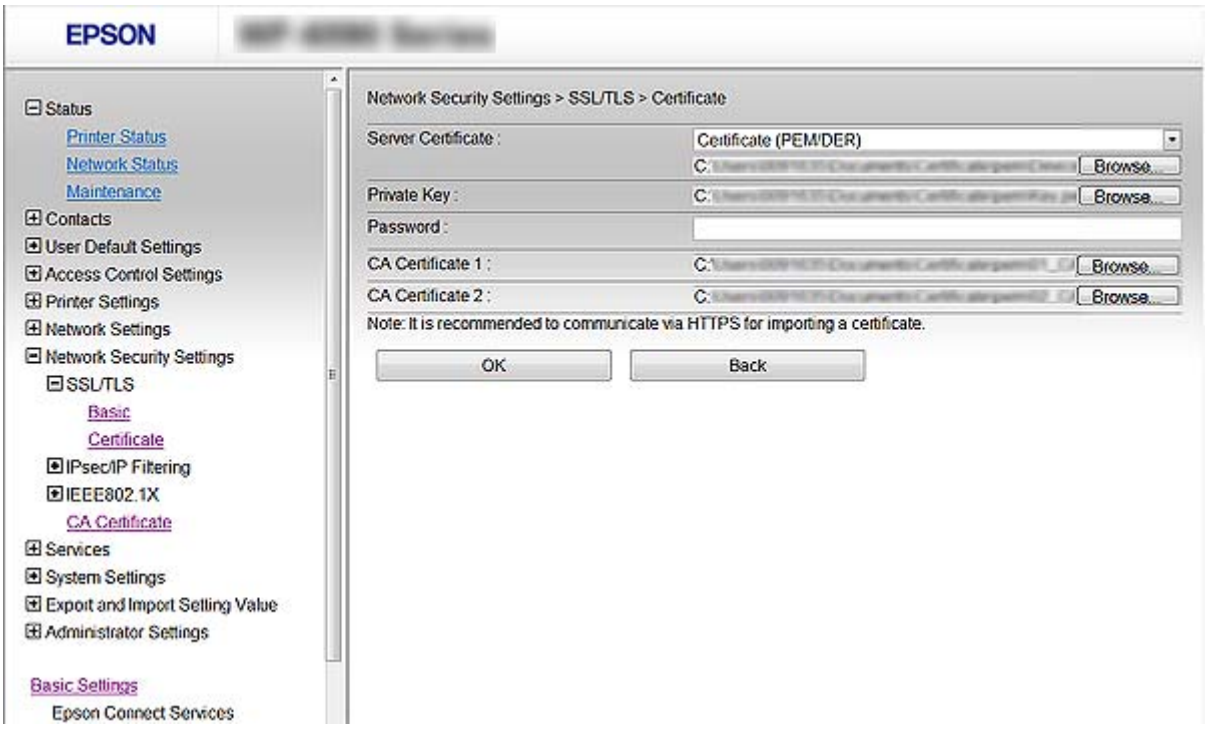
Note:
*Click **Confirm** to verify the certificate information.*

Related Information

➡ "Accessing Web Config" on page 10

➡ "CA-signed Certificate Importing Setting Items" on page 33

CA-signed Certificate Importing Setting Items



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

Related Information

➡ "Importing a CA-signed Certificate" on page 32

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

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

Related Information

➡ "Accessing Web Config" on page 10

Updating a Self-signed Certificate

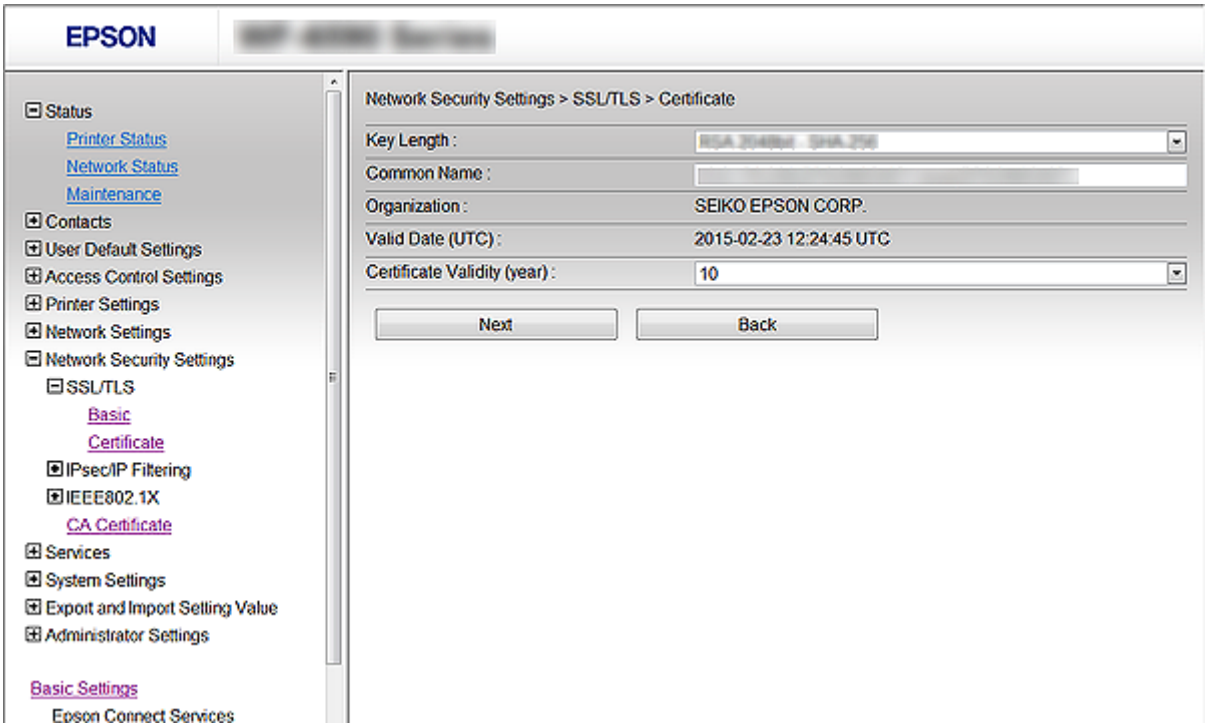
If the scanner supports the HTTPS server feature, you can update a self-signed certificate. When accessing Web Config using a self-signed certificate, a warning message appears.

