RSA Key Generation Vulnerability - Key Check and Fix

For imagePROGRAF series and PIXMA/MAXIFY series

1st Edition

Contents

1 Introduction

This guide explains how to update the firmware and register digital certificates.

Contents:

This guide contains the following chapters:

- Starting Remote UI
- Firmware Update
- Updating SSL/TLS Communication Digital Certificate
- Registering a Root Certificate

The screens used in this guide may differ slightly from those shown with your printer. For details, refer to the online manual for your printer model. https://ij.start.canon

2 Starting Remote UI

You can use the Remote UI to update the firmware over the network. Access the printer from your smartphone, tablet, or computer's web browser.

Note

Before using the Remote UI, connect the printer to your network.

See the online manual for your printer model for usable OSs and web browsers.

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

Important

The method to check the IP address of your printer may differ slightly from the instructions above. For details about each screen, see the online manual for your printer model. https://ij.start.canon

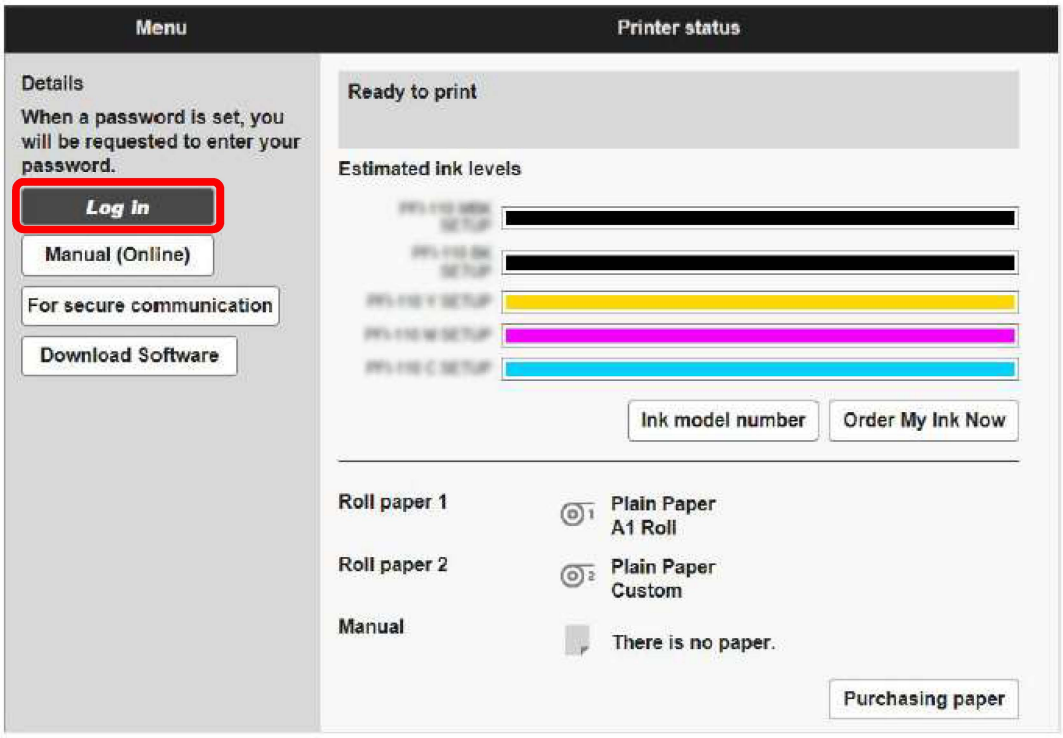
Remote UI

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



3. Select [Log in]

A password authentication screen is displayed.

4. Enter the password, and click [OK]

The Remote UI top screen is displayed.

3 Firmware Update

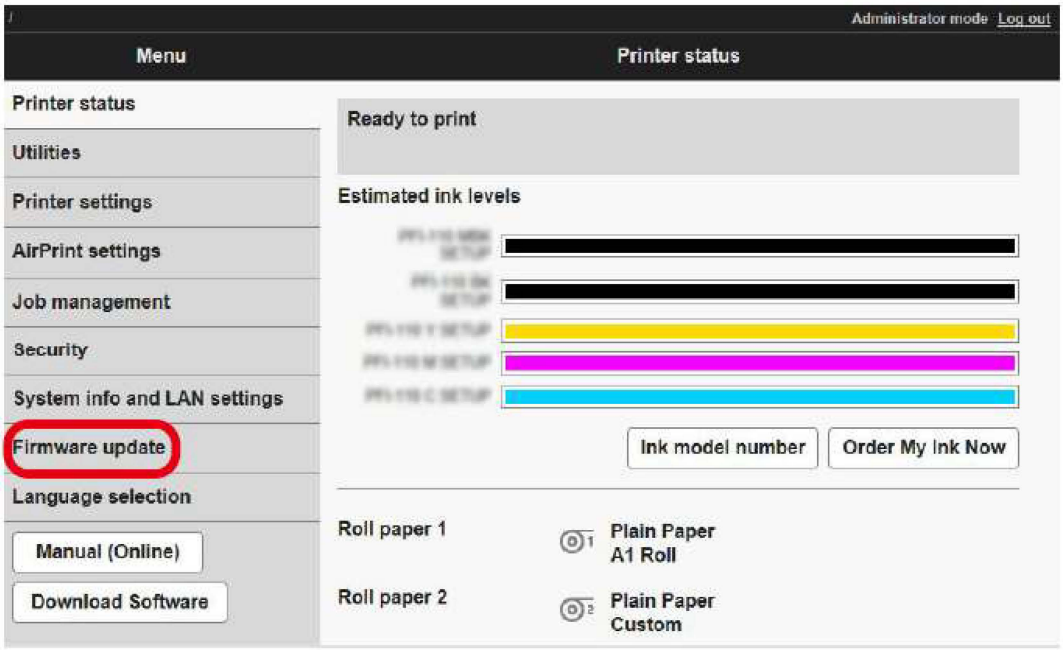
Once Remote UI is running, update the printer's firmware.

