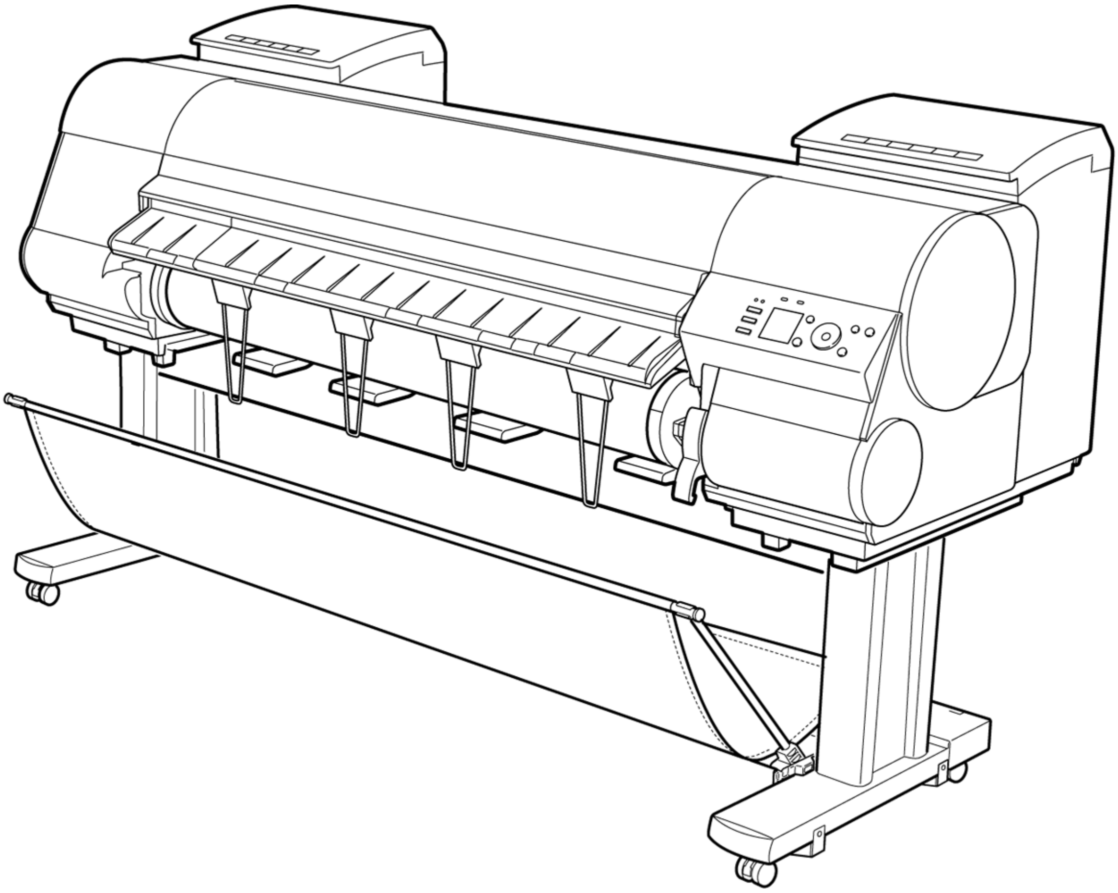
Canon

Useful Tips for Reducing the Risk of Unauthorized Access for Large-Format Inkjet Printer

IMPORTANT If you are an administrator, please read through this document.



Overview and Use of This Guide

Objectives

This guide provides additional information related to the Canon large-format inkjet printer, and in particular, steps you can take to enhance the secure operation of this device. This document will help you better understand how the device functions and will help you feel confident that it operates, stores or transmits device data in a secure and accurate manner, including any potential impact on security and network infrastructure.

We recommend that you read this document in its entirety and take appropriate actions consistent with your information technology security policies and practices as an enhancement to your organization's existing security policies. Since security requirements will vary from customer to customer, you have the final responsibility to ensure that all implementations, re-installations, and testing of security configurations, patches, and modifications are appropriate and required for your environment.

Intended Audience

This guide is intended for use by network administrators, dealers and other business customers. In order to get the most from this guide, you should have an understanding of:

- your network environment,
- any restrictions placed on applications that are deployed on that network, and
- the applicable operating system.

Limitations to This Guidance

This guide is meant to help you evaluate the device and the security of your network environment, but it cannot be a complete information source for all potential customers. This guide proposes a hypothetical customer printer environment; if your network environment differs from the hypothetical environment, your network administration team and your dealer or Authorized Canon Service Provider must understand the differences and determine whether any modifications or additional action is needed. Additionally:

- This guide only describes those features within the application that have some discernible impact to the general network environment, whether it be the overall network, security, or other customer resources.