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

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

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

   Note:
   You can separate distinguished name (CN) with commas.
4. Specify a validity period for the certificate.



5. Click **Next**.

   A confirmation message is displayed.

6. Click **OK**.

   The scanner is updated.

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

Related Information

➡ "Accessing Web Config" on page 10

Configure CA Certificate

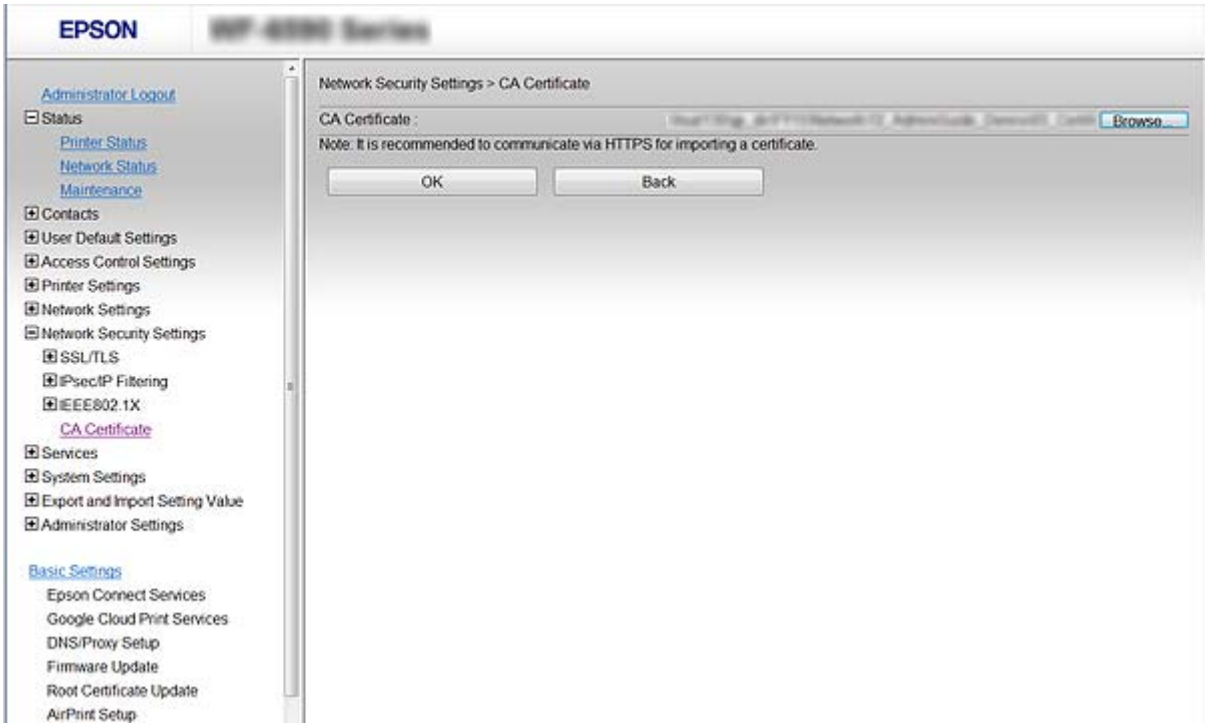
You can import, display, delete a CA Certificate.

