Canon

imagePROGRAF
series

NETWORK SECURITY GUIDE

1st Edition

Introduction

This guide describes network security for Canon (imagePROGRAF series) Large Format Printers. Refer to items as required for your particular application.

Effective and continued measures are a necessity for alleviating the different risks that exist when using a printer, such as leakage of personal information and unauthorized external access. To ensure the printer can be used as securely as possible, an administrator should make settings that are important to printer use, including access privileges and security.

This guide serves as a common guide for all Canon Large Format Printers in the imagePROGRAF series. The models covered are given below. Operation descriptions use imagePROGRAF TX-4100 as an example. A portion of the descriptions may not be applicable to your product depending on your product's specifications. Please note that descriptions are subject to change without notice.

Covered models:

imagePROGRAF TX-4100 / TX-3100 / TX-2100
imagePROGRAF TX-5410 / TX-5310 / TX-5210
imagePROGRAF TZ-30000
imagePROGRAF TZ-5300
imagePROGRAF PRO-6100 / PRO-4100 / PRO-2100 / PRO-6100S / PRO-4100S
imagePROGRAF PRO-561 / PRO-541 / PRO-521 / PRO-561S / PRO-541S
imagePROGRAF TA-30 / TA-20
imagePROGRAF TA-5300 / TA-5200
imagePROGRAF TM-305 / TM-300 / TM-205 / TM-200
imagePROGRAF TM-5305 / TM-5300 / TM-5205 / TM-5200
imagePROGRAF TX-4000 / TX-3000 / TX-2000
imagePROGRAF TX-5400 / TX-5300 / TX-5200
imagePROGRAF PRO-6000 / PRO-4000 / PRO-2000 / PRO-6000S / PRO-4000S
imagePROGRAF PRO-560 / PRO-540 / PRO-520 / PRO-560S / PRO-540S

Also see the online manual for each model.
https://ij.start.canon

Notations in This Guide

Each chapter of this guide describes a function and its operation.

Symbols

The following symbols indicate descriptions of limitations or precautions to observe when handling the product.

Important

Important information to be observed to prevent product malfunction/damage or mistaken operation. Be sure to read.

Note

Reference information and supplementary descriptions.

Panel

Steps to be performed on the printer's operation panel.

Remote UI

Steps that can be performed with the "Remote UI", which allows printer settings to be made via a computer web browser.

Trademarks

Microsoft is a registered trademark of Microsoft Corporation.

Windows is a trademark or registered trademark of Microsoft Corporation in the U.S. and/or other countries.

Microsoft Edge is a trademark or registered trademark of Microsoft Corporation in the U.S. and/or other countries.

Mac, Mac OS, macOS, OS X, AirPort, App Store, AirPrint, the AirPrint logo, Safari, Bonjour, iPad, iPad Air, iPad mini, iPadOS, iPhone and iPod touch are trademarks of Apple Inc., registered in the U.S. and other countries.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.

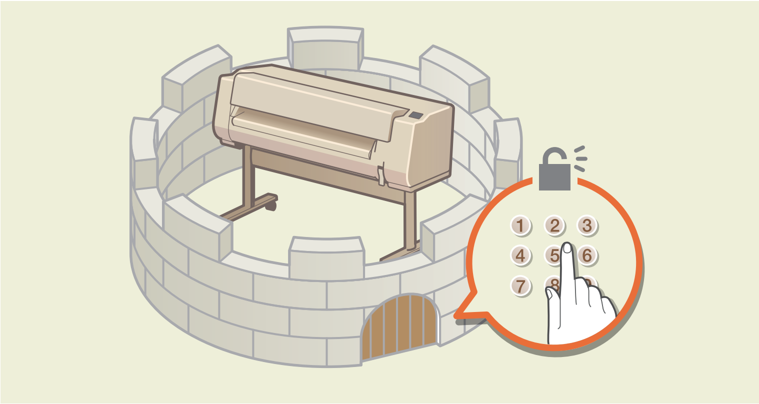
Contents

Overview

Sensitive information that is handled by information devices such as computers and printers is at times targeted by malicious third parties. However, in addition to unauthorized access and other such network attacks, carelessness or misoperation of the printer also have the potential to be damaging. To avert this kind of risk, the printer is designed with an array of security functionality. Take preventative measures as required by your system.

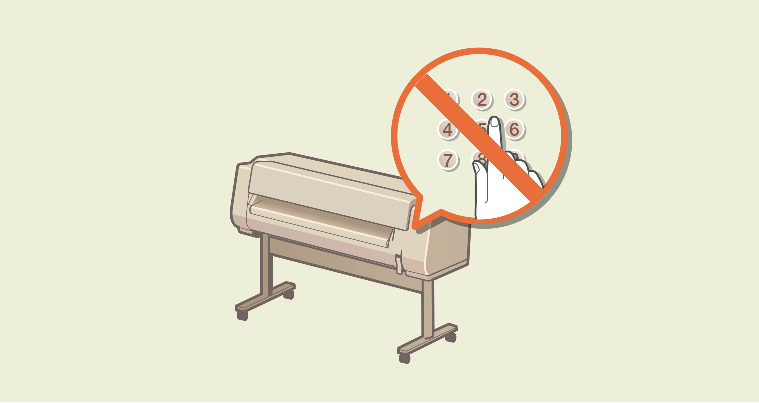
Administrator Password Settings

Allow only users with access privileges to change settings and prevent unauthorized use by third parties.



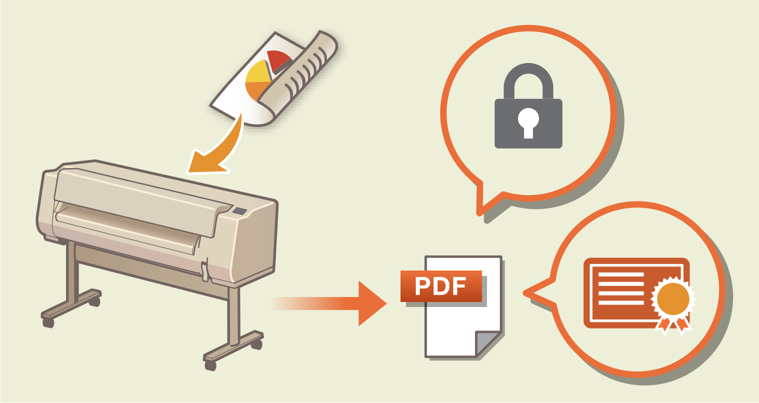
User Restrictions

Restrictions can be placed on operation in standard user mode.



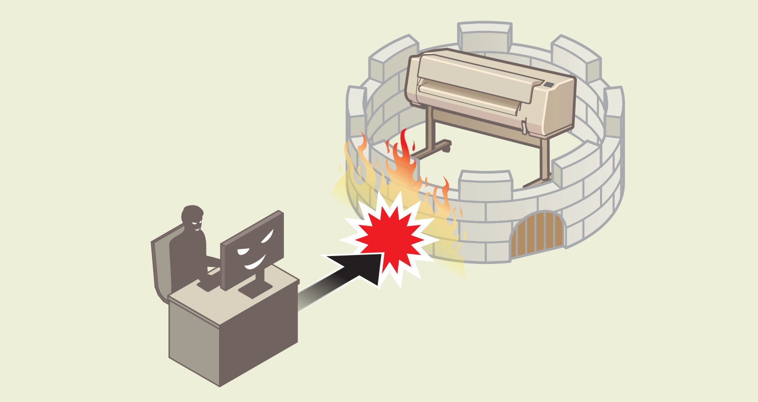
Protection for Hard Disk Data

Hard disk data can be managed as a way of ensuring data in the printer is protected.



Network Security

You can make security settings for the network and protect valuable data and information.



Firmware Updates

Keep firmware updated to the latest version to enjoy smooth and secure printer operation.

1 Before Using the Printer

How to use Remote UI and set an administrator password are described here, to allow you to make security settings for the network.

1.1 Remote UI

You can use Remote UI to check printer status and change settings over the network. Access the printer from your smartphone, tablet, or computer's web browser.

Remote UI can be used in either administrator mode or standard user mode. Administrator mode allows the user to change all printer settings and to place restrictions on operations in standard user mode. Standard user mode allows the user to change only certain settings.

Note

- Before using Remote UI, connect the printer to your network.
- See the online manual for your printer model for usable OSs and web browsers.

Starting Remote UI

Panel

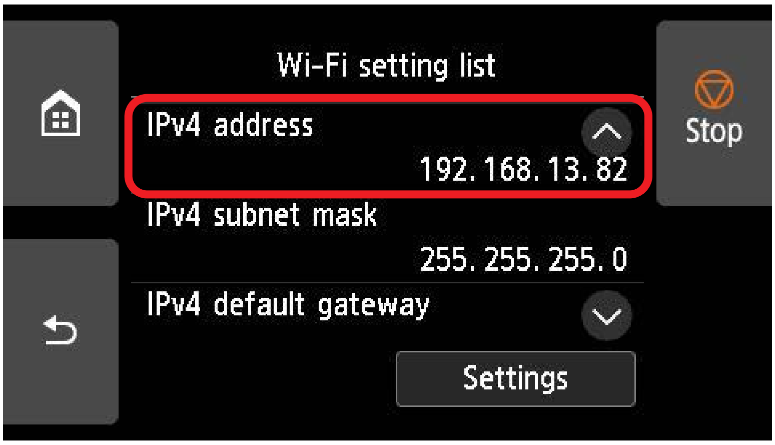
1. Check the IP address of the printer

(1) In the home screen, select [LAN settings]

(2) Select an enabled LAN

A disabled LAN is crossed out.

