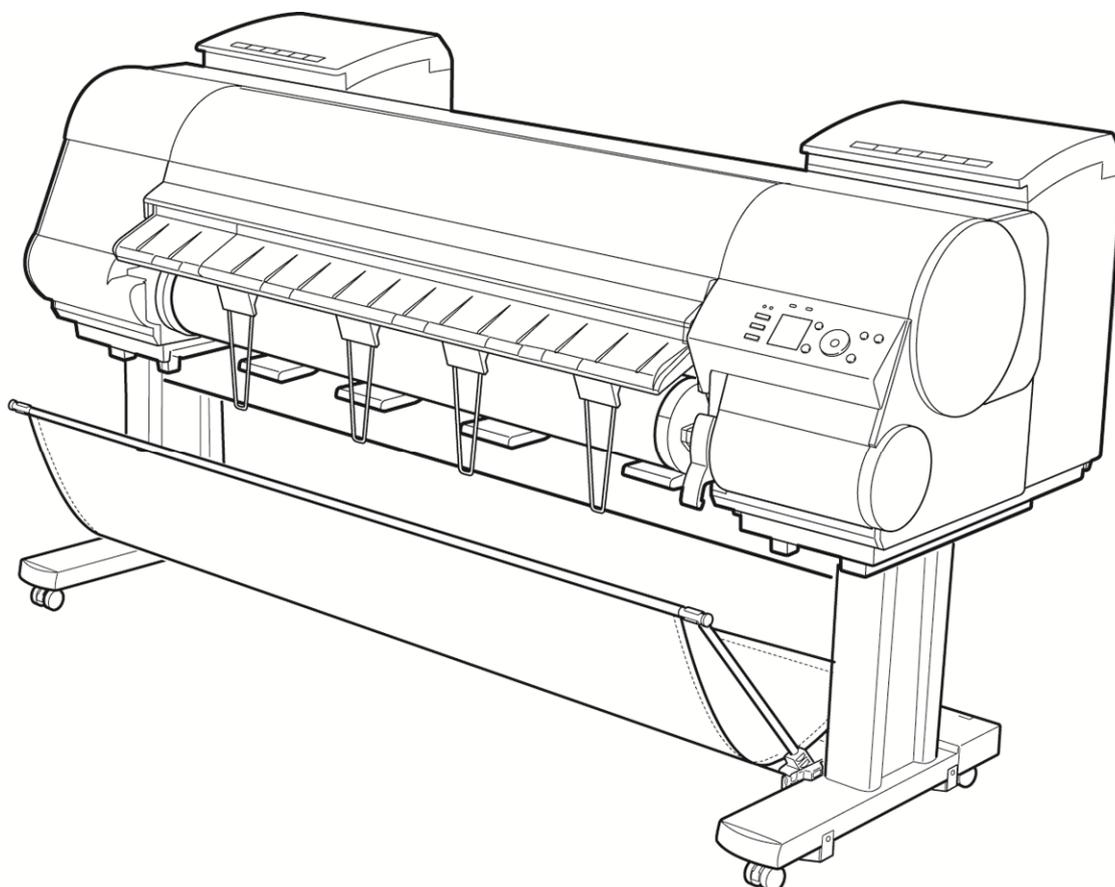




Useful Tips for Reducing the Risk of Unauthorized Access for Large -Format Inkjet Printer

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 a private IP address.
2. Use a firewall or Wi-Fi router to limit communication.
3. Set the password to your printer.
4. Note: Precautions when Using Remote UI

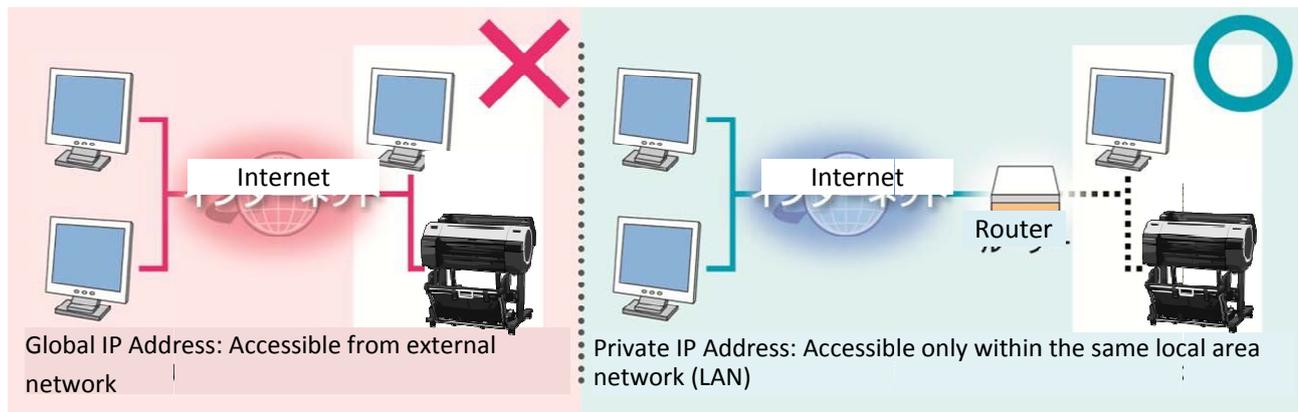
USE PRIVATE IP ADDRESS

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

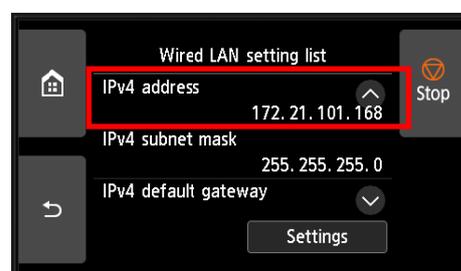


NOTE

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)

Setup
↓
[Device settings]
↓
[LAN settings]
↓
[Confirm LAN settings]
↓
[Wired LAN setting list]



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

RESTRICT COMMUNICATION BY USING FIREWALLS

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. IP addresses can also be filtered using functions included in a Canon LFP.