Importing a CA Certificate

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

2. Click **Import**.

3. Specify the CA Certificate you want to import.



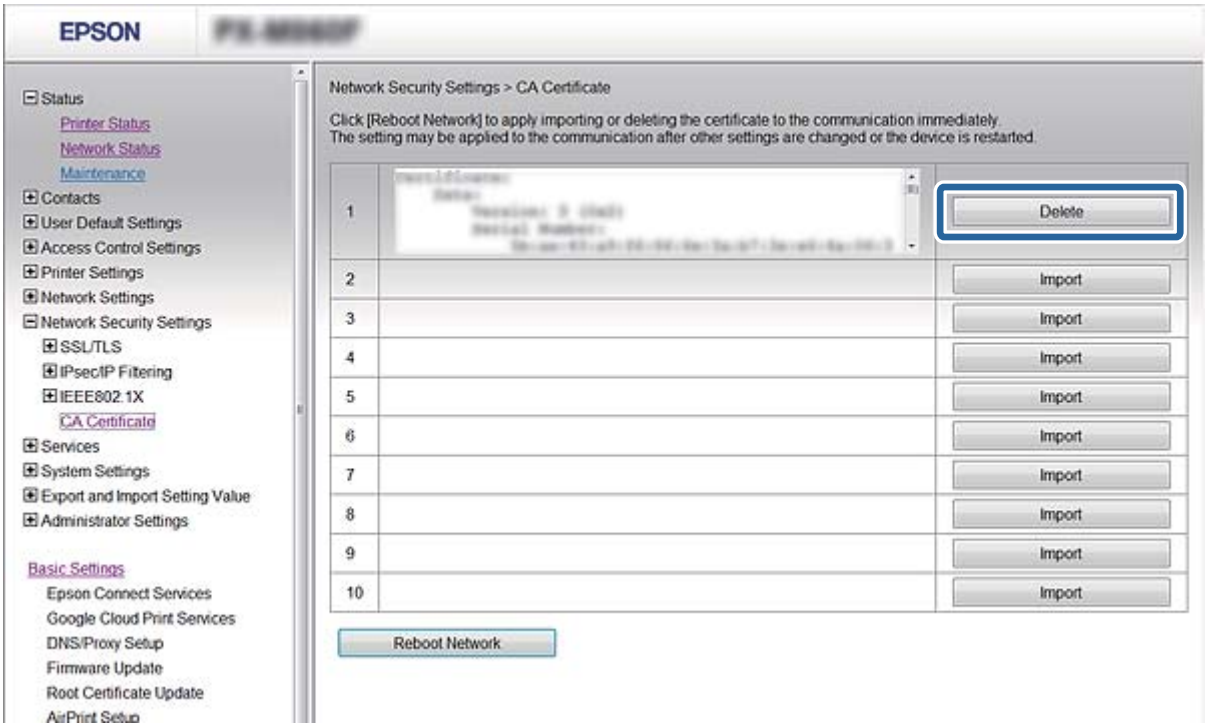
4. Click **OK**.

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

Deleting a CA Certificate

You can delete the imported CA Certificate.

1. Access Web Config, and then select **Network Security Settings** > **CA Certificate**.
2. Click **Delete** next to the CA Certificate that you want to delete.



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

Rebooting the Network

After importing or deleting a CA Certificate, reboot the network to reflect the changes.

1. Access Web Config, and then select **Network Security Settings** > **CA Certificate**.
2. Click **Reboot Network**.
3. Confirm the message and continue.

Solving Problems

Tips for Solving Problems

You can find more information in the following manuals.

❏ User's Guide (PDF manual)

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

Problems Using Network Software

Cannot Access Web Config

Is the IP address of the scanner properly configured?

Configure the IP address using EpsonNet Config or Epson Scan 2 Utility.

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

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

❏ 80bit: AES256/AES128/3DES

❏ 112bit: AES256/AES128/3DES

❏ 128bit: AES256/AES128

❏ 192bit: AES256

❏ 256bit: AES256

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

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

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

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

The scanner is being accessed via a proxy server.

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

❏ Windows:

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

❏ Mac OS X:

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

Example:

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

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

Related Information

➡ "Accessing Web Config" on page 10

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

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

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

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

Is the communication error timeout setting too short?

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

Related Information

➡ "Running EpsonNet Config - Windows" on page 12

➡ "Running EpsonNet Config - Mac OS X" on page 12

Problems Using Network Security Features

Forgot a Pre–shared Key

Configure the key again using Web Config.

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

Cannot Communicate with IPsec Communication

Are you using an unsupported algorithm for the computer settings?

The scanner supports the following algorithms.

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

*Available method may vary by models.

Related Information

➡ "Configuring IPsec/IP Filtering" on page 18

Cannot Communicate Suddenly

Is there an error in the certificate?

The scanner's date and time settings may be incorrect if power has not been supplied to the scanner for a long time.

When the scanner is connected using a client certificate for IPsec/IP filtering or IEEE802.1X, an error is indicated if a time lag occurs between the scanner's date and time and the validity period for the certificate. Because the scanner recognizes that the certificate is unavailable. For details on the scanner's error indicators, see the scanner's *User's Guide*.

You can solve this problem by correcting the scanner's date and time settings. Connect the scanner and the computer using a USB cable, turn the scanner on, and then perform scanning over USB using Epson ScanSmart. The scanner is synchronized with the computer and the date and time settings are corrected. The scanner indicates normal status.

If you cannot solve the problem, restore all network settings using the scanner's control panel. Connect the scanner and computer, make the network settings again, and then make the settings for client certification, IPsec/IP filtering, or IEEE802.1X.

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

Access the scanner through its MAC address using EpsonNet Config or EPSON Device Admin from another computer such as an administrator's computer. You can find the MAC address on the label stuck to the scanner.

When access is possible, change the scanner's IP address using EpsonNet Config or EPSON Device Admin. Use a static IP address.