- The guide's information is related to the specified Canon device above. Although much of this information will remain constant through the device life cycle, some of the data is revision-specific, and will be revised periodically. IT organizations should check with their Authorized Canon Service Provider to determine the appropriate deployment for your environment.

Thank you for using Canon products. This document gives information on how to protect your large-format inkjet printer (“LFP”) from unauthorized access from an external network. Users and system administrators are advised to read through this document before using an LFP in a network environment.

INTRODUCTION

In recent years, by connecting your LFP to a network, you can make use of various useful functions, such as printing via the network, controlling print jobs using Remote UI, which uses the HTTP protocol, and browsing the machine’s print history. The following are methods for protecting your LFP from unauthorized access when used in a network environment. Setting procedures and illustrations described here are examples provided for reference and may differ from those of your LFP. For more information, please refer to the user manual provided with your machine.

Methods for protecting your LFP from unauthorized access:

1. Use the LFP in an access-controlled environment.

2. Use a private IP address.

3. Use a firewall or Wi-Fi router to limit communication.

4. Secure the communication using security protocols.

5. Secure your LFP using password protection.

6. Note: Precautions when Using Remote UI

USE THE LFP IN AN ACCESS-CONTROLLED ENVIRONMENT.

Direct access to devices such as Canon LFP, computers, and Wi-Fi routers increases the risk of data leaks and malicious attacks.

To prevent access by unauthorized individuals, install the device in an access-controlled, lockable area.

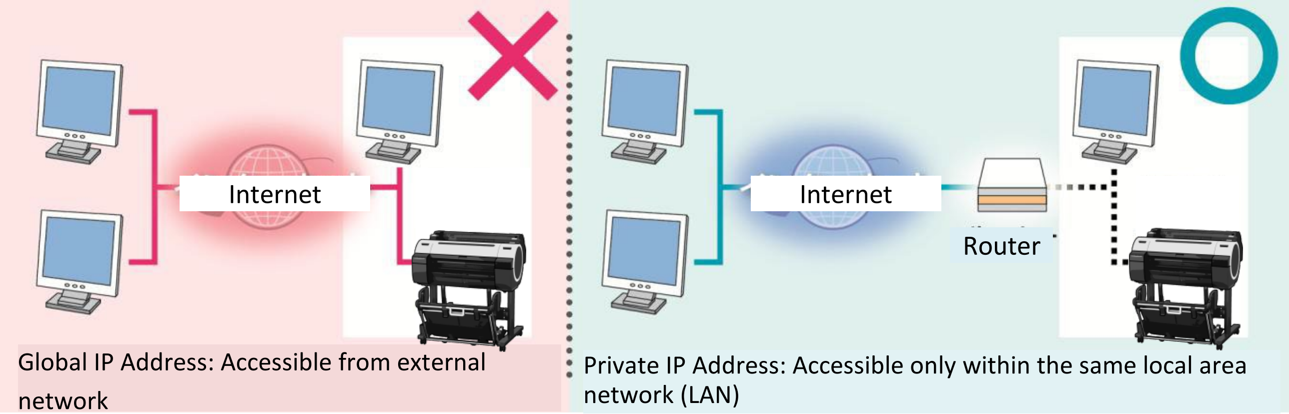
USE PRIVATE IP ADDRESS

An IP address is a number that is assigned to each device on a network. An IP address that is used to connect to the Internet is called a “global IP address,” while an IP address within a local area network (LAN) is called a “private IP address.” If a machine uses a global IP address, it becomes accessible by the general public, which raises the possibility of information leakage due to unauthorized access by third parties. On the other hand, if a machine uses a private IP address, then it can only be accessed by users connected to the same LAN.

In general, Canon recommends that you use a private IP address for your LFP. An IP address that falls within the ranges listed below is a private IP address. Please check that your LFP’s IP address is a private one.

Private IP address range:

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255



Global IP Address: Accessible from external network

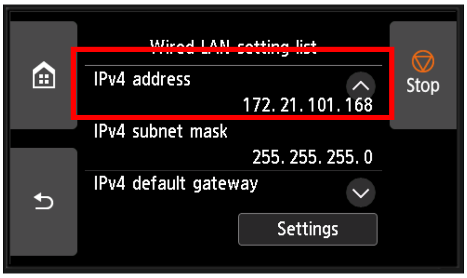
Private IP Address: Accessible only within the same local area network (LAN)

NOTE

Even if your LFP uses a global IP address, you can reduce the risk of unauthorized access by blocking access from an external network through such methods as using a firewall. Please consult with a corporate network administrator when assigning a global IP address to your LFP.