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.

The screenshot shows the Remote UI interface for device iPF755. The browser address bar displays `http://172.21.139.75/pages/_infoadm.htm`. The page title is "RemoteUI <Information> ;;... x". The interface includes a sidebar with navigation options: "English language", "Administrator Mode" (with a "Log Out" button), "Device Manager" (expanded), "Status", "Information" (highlighted), "Features", "Network", "Job Manager", "Device Selection", and "Support Links". The main content area is titled "Information" and shows "Last Updated :2015/04/08 11:13:59". It is divided into three sections: "Device Information" (with an "Edit..." button), "Head Information", and "Security" (with an "Edit..." button highlighted by a red box). The "Device Information" section lists: Device Name, Location, Administrator, Phone, Comments(E-mail), Manufacturer (CANON INC.), Product Name (iPF755), and Version (1.38). The "Head Information" section lists: Lot Number (redacted) and Days elapsed (26). The "Security" section lists: Administrator Password (with a "Change Password" button).

The screenshot shows the Remote UI "IPv4 Address Range Setting" page. The browser address bar displays `http://172.21.139.75/pages/ed_sclt.htm`. The page title is "RemoteUI <Edit Security> : ... x". The page is titled "IPv4 Address Range Setting" and features a checkbox labeled "Restrict TCP/IP Printing" which is checked and highlighted by a red box. Below this are two radio button options: "Permit for specified address only" (selected) and "Reject for specified address only". There is an "IP Address :" label followed by a text input field. A "Delete" button is located to the right of the input field. Below the input field, the IP address "172.68.0.123" is entered and highlighted by a red box. An "Add" button is located to the right of the input field. A note at the bottom states: "* Successive IP addresses can be set by entering 'Start Address-End Address.'"

Administrator Mode

Log Out

- Device Manager
 - Status
 - Information
 - Features
 - Network
- Job Manager
- Device Selection
- Support Links

Change the following settings. OK Cancel

SNMP Setting

Enable SNMPv1 : On Off
 Access Rights : ReadOnly ReadWrite
 Community Name :
 Enable SNMPv3 : On Off

IPP Authentication

Enable IPP Authentication : On Off
 User Name :
 Password :

FTP Authentication

Enable FTP Authentication : On Off
 User Name :
 Password :

IPv4 Address Range Setting

Restrict TCP/IP Printing
 Permit for specified address only
 Reject for specified address only

IP Address : Delete
 Add

* Successive IP addresses can be set by entering "Start Address-End Address."

Security Edit...

Administrator Password : Change Password

SNMP Setting

Enable SNMPv1 : On
 Access Rights : ReadWrite
 Community Name : public
 Enable SNMPv3 : Off
 Custom Settings : Display Custom Settings

IPP Authentication

Enable IPP Authentication : Off
 User Name :

FTP Authentication

Enable FTP Authentication : Off
 User Name :

IPv4 Address Range Setting

TCP/IP Printing : Restricted
 Restriction Method : Permit printing from specified address
 IP Address :

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.

Note: For more information regarding operating Remote UI, please refer to the LFP's user manual.

PPROTECT LFP DATA WITH PASSWORDS

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.

- **No password is set by default** depending on the printer model. Set the password.
- For specific procedures for setting the password, refer to the Instruction Manual of the printer.
- A password can be set for the machine's data

storage box using Remote UI. (A data storage box is only included in models employing a 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.
- Change the password periodically.
- Avoid using an easy-to-guess password.
- DO NOT tell the password to others.

Password Setting Screens

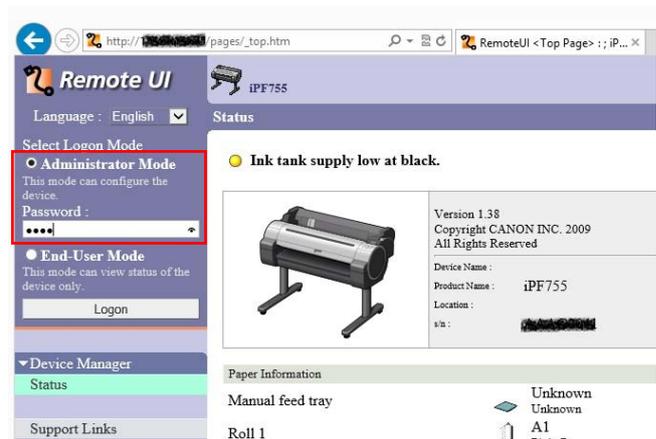
LFP Operation Panel

System Administrator Information input screen



Remote UI

Remote UI login password screen



LFP Operation Panel

Data storage box password input screen



Remote UI

Data storage box password screen



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 step away from the computer or after you finish changing settings.



Revision history:

January 1, 2023. The UI displays have been updated.