When access is not possible, restore all network settings using the scanner's control panel. Connect the scanner and computer, and then make the network settings again. Use a static IP address when setting the scanner's IP address.

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

Access the scanner according to its MAC address using EpsonNet Config or EPSON Device Admin from another computer, such as administrator's. You can find the MAC address on the label pasted on the scanner.

If you can access, change the computer's IP address using EpsonNet Config or EPSON Device Admin. Use a static IP address.

If you cannot access, restore all network settings using the scanner's control panel. Connect the scanner and computer, and then make the network settings again. Use a static IP address when setting the computer's IP address.

Related Information

➡ "Configuring IPsec/IP Filtering" on page 18

Cannot Connect After Configuring IPsec/IP Filtering

The set value may be incorrect.

Access the scanner according to its MAC address using EpsonNet Config or EPSON Device Admin from another computer, such as administrator's. You can find the MAC address on the label pasted on the scanner.

If you can access, make the IPsec/IP filtering settings using EpsonNet Config or EPSON Device Admin.

If you cannot access, restore all network settings using the scanner's control panel. Connect the scanner and computer, make the network settings again, and then make the IPsec/IP filtering settings.

Related Information

➡ "Configuring IPsec/IP Filtering" on page 18

Cannot Access the Scanner after Configuring IEEE802.1X

The settings may be incorrect.

Restore all network settings using the scanner's control panel. Connect the scanner and computer, make the network settings again, and then configure IEEE802.1X.

Related Information

➡ "Configuring an IEEE802.1X Network" on page 27

Problems on Using a Digital Certificate

Cannot Import a CA-signed Certificate

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

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

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

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

Is the CA-signed certificate more than 5KB?

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

Is the password for importing the certificate correct?

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

Related Information

➡ "Importing a CA-signed Certificate" on page 32

Cannot Update a Self-Signed Certificate

Has the Common Name been entered?

Common Name must be entered.

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

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

Is a comma or space included in the Common Name?

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

Related Information

➡ "Updating a Self-signed Certificate" on page 34

Cannot Create a CSR

Has the Common Name been entered?

The **Common Name** must be entered.

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

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

Is a comma or space included in the Common Name?

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

Related Information

➡ "Obtaining a CA-signed Certificate" on page 30

Warning Relating to a Digital Certificate Appears

Messages	Cause/What to do
Enter a Server Certificate.	**Cause:** You have not selected a file to import. **What to do:** Select a file and click **Import**.
CA Certificate 1 is not entered.	**Cause:** CA certificate 1 is not entered and only CA certificate 2 is entered. **What to do:** Import CA certificate 1 first.
Invalid value below.	**Cause:** Unsupported characters are contained in the file path and/or password. **What to do:** Make sure that the characters are entered correctly for the item.
Invalid date and time.	**Cause:** Date and time for the scanner have not been set. **What to do:** Set date and time using Web Config or EpsonNet Config.
Invalid password.	**Cause:** The password set for CA certificate and entered password do not match. **What to do:** Enter the correct password.

Messages	Cause/What to do
Invalid file.	**Cause:** You are not importing a certificate file in X509 format. **What to do:** Make sure that you are selecting the correct certificate sent by a trusted certificate authority.
	Cause: The file you have imported is too large. The maximum file size is 5KB. **What to do:** If you select the correct file, the certificate might be corrupted or fabricated.
	Cause: The chain contained in the certificate is invalid. **What to do:** For more information on the certificate, see the website of the certificate authority.
Cannot use the Server Certificates that include more than three CA certificates.	**Cause:** The certificate file in PKCS#12 format contains more than 3 CA certificates. **What to do:** Import each certificate as converting from PKCS#12 format to PEM format, or import the certificate file in PKCS#12 format that contains up to 2 CA certificates.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Cause:** The certificate is out of date. **What to do:** ❏ If the certificate is out of date, obtain and import the new certificate. ❏ If the certificate is not out of date, make sure the scanner's date and time are set correctly.
Private key is required.	**Cause:** There is no paired private key with the certificate. **What to do:** ❏ If the certificate is the PEM/DER format and it is obtained from a CSR using a computer, specify the private key file. ❏ If the certificate is the PKCS#12 format and it is obtained from a CSR using a computer, create a file that contains the private key.
	Cause: You have re-imported the PEM/DER certificate obtained from a CSR using Web Config. **What to do:** If the certificate is the PEM/DER format and it is obtained from a CSR using Web Config, you can only import it once.

Messages	Cause/What to do
Setup failed.	**Cause:** Cannot finish the configuration because the communication between the scanner and computer failed or the file cannot be read by some errors. **What to do:** After checking the specified file and communication, import the file again.

Related Information

➡ "About Digital Certification" on page 29

Delete a CA-signed Certificate by Mistake

Is there a backup file for the certificate?

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

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

Related Information

➡ "Deleting a CA-signed Certificate" on page 33

Scanning Problems

Cannot Perform WSD Scanning

Is the WSD port blocked?

You may not be able to scan if a firewall is blocking communication for WSD. Make sure that the WSD port (port: 5357) on the computer is available.

Appendix

Using an Email Server

To use email features, you need to configure the email server.

Configuring a Mail Server

Check the following before configuring.