(3) Check [IPv4 address] on the displayed screen



Wi-Fi setting list

IPv4 address
192.168.13.82

IPv4 subnet mask
255.255.255.0

IPv4 default gateway

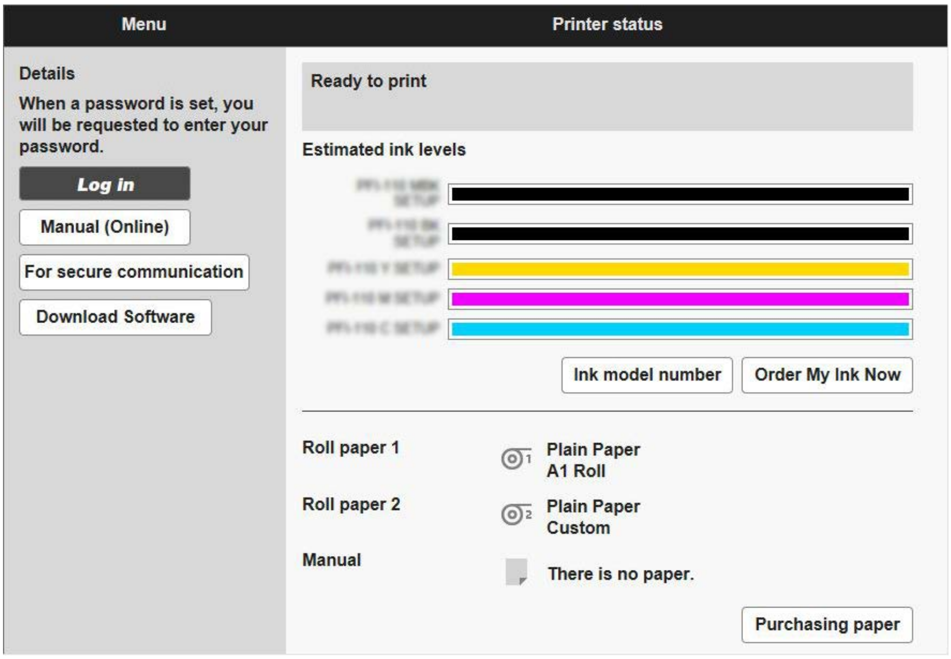
Remote UI

2. Open the web browser, and enter the IP address of the printer in the address bar

Enter the IP address in the following format.

http://XXX.XXX.XXX.XXX

After gaining access, Remote UI starts, and a login screen is displayed in the web browser.



Menu

Details

When a password is set, you will be requested to enter your password.

Printer status

Ready to print

Estimated ink levels

[illegible]
[illegible]
[illegible]
[illegible]
[illegible]

Roll paper 1	Plain Paper A1 Roll
Roll paper 2	Plain Paper Custom
Manual	There is no paper.

Note

- ► The first time you display Remote UI, download the root certificate and install it to your browser.

  ➡ Installing a Printer Root Certificate on the Web Browser for SSL Communication

- ► If the root certificate is not installed, an alert indicating that secure communication is not possible may be displayed.

3. Select [Log in]

A password authentication screen is displayed.

Important

- ► If standard user mode is enabled, select whether to log on in administrator mode or in standard user mode. However, to change network and security settings you must log on in administrator mode.

  ➡ 1.2 Changing/Setting Passwords

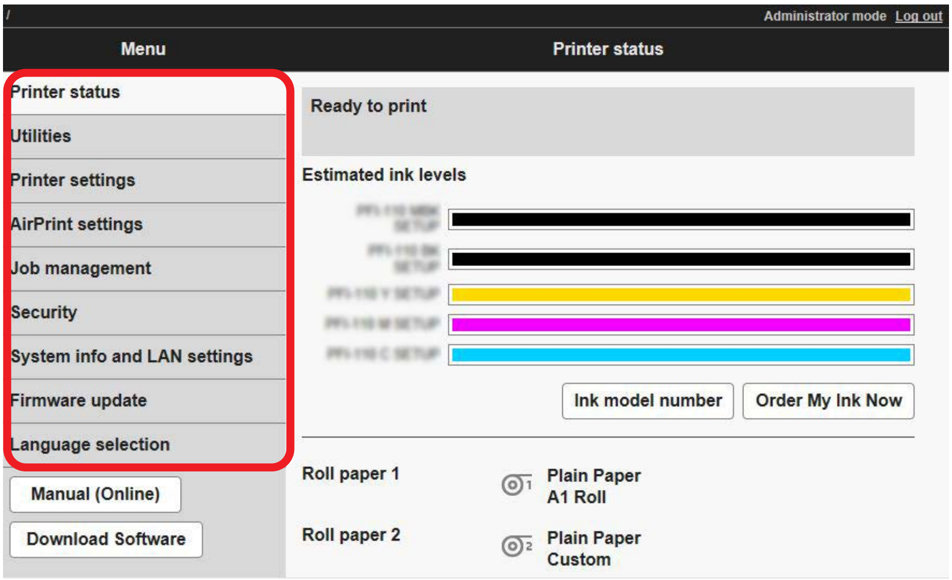
- ► The default administrator password is set to the printer's serial number.

  ➡ 4.2 Checking the Printer's Serial Number

4. Enter the password, and click [OK]

Remote UI top screen is displayed.

Items that Can Be Set from Remote UI



Ready to print

Estimated ink levels

Roll paper 1 Plain Paper A1 Roll

Roll paper 2 Plain Paper Custom

[Printer status]

Ink remaining, printer status, error details, etc. are displayed.

You can also access the support page and use the provided services.

[Utilities]

Perform printer maintenance such as cleaning.

[Printer settings]

Change printer settings such as power saving settings and print settings.

You can also change mail settings and set the printer to alert you when ink runs low, or an error occurs..

You can also restrict operation at the operation panel with [Operation panel lock] in [Custom settings].

[AirPrint settings]

Make print settings for using AirPrint in macOS or iOS operating systems.

[Job management]

View or print out the job history, as well as delete jobs.

[Security] (administrator mode)

Set a password, place operational restrictions on standard users, set up encrypted communication (SSL/TLS settings), etc.

[System info and LAN settings]

Check system information and make LAN settings.

[Firmware update] (administrator mode)

Check the firmware version and perform updates, and make settings for DNS and proxy servers.

[Language selection] (administrator mode)

Change the display language.

[Manual (Online)]

Display the online manual.

The computer on which Remote UI is open must be connected to the internet.

1.2 Changing/Setting Passwords

You can use Remote UI to check printer status and change settings over the network. Passwords can be set for both administrator mode and standard user mode.

Logging on in administrator mode allows you to change all printer settings and to place restrictions on operations in standard user mode. Logging in to standard user mode allows you to change only certain settings.

After setting an administrator password, entering the password is required for some operation panel options to use them each time. An administrator password can be set either using the operation panel on the printer or using Remote UI.

Important

- ► The password must be this length.
  Set a password between 4 and 32 characters long.
  Only letters, numbers, spaces, umlaut characters, and the symbols below can be used.
  - ! @ # $ % ^ & * _ ; : , . / ` = + ' " ( ) { } [ ] < > |
- ► To be as secure as possible, it is recommended that the password uses a combination of letters, numbers and symbols and be 8 characters or more.

Changing/Setting the Administrator Password with Remote UI

Note

- ► The administrator password can only be changed while logged on in administrator mode.

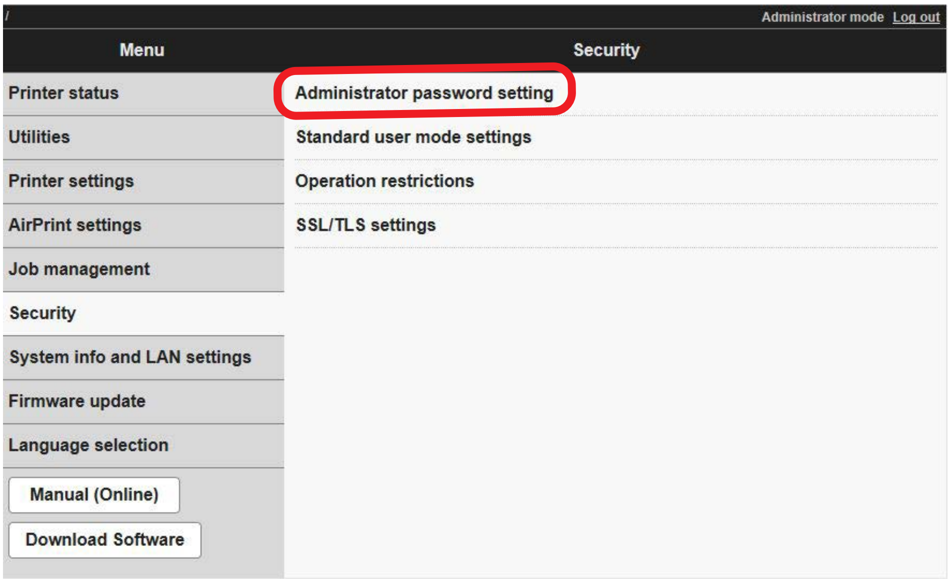
Remote UI

1. Start Remote UI

➡ Starting Remote UI

2. Select [Security]

3. Select [Administrator password setting]



4. Select [Change administrator password]

5. Select the range of coverage for the administrator password, and select [OK]

[Remote UI and other tools]

The administrator password is required when changing settings using Remote UI or some software.

[Operation panel/Remote UI/other tools]

The administrator password is required when changing settings using the printer's operation panel, Remote UI, or other software.