When new firmware is released, it will be displayed in the Remote UI. New firmware releases include improvements to security functionality, be sure to update firmware to the latest version.

Updating the Firmware from Remote UI

Remote UI

1. Select [Firmware update]



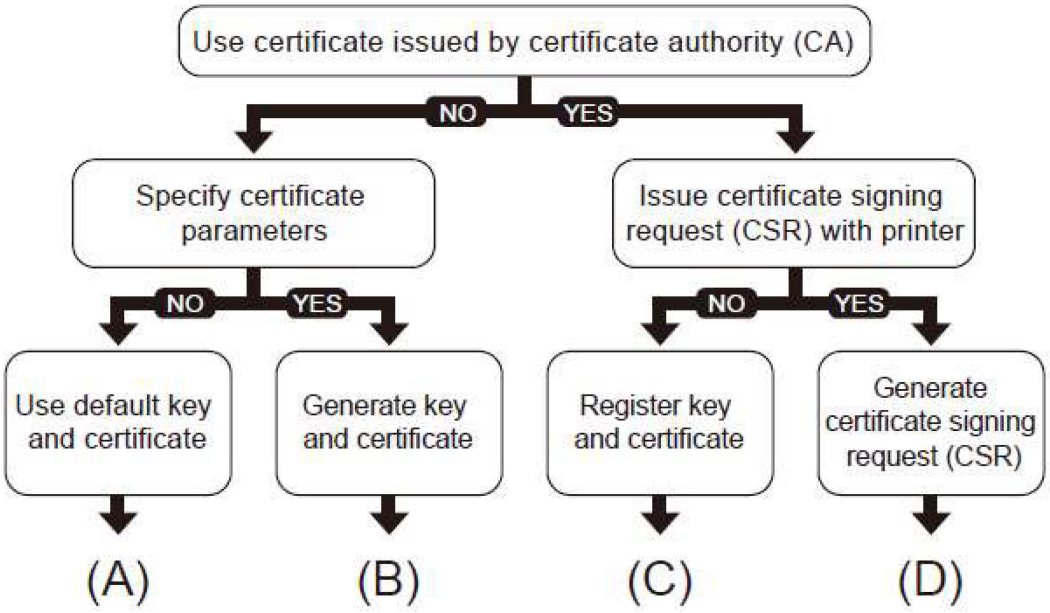
2. Select [Install update]

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

4 Updating SSL/TLS Communication Digital Certificate

After the firmware update is complete, refer to the chart below to determine the correct pattern for registering your SSL/TLS communication digital certificate. Update the SSL/TLS communication digital certificate if required.

SSL/TLS Digital Certificate Registration Patterns:



Determine the appropriate pattern, and follow the instructions for that pattern.

(A) Use default key and certificate:

The default key and certificate already installed in the printer can be used. The key and certificate do not need to be updated.

Finally, install the root certificate on your browser. > Registering a Root Certificate

(B) Generate key and certificate:

First, you must delete the current key and certificate. Follow the instructions below to delete your current key and certificate, and generate new ones.

1. Delete the key and certificate

Operation: [Security] > [SSL/TLS settings] > [Delete key and certificate]

Delete the displayed key and certificate.

2. Generate key and certificate

Operation: [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.

Finally, install the root certificate on your browser. > Registering a Root Certificate

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

The same key and certificate as before firmware update can be used, and no action is required after updating. Also, you do not need to install a root certificate on the browser.

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

First, you must delete the current key and certificate. Follow the instructions below to delete your current key and certificate, and generate new ones.

1. Delete the key and certificate

Operation: [Security] > [SSL/TLS settings] > [Delete key and certificate]

Delete the displayed key and certificate.

2. Generate key and certificate

Operation: [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.

3. Upload certificate

Operation: [Security] > [SSL/TLS settings] > [Upload key and certificate]

Follow the instructions below to upload a certificate signed by a certificate authority.

(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

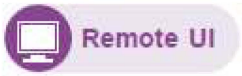
(5) Select the [Restart LAN] button

You do not need to install the root certificate on your browser.

5 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 the 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.

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



1. Select [For secure communication]

2. Select [Download]

The root certificate begins downloading.

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

A [Certificate] screen is displayed.

4. Select [Install Certificate]

A [Certificate Import Wizard] screen is displayed.

5. Select [Next]

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

   A [Select Certificate Store] screen is displayed.
8. **Select [Trusted Root Certification Authorities], and select [OK]**
9. **In the [Certificate Import Wizard] screen, select [Next]**
10. **After [Completing the Certificate Import Wizard] is displayed, select [Finish]**

    A [Security Warning] screen is displayed.
11. **Select [Yes] in the [Security Warning] screen**
12. **In the [Certificate Import Wizard] screen, select [OK]**

    The root certificate is installed.

Update is now complete.