❏ The scanner is connected to a network.

❏ The computer's email server information.

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

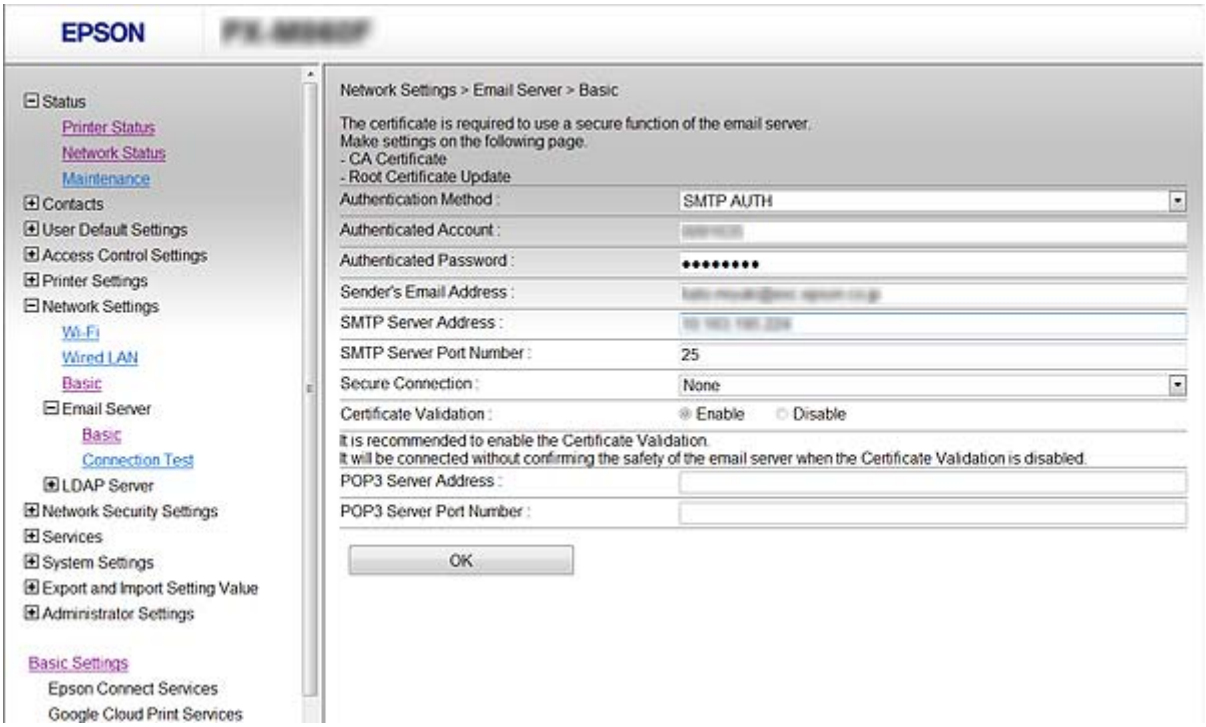
   The settings you have selected are displayed.

Related Information

➡ "Accessing Web Config" on page 10

➡ "Mail Server Setting Items" on page 46

Mail Server Setting Items



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

Items	Settings and Explanation	
Secure Connection	Specify the secure connection method for the email server.	
	None	If you select **POP before SMTP** in **Authentication Method**, the connection method is set to **None**.
	SSL/TLS	This is available when **Authentication Method** is set to **Off** or **SMTP AUTH**.
	STARTTLS	This is available when **Authentication Method** is set to **Off** or **SMTP AUTH**.
Certificate Validation	The certificate is validated when this is enabled. We recommend this is set to **Enable**.	
POP3 Server Address	If you select **POP before SMTP** as the **Authentication Method**, enter the POP3 server address between 0 and 255 characters using A-Z a-z 0-9 . - . You can use IPv4 or FQDN format.	
POP3 Server Port Number	If you select **POP before SMTP** as the **Authentication Method**, enter a number between 1 and 65535.	

Related Information

➡ "Configuring a Mail Server" on page 45

Checking a Mail Server Connection

1. Access Web Config and select **Network Settings** > **Email Server** > **Connection Test**.
2. Select **Start**.

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

Related Information

➡ "Accessing Web Config" on page 10

➡ "Mail Server Connection Test References" on page 47

Mail Server Connection Test References

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

Appendix

Messages	Explanation
POP3 server communication error. Check the following. - Network Settings	This message appears when ❏ The scanner is not connected to a network ❏ POP3 server is down ❏ Network connection is disconnected while communicating ❏ Received incomplete data
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	This message appears when ❏ Connecting to a DNS server failed ❏ Name resolution for an SMTP server failed
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	This message appears when ❏ Connecting to a DNS server failed ❏ Name resolution for an POP3 server failed
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	This message appears when SMTP server authentication failed.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	This message appears when POP3 server authentication failed.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	This message appears when you try to communicate with unsupported protocols.
Connection to SMTP server failed. Change Secure Connection to None.	This message appears when an SMTP mismatch occurs between a server and a client, or when the server does not support SMTP secure connection (SSL connection).
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	This message appears when an SMTP mismatch occurs between a server and a client, or when the server requests to use an SSL/TLS connection for an SMTP secure connection.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	This message appears when an SMTP mismatch occurs between a server and a client, or when the server requests to use an STARTTLS connection for an SMTP secure connection.
The connection is untrusted. Check the following. - Date and Time	This message appears when the scanner's date and time setting is incorrect or the certificate has expired.
The connection is untrusted. Check the following. - CA Certificate	This message appears when the scanner does not have a root certificate corresponding to the server or a CA Certificate has not been imported.
The connection is not secured.	This message appears when the obtained certificate is damaged.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	This message appears when an authentication method mismatch occurs between a server and a client. The server supports SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	This message appears when an authentication method mismatch occurs between a server and a client. The server does not support SMTP AUTH.