How to check your printer’s IP address (Example)

[Device settings]
↓
[LAN settings]
↓
[Wi-Fi]


Wired LAN setting list

IPv4 address 172. 21. 101. 168

IPv4 subnet mask 255. 255. 255. 0

IPv4 default gateway

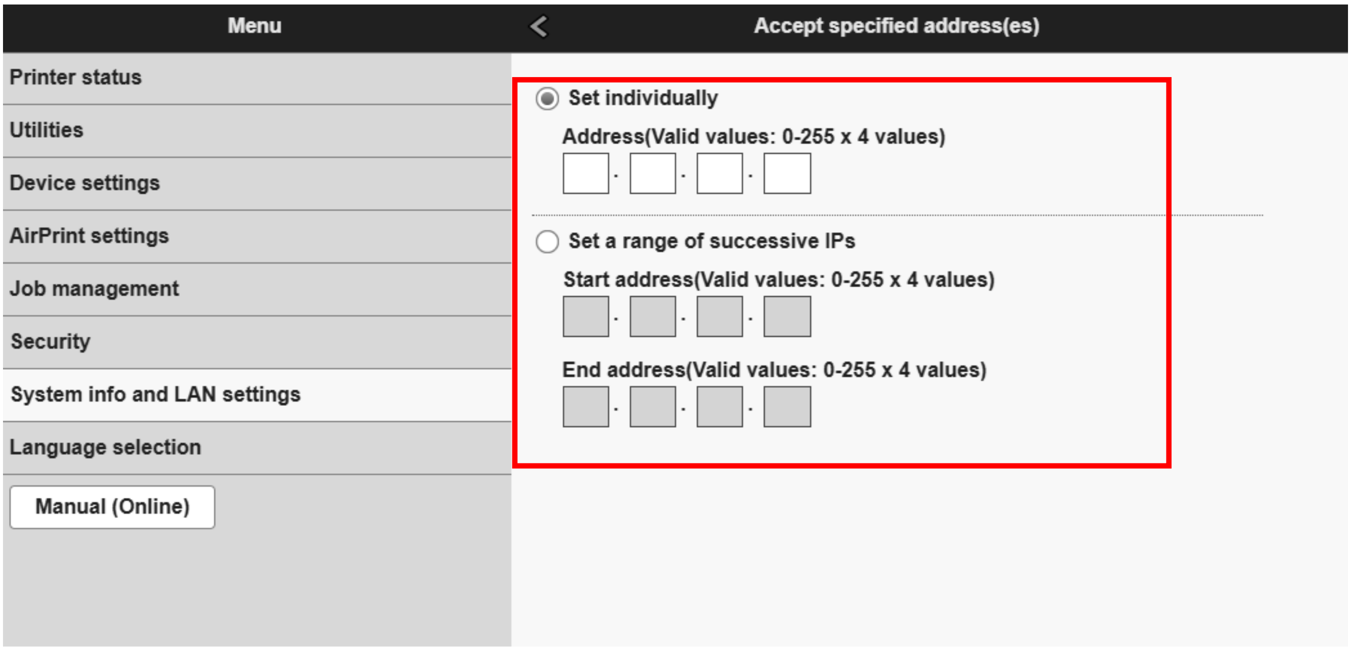
Note: For more information about how to verify the IP address of your LFP, please refer to the user manual.

USING A FIREWALL OR WI-FI ROUTER TO LIMIT COMMUNICATION

A firewall is a system that prevents not only access by external networks, but also attacks on and intrusions to a local network. Firewalls can block potentially dangerous unauthorized access from external networks by restricting specified external IP addresses from accessing a network environment.
Canon's LFP is equipped with an IP address range configuration feature that enables IP address filtering.
Similarly, most Wi-Fi routers include comparable functionality. It is essential to secure the router with a strong password and, exercise caution when making any configuration changes.

IP Address Range Setting Screens

Remote UI includes a function for selecting an IP address range.
Note: For more information regarding operating Remote UI, please refer to the LFP's user manual.



Accept specified address(es)

● Set individually
Address(Valid values: 0-255 x 4 values)
□.□.□.□

○ Set a range of successive IPs
Start address(Valid values: 0-255 x 4 values)
□.□.□.□
End address(Valid values: 0-255 x 4 values)
□.□.□.□

NOTE
Remote UI (User Interface) is software that allows you to access the LFP from a Web browser. Remote UI allows users to verify and modify various printer settings without having to operate the machine directly. Users can access the Remote UI's portal page from a computer screen by entering the machine's IP address into a Web browser.

SECURE THE COMMUNICATION USING SECURITY PROTOCOLS.

A security protocol is a standard designed to protect the security of a Wi-Fi network. When connecting a Wi-Fi router to your LFP, make sure that each device uses the most secure security protocol it supports, such as WPA2 or higher.