6. Follow the onscreen instructions, enter the password and select [OK]

7. When the completion message is displayed, select [OK]

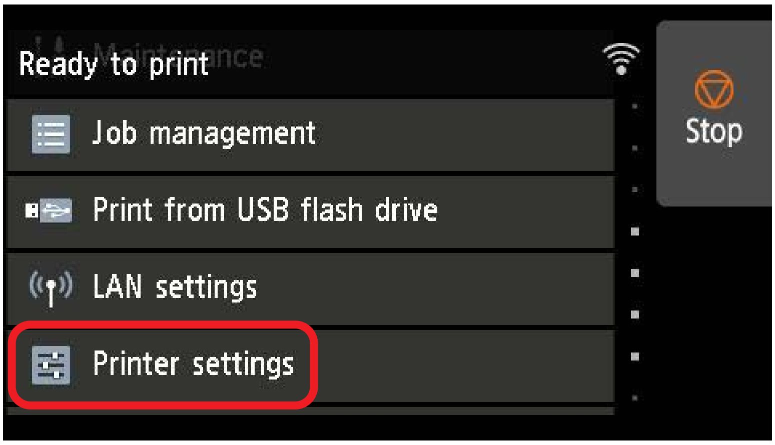
Note

► After setting the administrator password, enter administrator information. This is displayed in Remote UI top screen. Administrator information can be entered in [Printer settings] ▶ [Custom settings] ▶ [Administrator information].

Changing/Setting the Administrator Password with the Operation Panel

Panel

1. **In the home screen, select [Printer settings]**



2. **Select [Security settings]**

3. **Select [Administrator password settings]**

4. **Enter the administrator password in the entry screen, and select [OK]**

   If the administrator password is not set, a registration confirmation message is displayed.

   Select [Yes].

   A message is displayed again. Select [OK].

5. **Select [Change administrator password]**

6. **Select the range for the administrator password**

   [Remote UI and other tools]

   The administrator password is required when changing settings using Remote UI or some software.

   [LCD, Remote UI, and other tools]

   The administrator password is required when changing settings using the printer's operation panel, Remote UI, or some software.

7. **Enter the administrator password**

8. **Select [Apply]**

9. **Enter the administrator password again**

10. **Select [Apply]**

    The administrator password is enabled.

Setting the Standard User Password

To restrict functions available to standard users, use the steps below to enable standard user mode settings, and set the standard user password.

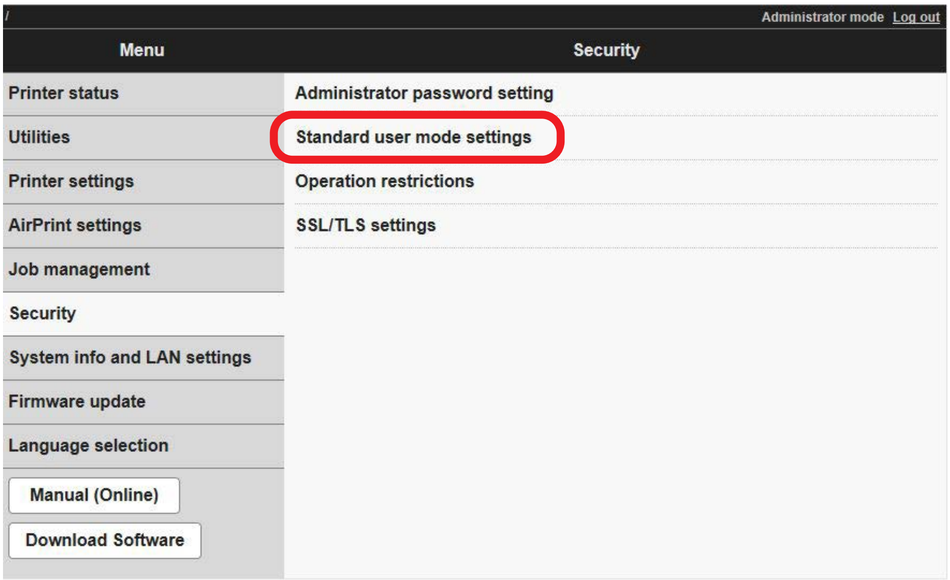
Remote UI

1. Start Remote UI

➡ Starting Remote UI

2. Select [Security]

3. Select [Standard user mode settings]



4. After a confirmation message is displayed, select [Yes]

5. Follow the onscreen instructions, enter the password and select [OK]

6. When the completion message is displayed, select [OK]

1.3 Registering a Root Certificate

If a root certificate is not installed on the web browser, an alert indicating that secure communication is not possible may be displayed. The first time you open Remote UI, download the root certificate and install it on the web browser. Secure communication will be confirmed, and the alert will no longer be displayed. However, an alert will continue to be displayed in some browsers even after installing a root certificate.

Installing a Printer Root Certificate on the Web Browser for SSL Communication

How to install a root certificate depends on the web browser type and version. Microsoft Edge is described in this guide as an example.

Important

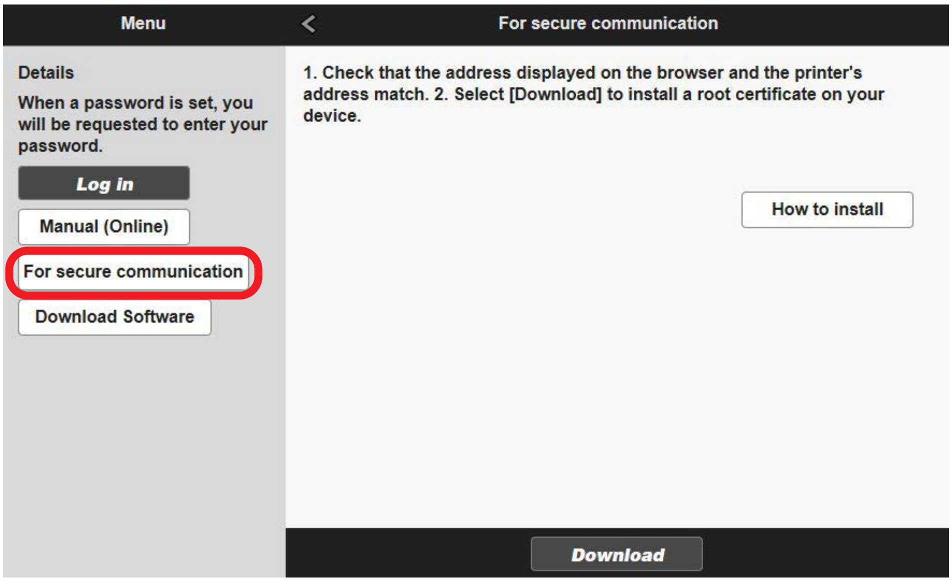
- When installing a root certificate, check the web browser's URL box to ensure that the printer's IP address is correct.

Remote UI

1. Start Remote UI

➡ Starting Remote UI

2. Select [For secure communication]



When a password is set, you will be requested to enter your password.

1. Check that the address displayed on the browser and the printer's address match. 2. Select [Download] to install a root certificate on your device.

3. Select [Download]

The root certificate begins downloading.

4. After a download confirmation screen is displayed, select [Open]

A [Certificate] screen is displayed.

5. Select [Install Certificate]

A [Certificate Import Wizard] screen is displayed.

6. Select [Next]

7. Select [Place all certificates in the following store]

8. Select [Browse]

A [Select Certificate Store] screen is displayed.

9. Select [Trusted Root Certification Authorities], and select [OK]

10. In the [Certificate Import Wizard] screen, select [Next]

11. After [Completing the Certificate Import Wizard] is displayed, select [Finish]

A [Security Warning] screen is displayed.

12. Check that the fingerprint field in the [Security Warning] screen and the fingerprint on the printer's root certificate match.

For the fingerprint on the printer's root certificate, in the home screen on the operation panel, select [Printer information]→[System information], and check [Root cert. thumbprint (SHA-1)] or [Root cert. thumbprint (SHA-256)].

13. If the fingerprint field and the fingerprint on the printer's root certificate match, select [Yes] in the [Security Warning] screen

14. In the [Certificate Import Wizard] screen, select [OK]

The root certificate is installed.

2 Protection for Hard Disk Data

Appropriately protecting data, such as by setting passwords to personal boxes, is recommended so as to prevent data saved on the printer's hard disk (print jobs and settings information) from inadvertently becoming accessible. Also be sure to erase data and take any other steps necessary to prevent unauthorized access when not using the printer for an extended period or when disposing of the printer.

2.1 Setting a Password to a Personal Box

After setting a password, entering the password is required each time you access the following.

- Changing the settings of a personal box
- Displaying or printing a job list saved in a personal box
- Printing, deleting, moving, or changing the name of a saved job

Note

- ► Personal boxes do not have a default password set.
- ► A password cannot be set to a common box.
- ► Set a password of 7 digits from 0000001 to 9999999.
- ► Even when a password is set, entering the password is not required if you log on in administrator mode in Remote UI.