Messages	Explanation
Sender's Email Address is incorrect. Change to the email address for your email service.	This message appears when the specified sender's Email address is wrong.
Cannot access the product until processing is complete.	This message appears when the scanner is busy.

Related Information

➡ "Checking a Mail Server Connection" on page 47

Receiving Email Notifications When Events Occur

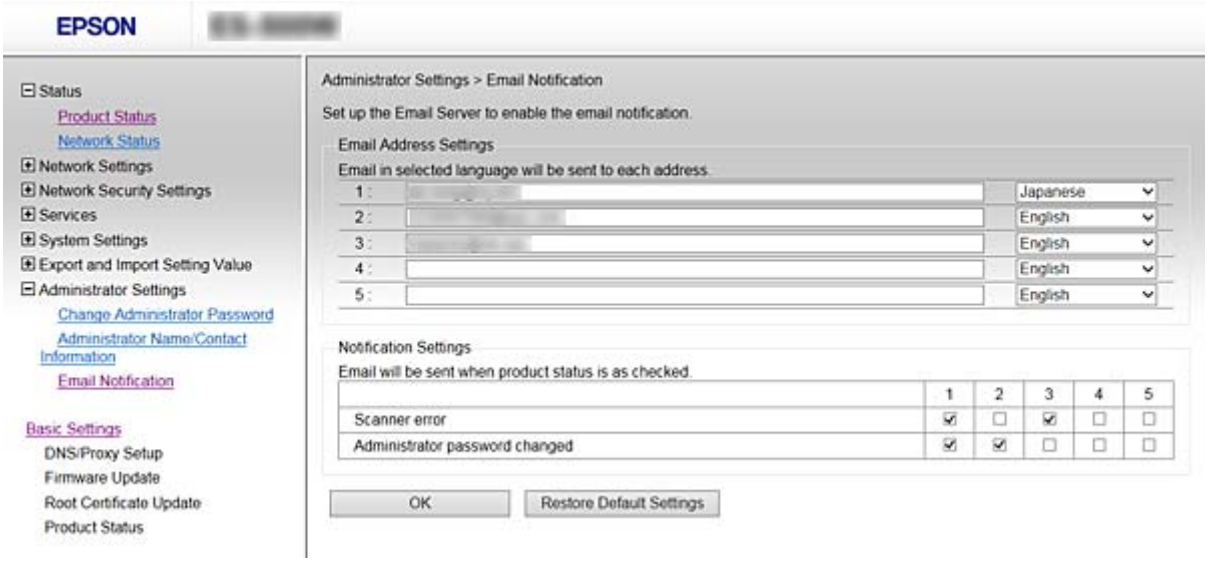
About Email Notifications

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

Configuring Email Notification

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

1. Access Web Config and select **Administrator Settings** > **Email Notification**.
2. Enter an email address that you want to receive email notifications.
3. Select the language for the email notifications.
4. Check the boxes for the notifications you want to receive.



5. Click **OK**.

Related Information

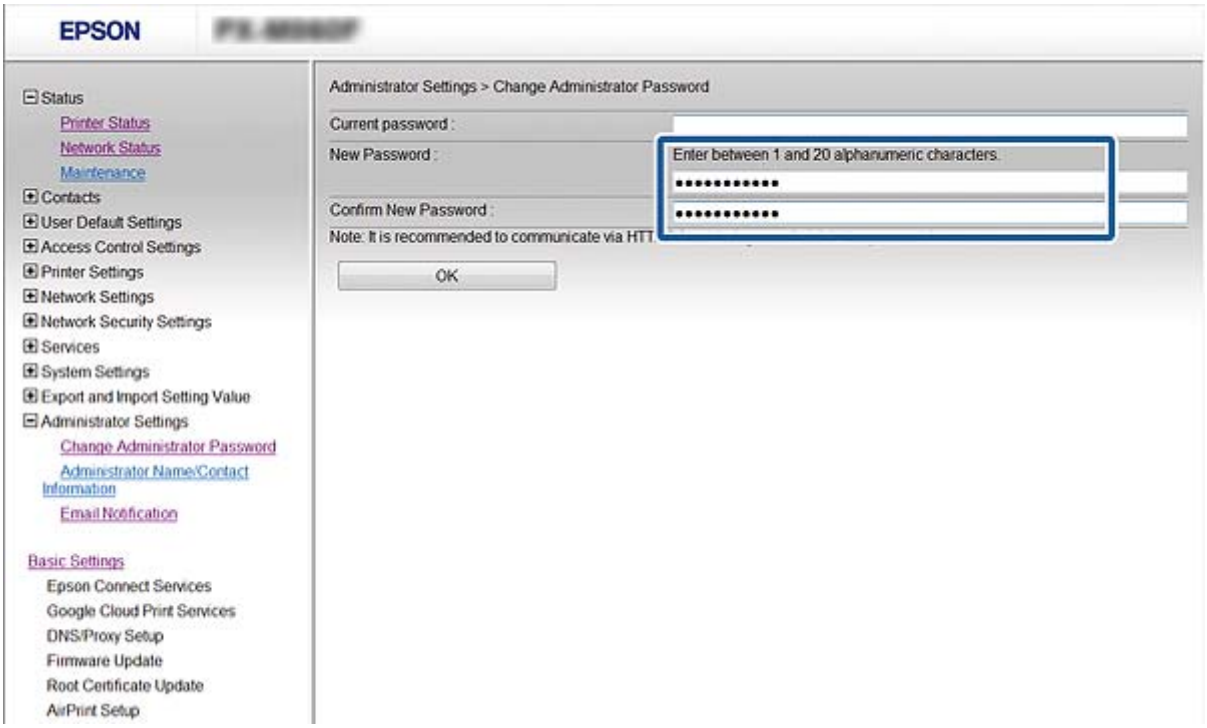
➡ “Accessing Web Config” on page 10
➡ “Using an Email Server” on page 45