MEMO

Refer to the product specifications of your Wi-Fi router and Canon LFP to check which security protocols are supported.

To enhance the security of communication between your LFP and the PC, it is also effective to configure encrypted communication (SSL/TLS) using a server certificate and key.

Launch the Remote UI and select TLS version 1.2 or higher.

MEMO

Some products do not support encrypted communication settings.
In such cases, it is recommended to connect the Canon LFP to a device (such as a PC or smartphone) that supports TLS 1.2 or higher.

SECURE YOUR LFP USING PASSWORD PROTECTION

By setting a password, you can protect various data on your LFP and significantly reduce the risk of information leakage in case the machine is hacked.

Note: - If a default password has been set, change it.

- **<u>No password is set by default</u>** depending on the printer model. Set the password.

- For specific procedures for setting the password, refer to the Instruction Manual of the printer.

- Password settings for the printer’s data storage box can be configured via the Remote UI. (Note that the data storage box is available only on models equipped with a built-in hard disk.)

MEMO

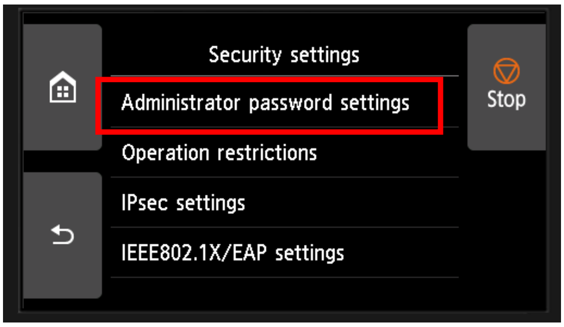
Printers have the password functionality for printer protection. What is important for your security is the proper use of the password. Keep the following in your mind in using the password:

● Always set the password.
● Avoid using an easy-to-guess password.
● DO NOT tell the password to others.

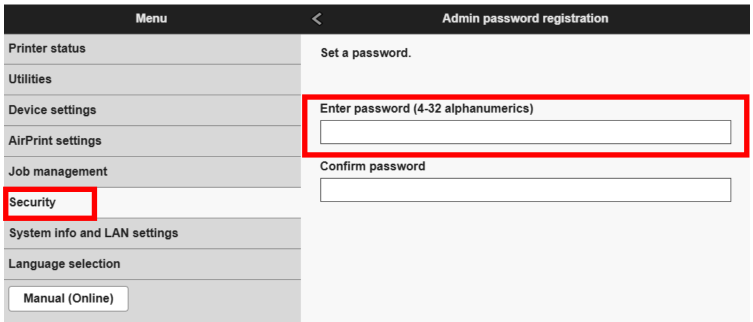
Password Setting Screens

System Administrator Information input screen

LFP Operation Panel

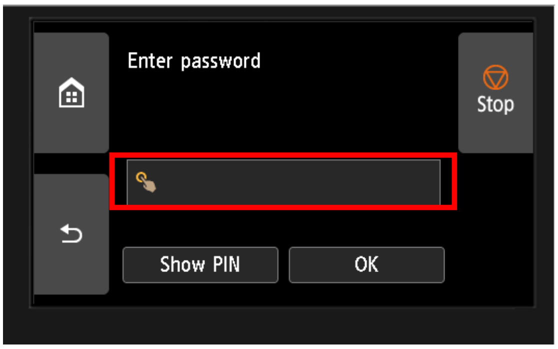


Remote UI

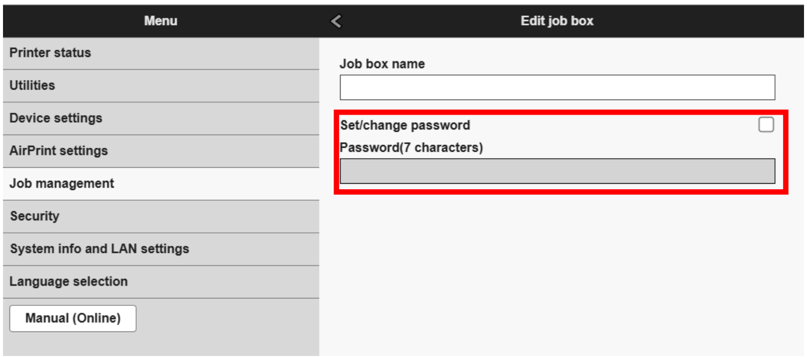


Data storage box password screen

LFP Operation Panel



Remote UI



NOTE

■ Precautions When Using Remote UI

Do not access other websites when the browser is accessing the Remote UI of your LFP.

Do not forget to close the web browser if you leave the computer or after the configuration is complete.

Canon

Revision history:

June 1, 2025	Security-related information has been updated.
January 1, 2023.	The UI displays have been updated.