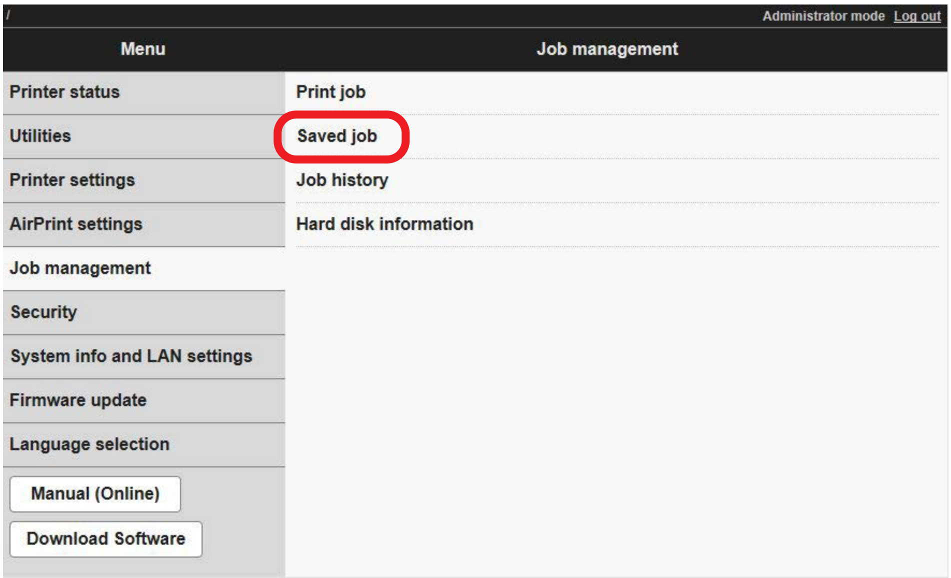
Remote UI

1. Start Remote UI

➡ Starting Remote UI

2. Select [Job management]

3. Select [Saved job]



4. In the list, select the box

5. Select [Edit]

6. Select the [Set/change password] check box, and enter the password (7 digit number between 0000001 and 9999999)

7. Select [OK]

2.2 Completely Erasing Hard Disk Data

Any data remaining in the printer has the risk of being accessed by third parties. Before disposing of the printer, be sure to erase any data.

Also, if having the printer repaired, lending it for use, or transferring possession of the printer, be sure to initialize the printer settings.

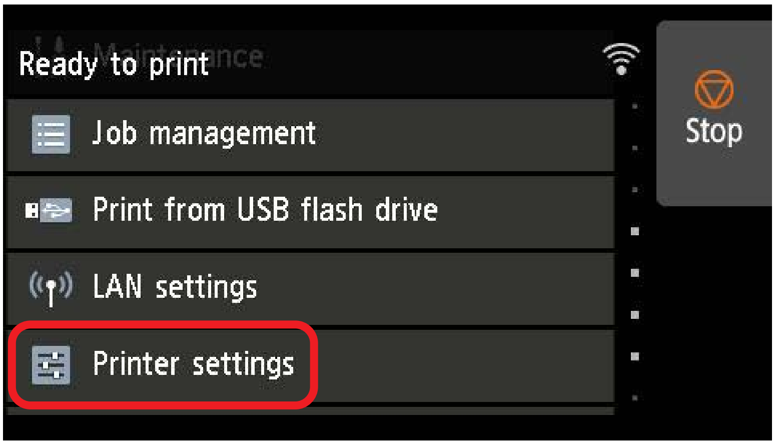
➡ 2.4 Initializing Settings Information

Important

- ► If an administrator password is set for making settings changes at the operation panel, the administrator password is required when erasing data.
- ► To completely prevent data restoration, it is recommended to physically or magnetically destroy the hard disk. Once destroyed, a hard disk cannot be used again.
- ► Data cannot be erased where a job queue exists. Also, print jobs are not processed while data is being erased.

Panel

1. In the home screen, select [Printer settings]



Ready to print

Job management

Print from USB flash drive

LAN settings

Printer settings

Stop

2. Select [Hard disk settings]

If the administrator password is set, enter the administrator password.

3. Select [Data deletion]

4. Select an erasing method

[Fast]

File management information for data on the hard disk is erased. Select this to erase data in a short time. Since only file management data is erased, the data itself is not erased.

[Fast secure]

The data encryption key set to the hard disk is erased. Resetting an encryption key prevents previously saved data from being accessed and used.

Select this to securely erase sensitive data in a short time.

[Secure]

The data encryption key set to the hard disk is first erased, and then the entire hard disk is overwritten with 00/FF/random data once each.

A verify check is performed to check that data has been written to the hard disk correctly.

Select this to erase particularly sensitive data.

Restoring overwritten data is almost impossible.

Conforms to US Department of Defense standards (DoD5220.22-M).

[Secure (VSITR)]

The data encryption key set to the hard disk is first erased, and then the entire hard disk is overwritten with 00 once, and then with FF.

This is repeated three times, after which the entire hard disk is overwritten with AA.

Restoring overwritten data is almost impossible.

Conforms to German federal guidelines (VS-ITR).

5. Check the message on the operation panel, and select [Yes]

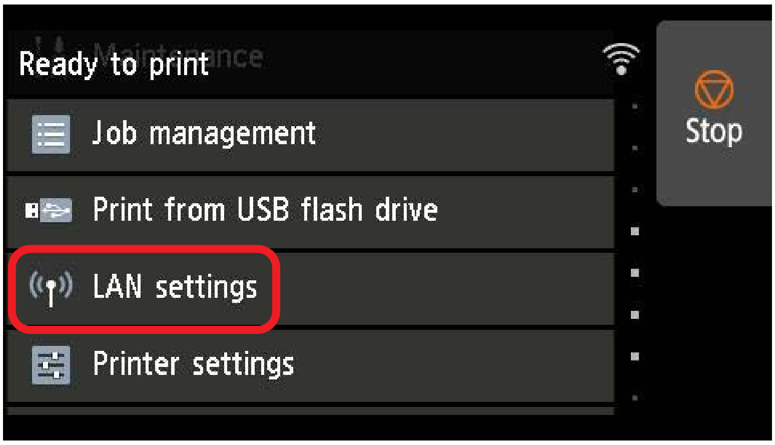
Data on the hard disk is erased.

2.3 Initializing Network Settings

When reconfiguring network settings, first initialize the network settings from the printer's operation panel.

Panel

1. **In the home screen, select [LAN settings]**



If the administrator password is set, enter the administrator password.

2. **Select [Wi-Fi], [Wireless Direct], or [Wired LAN]**

3. **Select [Settings]**

4. **Select [Advanced]**

5. **Select [Reset LAN settings]**

6. **Select [Yes]**

2.4 Initializing Settings Information

Any personal information that has been registered to the printer is stored in the printer. To prevent leakage of information, initialize the printer's settings when it is being entrusted to others (when having it repaired, lending it, etc.) as well as when transferring its possession or disposing of it.

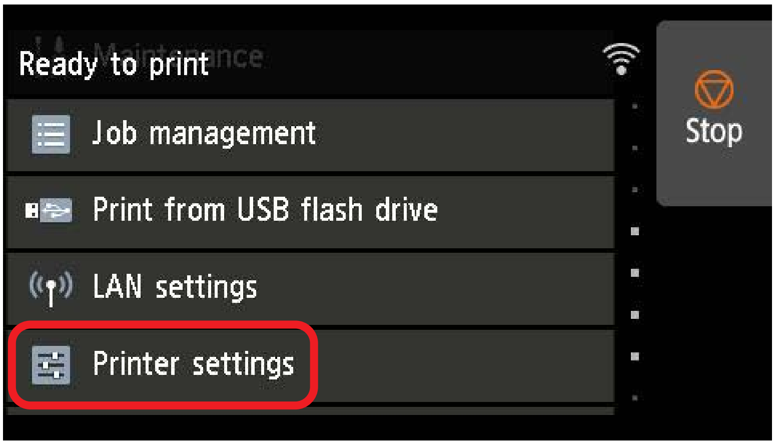
The following printer settings are initialized in this process.

- Paper settings information
- Paper prediction data
- SSL certificate
- LAN settings
- Administrator password
- Hard disk data
- Job history
- Panel access lock settings

Initializing from the Operation Panel

Panel

1. In the home screen, select [Printer settings]



2. Select [Initialize printer settings]

If the administrator password is set, enter the administrator password.

3. Check the message on the operation panel, and select [Yes]

Initialization starts.

Initializing from Remote UI

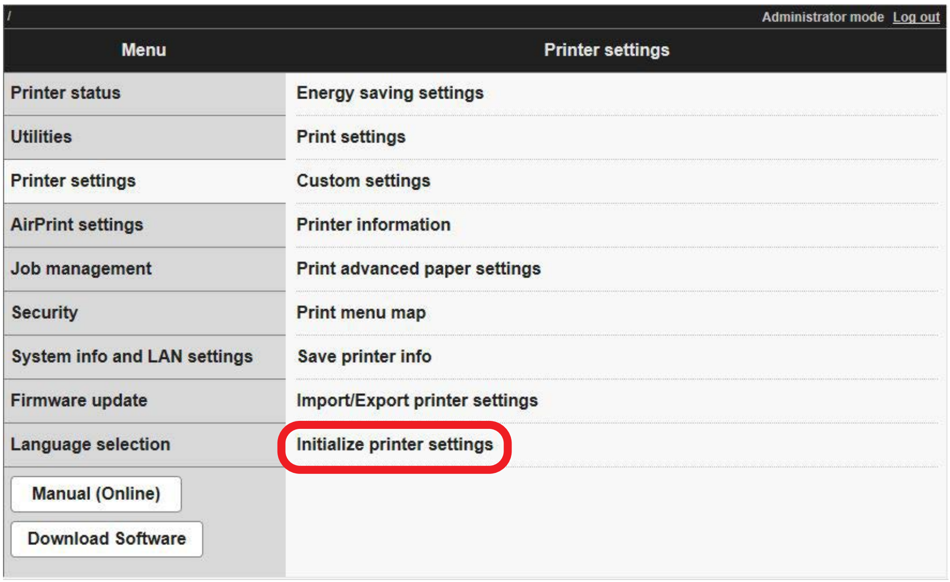
Remote UI

1. Start Remote UI

➡ Starting Remote UI

2. Select [Printer settings]

3. Select [Initialize printer settings]



4. Check the onscreen message, and select [Yes]

Initialization starts, and Remote UI disconnects.