Configuring the Administrator Password

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

1. Access Web Config and select **Administrator Settings** > **Change Administrator Password**.
2. Enter a password to **New Password** and **Confirm New Password**.

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



3. Select **OK**.

   Note:
   The administrator password is the same for Web Config and EpsonNet Config.

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

Related Information

➡ “Accessing Web Config” on page 10

Configuring Protocols

You can enable or disable protocols that can be controlled.

Note:
If you want to use the SNMPv3 protocol, see [Using SNMPv3 Protocol].

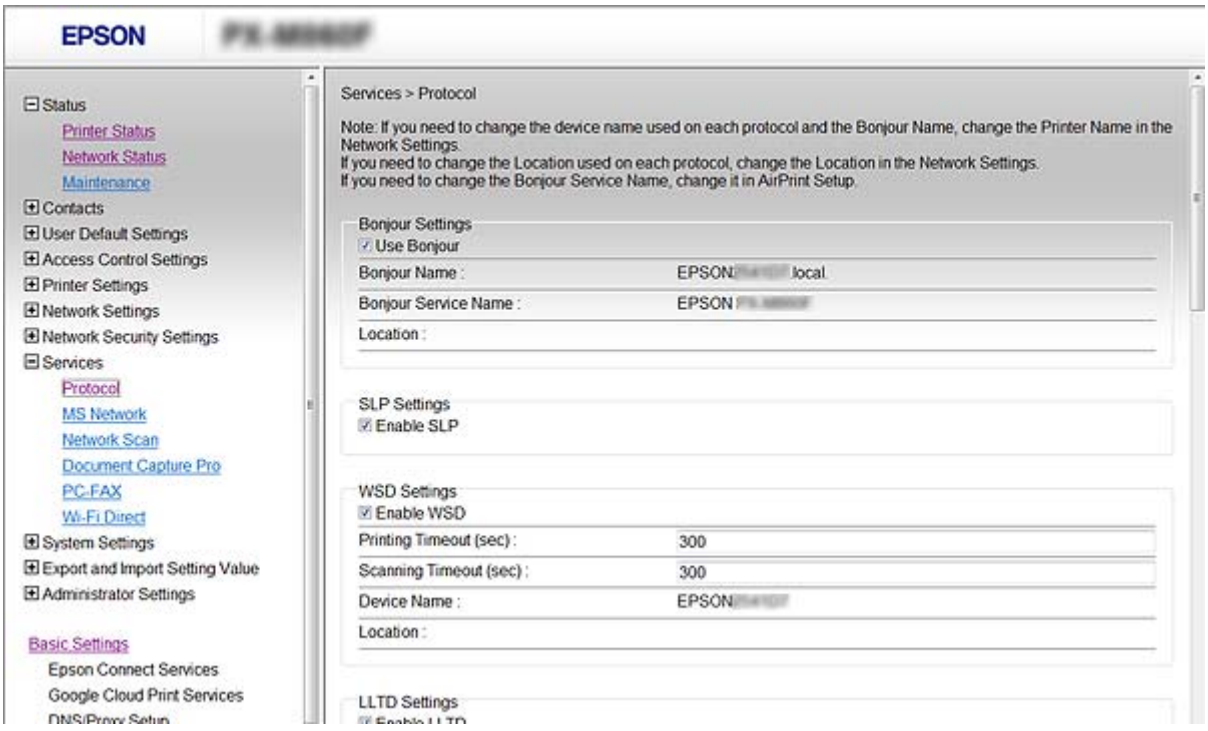
1. Access Web Config, and then select **Services** > **Protocol**.
2. Configure each item.
3. Click **Next**.
4. Click **OK**.

   The settings are applied to the scanner.

Related Information

➡ "Using SNMPv3 Protocol" on page 25

Protocol Setting Items



Items	Setting value and Description
Bonjour Settings	
Use Bonjour	Select this to search for or use devices through Bonjour.
Bonjour Name	Displays the Bonjour name.

Items	Setting value and Description
Bonjour Service Name	Displays the Bonjour service name.
Location	Displays the Bonjour location name.
SLP Settings	
Enable SLP	Select this to enable the SLP function. This is used with the Push Scan function and network searching in EpsonNet Config.
WSD Settings	
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	
Enable LLTD	Select this to enable LLTD. The scanner is displayed in the Windows network map.
Device Name	Displays the LLTD device name.
LLMNR Settings	
Enable LLMNR	Select this to enable LLMNR. You can use name resolution without NetBIOS even if you cannot use DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Select to enable SNMPv1/v2c. Only scanners that support SNMPv3 are displayed.
Access Authority	Set the access authority when SNMPv1/v2c is enabled. Select **Read Only** or **Read/Write**.
Community Name (Read Only)	Enter 0 to 32 ASCII (0x20 to 0x7E) characters.
Community Name (Read/Write)	Enter 0 to 32 ASCII (0x20 to 0x7E) characters.

Exporting and Importing the Web Config Settings

You can export the Web Config settings and copy them to another scanner.

Export the settings

Export each setting for the scanner.

1. Access Web Config, and then select **Export and Import Setting Value** > **Export**.

2. Select the settings that you want to export.

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

3. Enter a password to encrypt the exported file.

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

4. Click **Export**.

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

Import the settings

Import the exported Web Config file to the scanner.

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

1. Access Web Config, and then select **Export and Import Setting Value** > **Import**.
2. Select the exported file, and then enter the encrypted password.
3. Click **Next**.
4. Select the settings that you want to import, and then click **Next**.
5. Click **OK**.

The settings are applied to the scanner.

Configuring a Computer Connected to the Scanner

Connecting a Scanner to the Network

You need to install the scanner driver on your computer to use scanners on a network.

1. Install the scanner driver.

   Download the software from the following website, and then install.

   http://epson.sn > **Additional Software**

2. Start Epson Scan 2 Utility.

   ❏ Windows 10/Windows Server 2016

   Click the start button, and then select **EPSON** > **Epson Scan 2 Utility**.

   ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

   Enter the application name in the search charm, and then select the displayed icon.

   ❏ Windows 7/Windows Vista/Windows XP/Windows Server 2008 R2/Windows Server 2008/Windows Server 2003 R2/Windows Server 2003

   Click the start button, and select **All Programs** or **Programs** > **EPSON** > **Epson Scan 2** > **Epson Scan 2 Utility**.

   ❏ Mac OS

   Click **Go** > **Application** > **Epson Software** > **Epson Scan 2 Utility**.

   The Scanner Settings screen is displayed when you start Epson Scan 2 Utility for the first time. If the Epson Scan 2 Utility screen is displayed, select **Settings** from **Scanner**.

3. If **Add** and **Delete** are disabled, click **Enable Editing**, and then allow changes on the User Account Control window.

   Note:
   Status and operations vary depending on the operation system and authority for the logged on user. For Mac OS, you can edit if you click the key icon and enter the user name and password for an administrator.

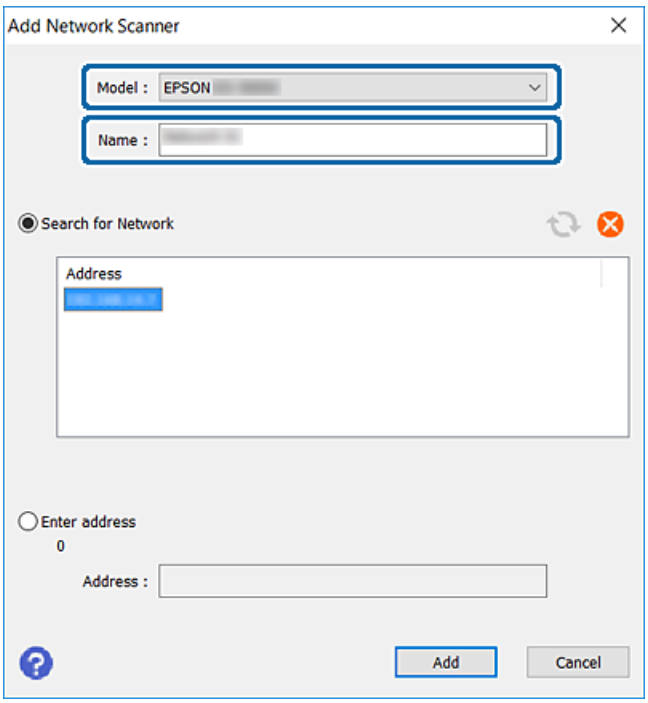
4. Click **Add**.

   The Add Network Scanner screen is displayed.

   Note:
   For Mac OS, click +.

5. Select the scanner you want to use from **Model**.

6. Enter the scanner's registration name in **Name**.



7. Click the scanner's IP address, and then click **Add**.

> ***Important:***
>
> *You cannot search for a scanner in a different network segment over the router. Select **Enter address** to enter the IP address directly.*

8. Click **OK** on the Scanner Settings screen.