3 Network Security

Eavesdropped communication, manipulated data, and identity theft by malicious third parties can cause serious damage. Network security to protect valuable data and information is described here.

3.1 Port Number Allocation

Predetermined port numbers are allocated to each protocol used for communication with external devices. Be aware that a firewall blocking a port can affect printer operation.

◆ TCP

Protocol	Port	Initial value	Usage and what it affects
LPD	515	ON	Used for LPR printing. LPR printing not possible if set to OFF.
RAW	9100	ON	Used for RAW printing. RAW printing not possible if set to OFF.
CPCA	9007	ON	Used for communication with Canon's CPCA (Common Peripheral Controlling Architecture). Product advanced settings and browsing not possible if set to OFF.
HTTP	80	-	Used for printing and obtaining information between a computer and the printer. Be sure not to block this port.
HTTPS	443	-	Used for obtaining information between a computer and the printer. Be sure not to block this port.
IPP	631	ON	Used for IPP printing.
IPPS	631	ON	Used for IPP secure printing.
FTP	20	OFF	Used for data transfer in FTP printing. FTP printing not possible if set to OFF.
FTP	21	OFF	Used for control in FTP printing.

◆ UDP

Protocol	Port	Initial value	Usage and what it affects
SNMP	161	v1: ON v3: ON	Used for communication with Simple Network Management Protocol. Status responses to a Mac or Windows printer driver not possible if set to OFF. • Management with a management application or Media Configuration Tool not possible. • "Easy wireless connect" not usable.
CPCA	47545	ON	Used for communication with Canon's CPCA (Common Peripheral Controlling Architecture). Settings and browsing of the product's detailed information not possible if set to OFF.
WSD	3702	OFF	Used for WSD device discovery (WS-Discovery). Printing using WSD not possible if set to OFF.
mDNS	5353	ON	Used for Bonjour. Bonjour not usable if set to OFF.
LLMNR	5355	ON	Used for name resolution requests by LLMNR. Response to name resolution requests by LLMNR not possible if set to OFF.
IKEv1	500	OFF	Used for key exchanges by IKEv1. IPsec not usable if set to OFF.
DHCP Client	68	ON	If set to OFF, it is necessary to allocate an IP address with a protocol other than DHCP or to set an IP address manually.
DHCPv6 Client	546	ON	Used for allocating an IPv6 address automatically. If set to OFF, it is necessary to use an address obtained other than from DHCP.
SNTP Client	123	OFF	Used for setting the correct time on the printer automatically over the network. If set to OFF, it is necessary to correct the time on the printer manually.

3.2 Enabling/Disabling the Interface

Of available Wi-Fi, Wireless Direct, and Wired LAN connections, only one connection can be enabled. Differing types of network connection cannot be used at the same time.

Enabling/Disabling a Wi-Fi Connection

Panel

[LAN settings] ▶ [Wi-Fi] ▶ [Settings] ▶ [Enable/disable Wi-Fi]

Remote UI

[System info and LAN settings] ▶ [LAN settings] ▶ [Wi-Fi] ▶ [Yes] ▶ [Enable/disable Wi-Fi]

Enabling/Disabling a Wireless Direct Connection

Panel

[LAN settings] ▶ [Wireless Direct] ▶ [Settings] ▶ [Enable/disable Wireless Direct]

Remote UI

[System info and LAN settings] ▶ [LAN settings] ▶ [Wireless Direct] ▶ [Yes] ▶ [Enable/disable Wireless Direct]

Enabling/Disabling a Wired LAN Connection

Panel

[LAN settings] ▶ [Wired LAN] ▶ [Settings] ▶ [Enable/disable Wired LAN]

Remote UI

[System info and LAN settings] ▶ [LAN settings] ▶ [Wired LAN] ▶ [Yes] ▶ [Enable/disable wired LAN]

Using/Not Using a USB Connection

Panel

[Printer settings] ▶ [Other printer settings] ▶ [Use USB connection]

3.3 Enabling/Disabling Communication Protocols

You can enable and disable use of communication protocols such as WSD, Bonjour, LPR, RAW, IPP, FTP, and SNMP. Use the printer's operation panel or Remote UI to enable or disable protocols. See "Starting Remote UI" for how to access with Remote UI.

WSD / Bonjour / IPP

Panel

[LAN settings] ▶ Select [Wi-Fi], [Wireless Direct], or [Wired LAN] ▶ [Settings] ▶ [Advanced]

Remote UI

[System info and LAN settings] ▶ [LAN settings] ▶ [Advanced setup] ▶ [Yes]

LPR / LLMNR / RAW

Panel

[LAN settings] ▶ Select [Wi-Fi], [Wireless Direct], or [Wired LAN] ▶ [Settings] ▶ [Advanced]

Remote UI

[System info and LAN settings] ▶ [LAN settings] ▶ [Advanced setup] ▶ [Yes] ▶ [LPD print]

SNMP / FTP

Remote UI

[System info and LAN settings] ▶ [LAN settings] ▶ [Advanced setup] ▶ [Yes]

CPCA

Panel

[LAN settings] ▶ Select [Wi-Fi], [Wireless Direct], or [Wired LAN] ▶ [Settings] ▶ [Advanced] ▶ [Use Dedicated Port]

3.4 Filtering to Restrict Communication

Connecting communication devices, including your computer and Large Format Printer, to a network without appropriate security measures in place allows the risk of unintended and unauthorized access by a third party.

Such risk can be reduced on a Large Format Printer by setting packet filtering, which works to allow communication only with devices having specific IP addresses or MAC addresses. Set this filtering with Remote UI. See "Starting Remote UI" for how to access with Remote UI.

Important

► MAC address filtering is enabled only with a wired connection. Cannot be set with a wireless connection.

IP Filtering

Remote UI

[System info and LAN settings] ▶ [LAN settings] ▶ [Advanced setup] ▶ [Yes] ▶ [IP filtering]

MAC Filtering

Remote UI

[System info and LAN settings] ▶ [LAN settings] ▶ [Advanced setup] ▶ [Yes] ▶ [MAC address filtering settings]

3.5 Encrypting Communication: SSL/TLS

Set this encryption to increase the level of security for communication when the printer operates as a server (HTTP/IPP, etc.) A certificate and key pair is used in encrypted communication.

Example of server authentication:

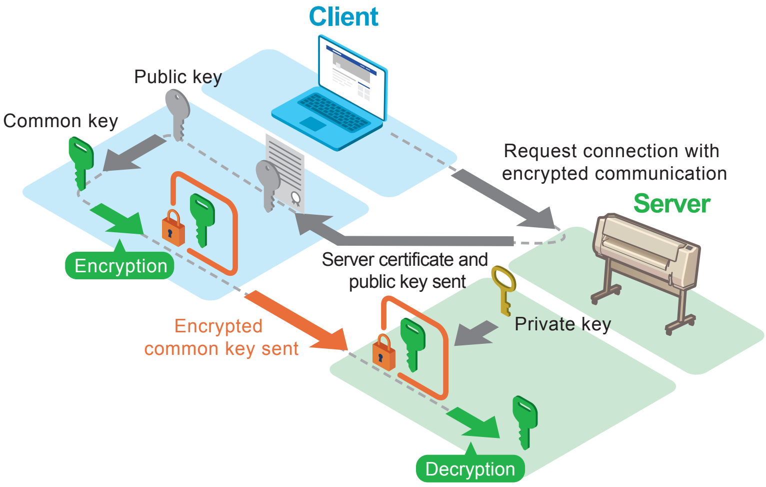
Server (printer) – client (computer) communication proceeds as follows.

(1) [Client] Request connection with encrypted communication

(2) [Server] Send server certificate and public key set

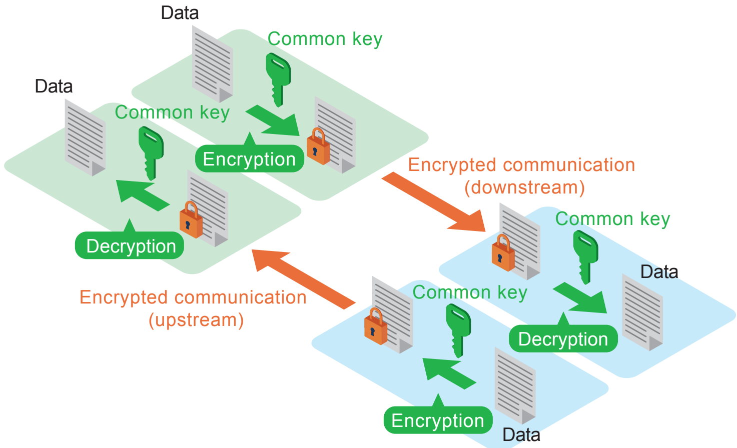
(3) [Client] Create common key

(4) [Client] Use received public key to encrypt common key and send to server (printer)


Client
Public key
Common key
Request connection with encrypted communication
Server
Encryption
Server certificate and public key sent
Private key
Encrypted common key sent
Decryption

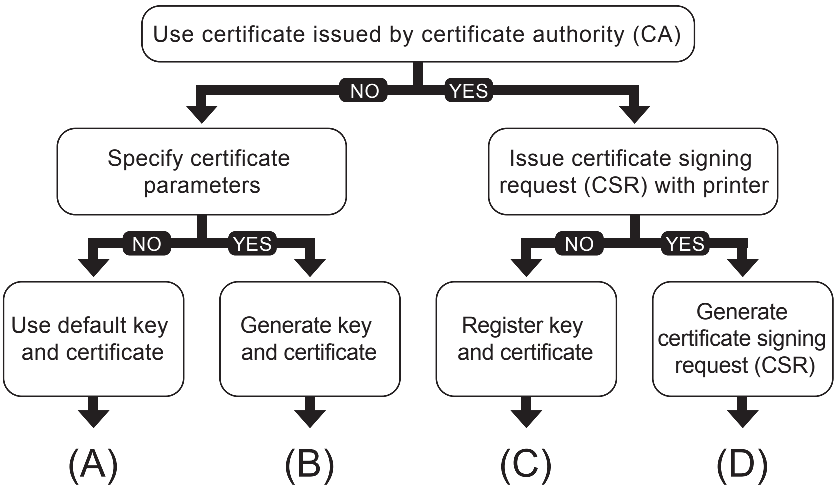
(5) [Server] Decrypt received common key with private key

(6) [Client/server] Use matching common key to encrypt/decrypt data route taken by sent and received data to establish encrypted communication



Canon Large Format Printers use a key and certificate (server certificate) stored in the printer, used for TLS encrypted communication, in carrying out Remote UI communication and IPP communication wherein the printer acts as an SSL/TLS server. In addition to the default certificate pre-installed in the printer, a certificate generated by the user with Remote UI or an externally created certificate can also be used as a server certificate.

Patterns that can be used for registering a digital certificate for SSL/TLS communication are as follows. Select a pattern for registering the certificate.


Use certificate issued by certificate authority (CA)
NO
YES
Specify certificate parameters
Issue certificate signing request (CSR) with printer
NO
YES
NO
YES
Use default key and certificate
Generate key and certificate
Register key and certificate
Generate certificate signing request (CSR)
(A)
(B)
(C)
(D)

(A) Use default key and certificate:

The default key and certificate already installed in the printer can be used.

In this case, it is not required to use Remote UI to register a key and certificate.

(B) Generate key and certificate:

To use a certificate having information you set yourself, such as a common name and validity period, you can use Remote UI to generate a new key and certificate.

Remote UI

[Security] ▶ [SSL/TLS settings] ▶ [Generate key and certificate] ▶ [Generate self-signed cert]

1. Set required items
   - Signature algorithm: select one of [SHA256], [SHA384], and [SHA512].
   - Public key bit length: Select [2048 bits].
   - Validity:

     Enter the date the server certificate is created in [Valid from].

     Enter the expiration date of the server certificate in [Valid to].
   - Common name: Enter letters and numbers.
2. Select [Next]
   - [Country], [State or province], [Locality], [Organization], and [Organizational unit] can be entered optionally.
   - Select [Generate]: The server certificate is then generated.
   - Select [Restart LAN].

The signed server certificate is created with the root certificate generated with the printer.

Depending on the web browser type and version, an alert indicating that secure communication is not possible may be displayed.

(C) Register key and certificate (use an externally created certificate):

You can use a key and certificate or CA certificate obtained from an issuing organization. Use Remote UI to upload the obtained key and certificate files.

Remote UI

[Security] ▶ [SSL/TLS settings] ▶ [Upload key and certificate]

1. Select the file format

   Select [PKCS#12] or [DER].
2. Select the files, and enter the password
3. Select the [Upload] button
4. If the administrator password is requested, enter the administrator password
5. Select the [Restart LAN] button

(D) Generate a certificate signing request (CSR):

Since a certificate generated with the printer is not signed by a certificate authority, a communication error may result depending on the connected device.

To obtain a certificate signed by a certificate authority, it is necessary to send a CSR (certificate signing request) file to a certificate authority and have a certificate issued.

Use Remote UI in administrator mode to generate the CSR. After the certificate is issued, upload the certificate with Remote UI.

Remote UI

[Security] ▶ [SSL/TLS settings] ▶ [Generate key and certificate] ▶ [Generate CSR (cert request)]

If [A generated CSR already exists. If you start generating, the existing CSR will be deleted. Continue to generate?] is displayed, select [Yes]

1. Set required items
   - Signature algorithm: select one of [SHA256], [SHA384], and [SHA512].
   - Public key bit length: Select [2048 bits].
   - Common name
2. Select [Next]
   - [Country], [State or province], [Locality], [Organization], and [Organizational unit] can be entered optionally.
   - Select [Generate]
   - Select [Download]
   - Specify where to save the CSR and save

Send the saved CSR file to a certificate authority, and have a certificate issued that is signed by the certificate authority (CA certificate).

Upload the CA certificate following the steps at (C).

Important

- ► To reset a generated server certificate, make the following setting in the home screen on the operation panel.

Panel

[LAN settings] ▶ [Wi-Fi], [Wireless Direct], or [Wired LAN] ▶ [Settings] ▶ [Advanced] ▶ [Reset SSL certificates]

Note

- ► If it is not possible to connect to Remote UI after restarting the LAN, reload the page in the web browser.

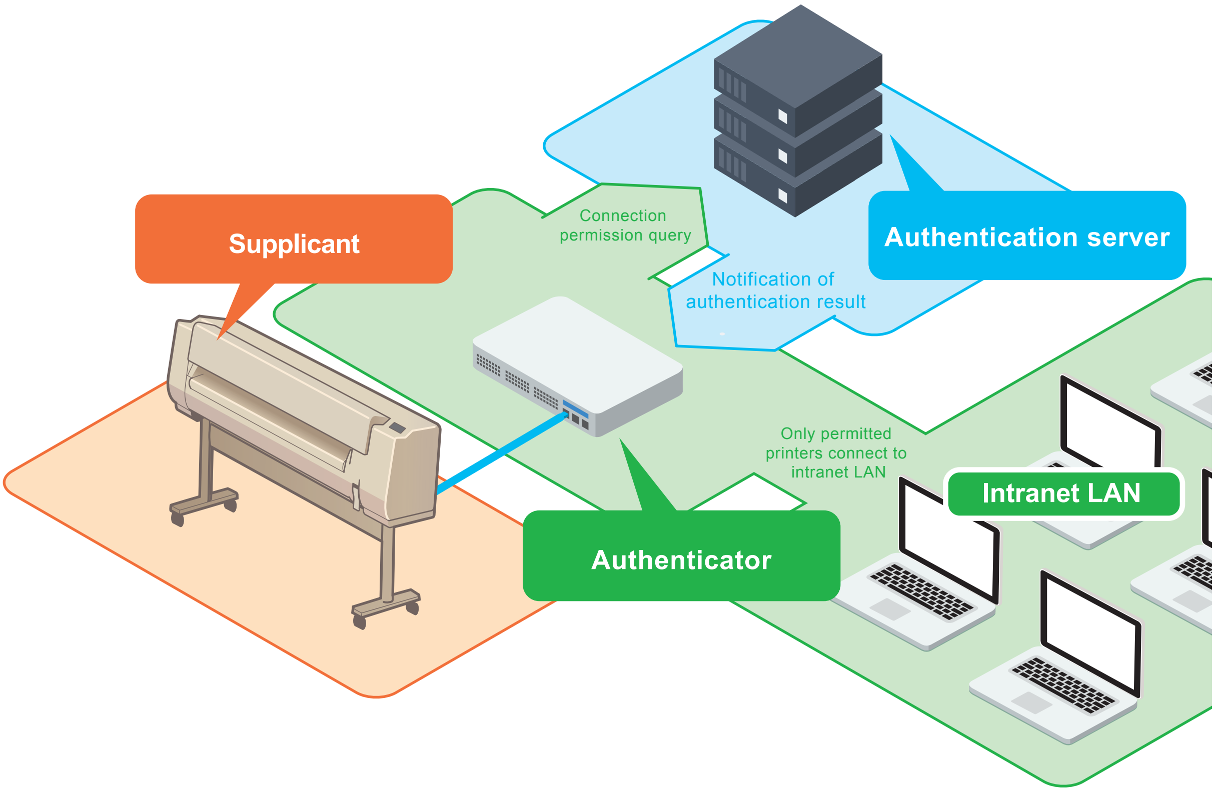
Specifications of keys and certificates that can be used for encrypted communication

➡ 4.3 Algorithms and Formats for Registerable Keys and Certificates

3.6 Settings for IEEE 802.1X Authentication

IEEE 802.1X is one of several LAN standards, and is an authentication standard that enables authentication of a client using a networked communication control device as an authenticator. Authentication requires the following 3 elements.

- Supplicant
- Authentication server
- Authenticator


Supplicant
Connection permission query
Authentication server
Notification of authentication result
Only permitted printers connect to intranet LAN
Intranet LAN
Authenticator

The supplicant installed in the device connecting to the network sends authentication information to the authentication server. The authentication server compares the received authentication information and determines whether to permit connection to the network. The authenticator then controls access of the connecting device to the network, based on the result determined by the authentication server. Connection to a network takes place with interaction between a supplicant, an authentication server, and an authenticator. The printer can connect to this sort of network as a supplicant.

IEEE 802.1X authentication methods

- EAP-TLS

  The printer and authentication server authenticate each other using their certificates. The printer uses a CA certificate for server authentication. The server requires key and client certificates issued by a certificate authority for printer (client) authentication. At time of shipment, a client certificate is not installed in the printer.
- EAP-TTLS

  Authentication method which uses a user name and password for printer authentication, and a CA certificate for server authentication. Select MSCHAPv2 or PAP as an internal protocol.
- PEAP

  Setting requirements are almost the same as those with TTLS, with MSCHAPv2 being used as the internal protocol.

Making IEEE 802.1X Settings

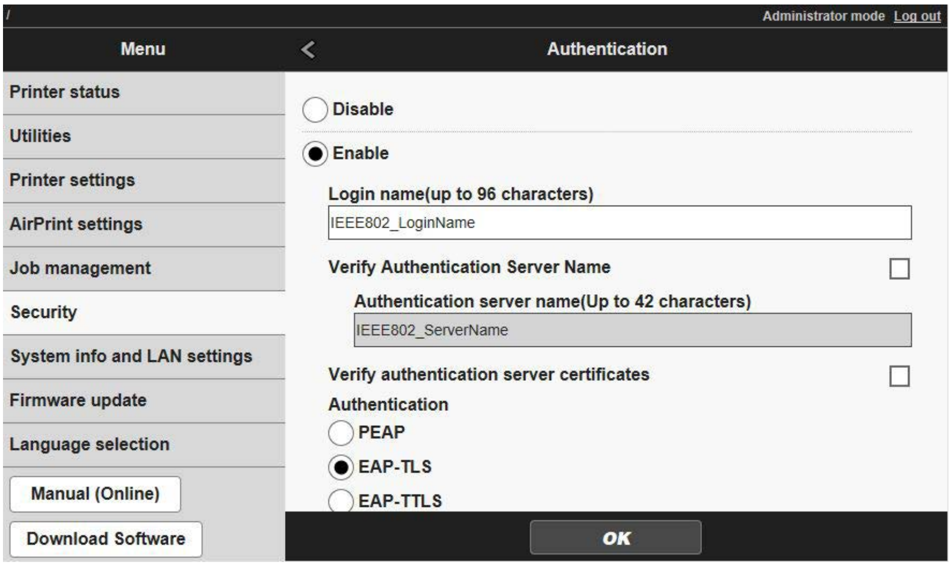
1. Enable the authentication method

Set [Authentication] to [Enable] with the following step.

Remote UI

[Security] ▶ [IEEE802.1X settings] ▶ [Authentication]

When [Enable] is selected, the following settings screen is displayed.



○ Disable

● Enable

Login name(up to 96 characters)

IEEE802_LoginName

Verify Authentication Server Name □

Authentication server name(Up to 42 characters)

IEEE802_ServerName

Verify authentication server certificates □

Authentication

○ PEAP

● EAP-TLS

○ EAP-TTLS

2. Set a Login name, Authentication Server Name, etc.

- Login name

  Set a login name up to 96 characters long to use for connecting to the network.

- Verify Authentication Server Name

  Use the checkbox to turn on or off. On by default.

- Authentication server name

  When [Verify Authentication Server Name] is on, set an authentication server name up to 42 characters long in 1-byte letters and numbers.

- Verify authentication server certificates

  Use the checkbox to turn on or off. On by default.

  When on is selected, a CA certificate must be registered separately.

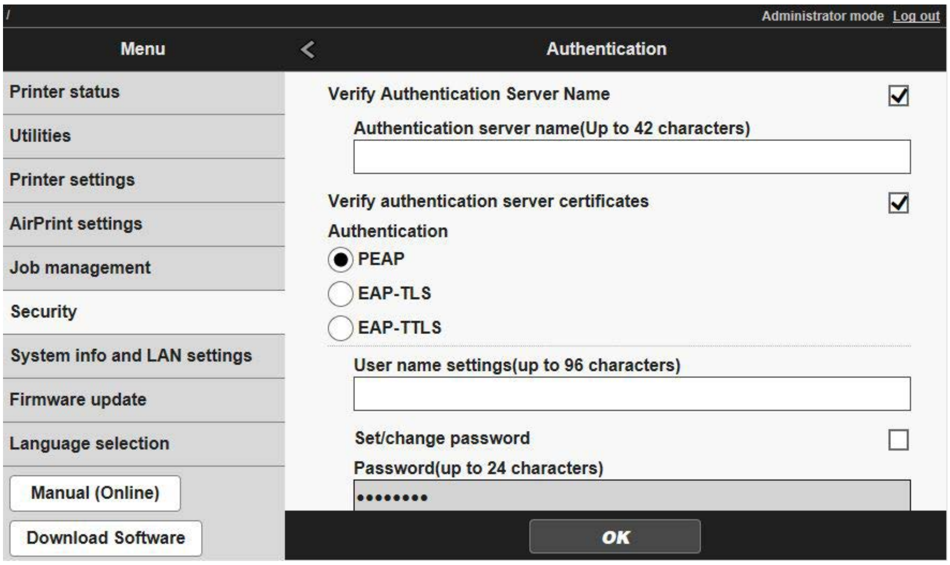
  ➡ Register a CA certificate

3. Set an Authentication Method

Select from [PEAP] / [EAP-TLS] / [EAP-TTLS]. [EAP-TLS] by default.

Depending on the selected authentication method, additional settings may be available.

When PEAP is selected



Verify Authentication Server Name ☑

Authentication server name(Up to 42 characters)

Verify authentication server certificates ☑

Authentication

● PEAP

○ EAP-TLS

○ EAP-TTLS

User name settings(up to 96 characters)

Set/change password □

Password(up to 24 characters)

••••••••

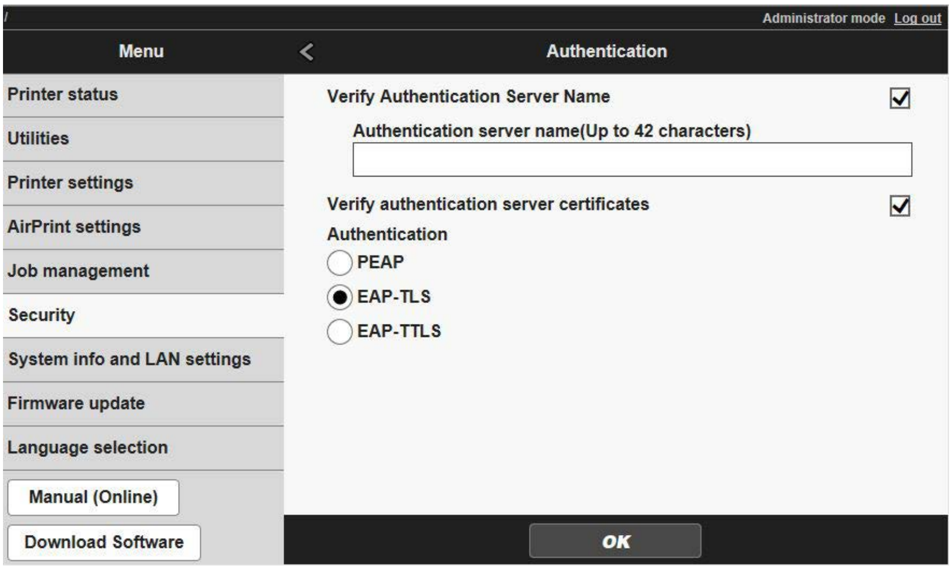
- User name settings

  Set a user name up to 96 characters long to be used for authenticating connection to a network.

- Password

  Set a password up to 24 characters long to be used for authentication.

When EAP-TLS is selected



Verify Authentication Server Name ☑

Authentication server name(Up to 42 characters)

Verify authentication server certificates ☑

Authentication

○ PEAP

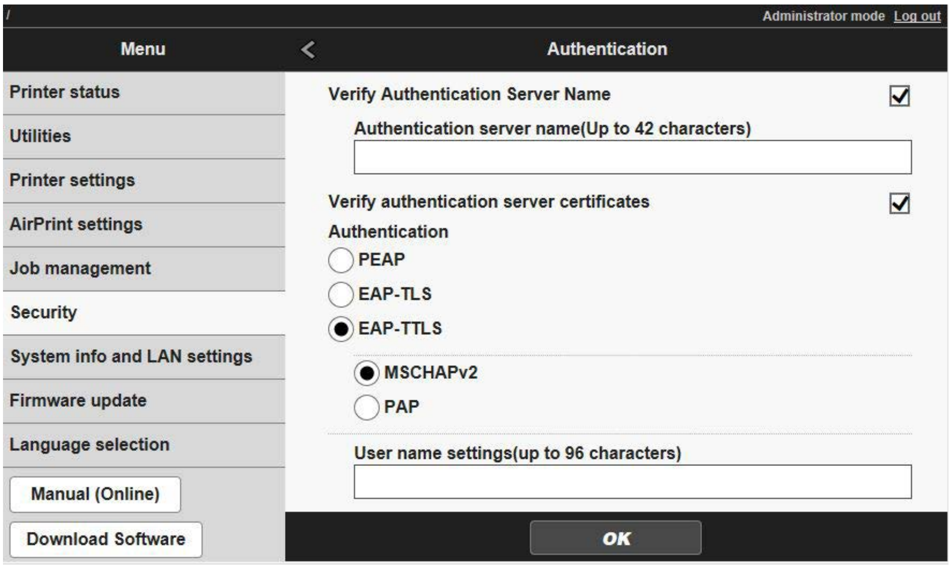
● EAP-TLS

○ EAP-TTLS

A client certificate must be registered separately.

➡ Register a client certificate

When EAP-TTLS is selected



Verify Authentication Server Name ☑

Authentication server name(Up to 42 characters)

Verify authentication server certificates ☑

Authentication

○ PEAP

○ EAP-TLS

● EAP-TTLS

● MSCHAPv2

○ PAP

User name settings(up to 96 characters)

- Internal protocols used for authentication

  Select from [MSCHAPv2] / [PAP]. [MSCHAPv2] by default.
- User name settings

  Set a user name up to 96 characters long to be used for authenticating connection to a network.
- Password

  Set a password up to 24 characters long to be used for authentication.

4. Select [OK]

5. Set a weak encryption restriction and weak certificate restriction

Remote UI

[Security] ▶ [IEEE802.1X settings] ▶ [Weak encryption restriction]

Select from [Restrict] / [Do not restrict]. [Restrict] by default.

Remote UI

[Security] ▶ [IEEE802.1X settings] ▶ [Weak certificate restriction]

Select from [Restrict] / [Do not restrict]. [Restrict] by default.

Registering Certificates

1. Register a client certificate

When EAP-TLS is selected for the authentication method, it is necessary to upload (register) key and client certificates issued by a certificate authority with Remote UI.

Remote UI

[Security] ▶ [IEEE802.1X settings] ▶ [Key and certificate settings] ▶ [Upload key and certificate]

2. Register a CA certificate

It is necessary to enable [Verify authentication server certificates] and register a CA certificate. Upload (register) the certificate with Remote UI.

Remote UI

[Security] ▶ [IEEE802.1X settings] ▶ [CA certificate] ▶ [Upload CA certificate]

Any authentication method also allows you to make settings not to verify a server certificate. In this instance, it is not necessary to upload a CA certificate.

Remote UI

[Security] ▶ [IEEE802.1X settings] ▶ [Authentication] ▶
Deselect [Verify authentication server certificates]

Note

- If it is not possible to connect to Remote UI after restarting the LAN, reload the page in the web browser.

Specifications of keys and certificates that can be used for encrypted communication

➡ 4.3 Algorithms and Formats for Registerable Keys and Certificates

3.7 Encrypting Communication: IPsec

IP Security Protocol (IPsec) is a protocol for encrypted communication over networks. While TLS encrypted communication is a technology for encryption with specific applications such as web browsers and e-mail clients, IPsec communication encrypts at an IP protocol level, enabling more versatile security. Supported only when the IP address setting is IPv6. Not supported with IPv4.

IPsec settings

Panel

[LAN settings] ▶ Select [Wi-Fi], [Wireless Direct], or [Wired LAN] ▶ [Settings] ▶ [Advanced] ▶ [TCP/IP settings] ▶ [IPv6] ▶ [IPsec settings] ▶ Select [Enable] or [Disable]

◆ IPsec-supporting protocols

- IPv6IPsec
- AH
  - HMAC-SHA-1-96
- ESP
  - HMAC-MD5-96
  - DES-CBC
  - 3DES-CBC
  - AES-CBC (* 128, 192, and 256-bit key lengths supported)

◆ IKE-supporting protocols

- IKEv1
- IKEv1 Phase1
  - Main mode
- Authentication method (IKEv1)
  - Pre-shared key (16 characters or less, 1-byte letters and numbers)
- DH key (IKEv1)
  - Group 1
  - Group 2
  - Group 5
  - Group 14
- Encryption (IKEv1)
  - DES-CBC
  - 3DES-CBC
  - AES-CBC (* 128, 192, and 256-bit key lengths supported)
- Authentication (IKEv1)
  - AUTH-HMAC-SHA1-96
  - AUTH-HMAC-MD5-96

4 Appendix

Describes how to update the printer's firmware and how to check the serial number.

4.1 Updating the Firmware

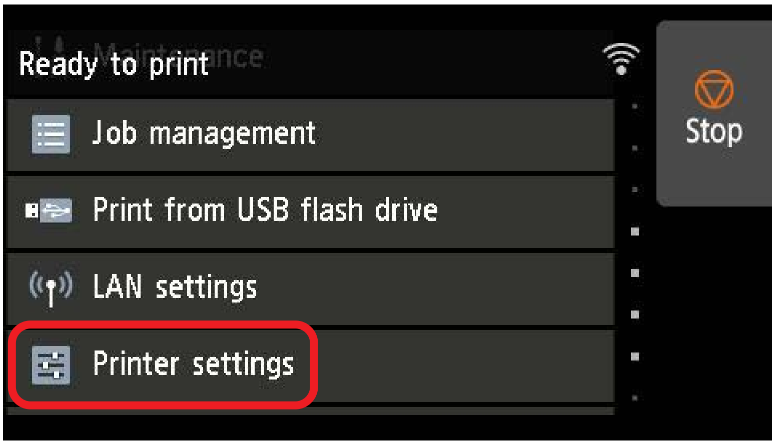
When new firmware is released, it will be displayed in Remote UI. New firmware releases sometimes include improvements to security functionality, so always be sure to update firmware to the latest version. Update firmware at the operation panel or with Remote UI.

Important

- ► Before updating the firmware, check that the printer is connected to the Internet.
- ► If the administrator password is set, it will be necessary to enter the administrator password when updating the firmware.

Updating Firmware from the Operation Panel

1. **In the home screen, select [Printer settings]**



2. **Select [Firmware update]**

If an administrator password is set, enter the administrator password.

3. Select [Install update]

4. Select [Yes]

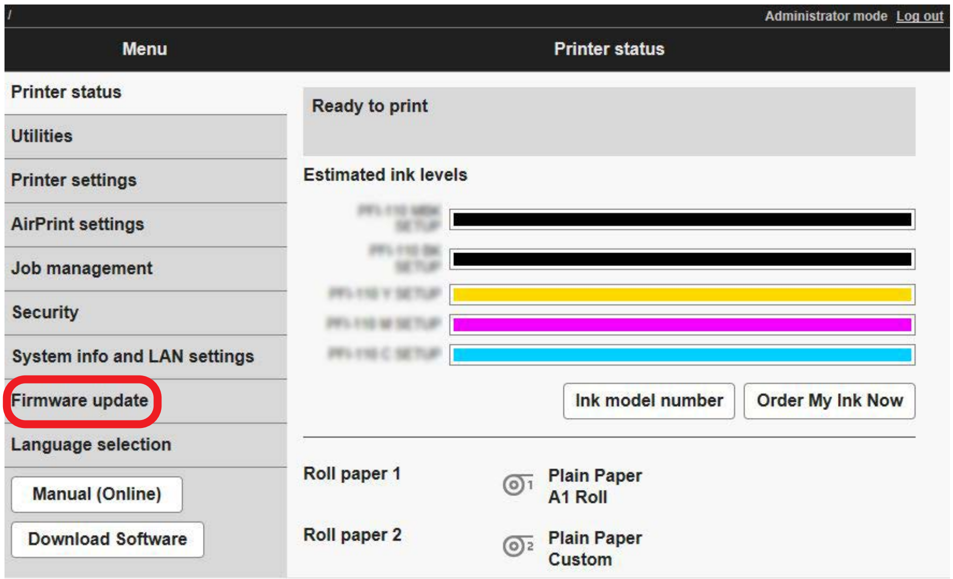
5. Check the message on the operation panel, and select [Start update]

Updating the Firmware from Remote UI

1. Start Remote UI

➡ Starting Remote UI

2. Select [Firmware update]



Ready to print

Estimated ink levels

Roll paper 1 Plain Paper A1 Roll

Roll paper 2 Plain Paper Custom

3. Select [Install update]

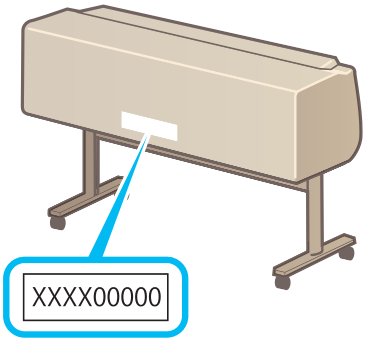
4. Check the onscreen message, and select [Update]

Note

- If an update fails, check the Wi-Fi router and other network settings.

4.2 Checking the Printer's Serial Number

The printer's serial number is 9 characters (4 letters followed by 5 numbers) and appears on a sticker on the printer.



Note

- ► The printer's serial number also appears on the warranty.

4.3 Algorithms and Formats for Registerable Keys and Certificates

Item	Description
RSA signature algorithm	SHA-256
RSA public key algorithm (key length)	RSA (2048 bits)
DSA signature algorithm	Not supported
DSA public key algorithm (key length)	Not supported
ECDSA signature algorithm	SHA-256
ECDSA public key algorithm (key length)	ECDSA (P256 / P384 / P521)
Certificate formats	PKCS#12 format X.509 DER format (Key pair used with EAP-TLS is PKCS#12 only, CA certificate is X.509 DER format only)
Extensions	PKCS#12 format: p12/pfx X.509 DER format: cer/der
Registerable number of items	Keys/certificates: 2 (server certificate for TLS, client certificate for IEEE 802.1X) CA certificates: 5 (for IEEE 802.1X)
Certificate file size limits	• Server certificate for TLS: 4 KB/certificate (However, for the models below, certificate: 1.5 KB and private key: 2.5 KB totalling 4 KB) • Client certificate for IEEE 802.1X: 4 KB/certificate (However, for the models below, 2 KB/certificate) • CA certificate: (for IEEE 802.1X): 4 KB/certificate (However, for the models below, 2 KB/certificate) [Model name] • imagePROGRAF TA-30 / TA-20 • imagePROGRAF TA-5300 / TA-5200 • imagePROGRAF TM-305 / TM-300 / TM-205 / TM-200 • imagePROGRAF TM-5305 / TM-5300 / TM-5205 / TM-5200 • imagePROGRAF PRO-6000 / PRO-4000 / PRO-2000 / PRO-6000S / PRO-4000S • imagePROGRAF PRO-560 / PRO-540 / PRO-520 / PRO-560S / PRO-540S • imagePROGRAF TX-4000 / TX-3000 / TX-2000, with firmware version 1.39 or earlier • imagePROGRAF TX-5400 / TX-5300 / TX-5200, with firmware version 1.39 or earlier