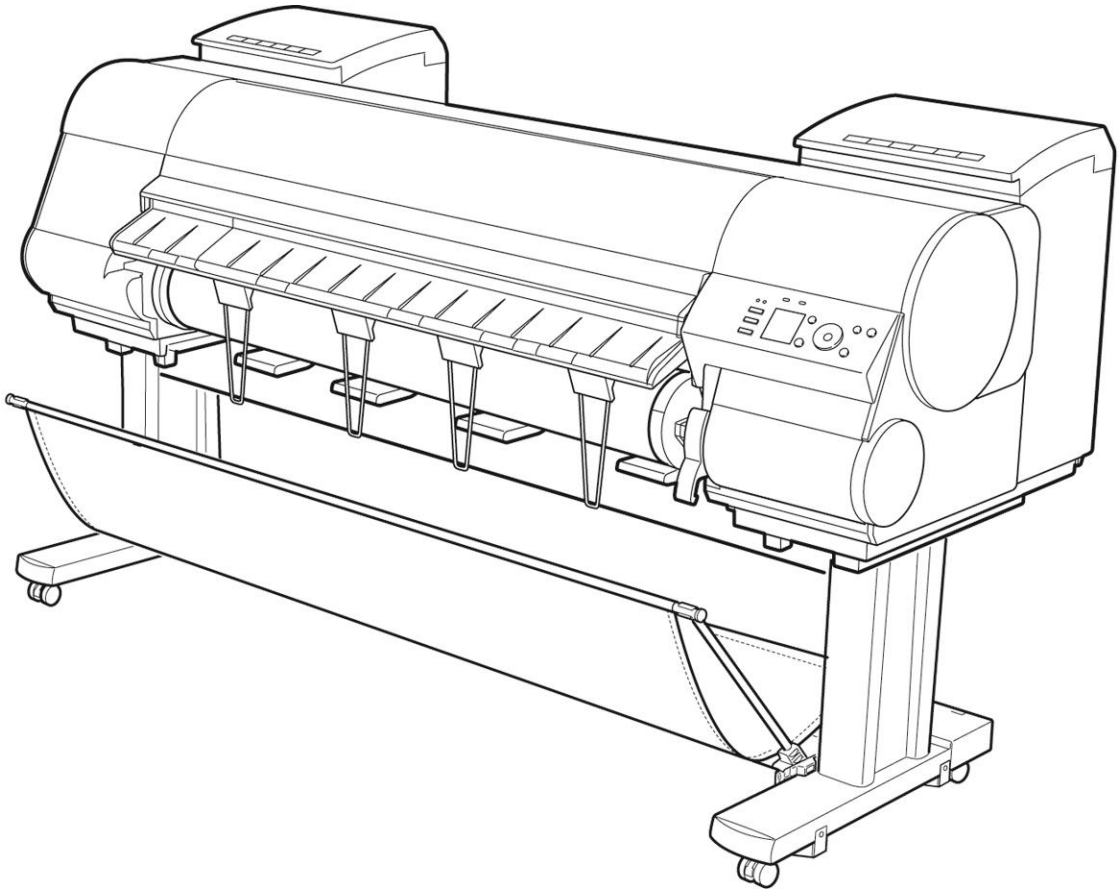
Useful Tips for Reducing the Risk of Unauthorized Access for Large-Format Inkjet Printer (imagePROGRAF Series)

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 imagePROGRAF Series, 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 imagePROGRAF-series 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. Restrict communication by using firewalls
3. Protect LFP data with passwords

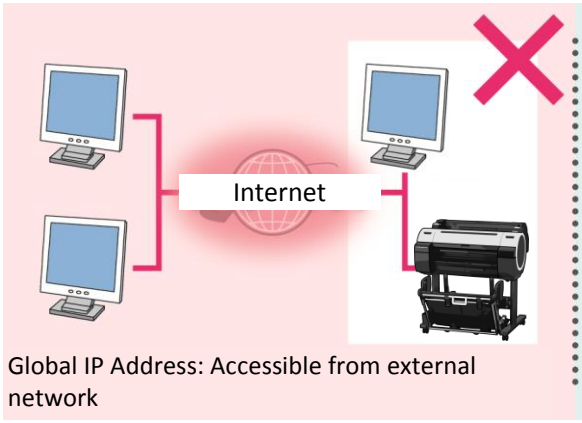
USE PRIVATE IP ADDRESS

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.

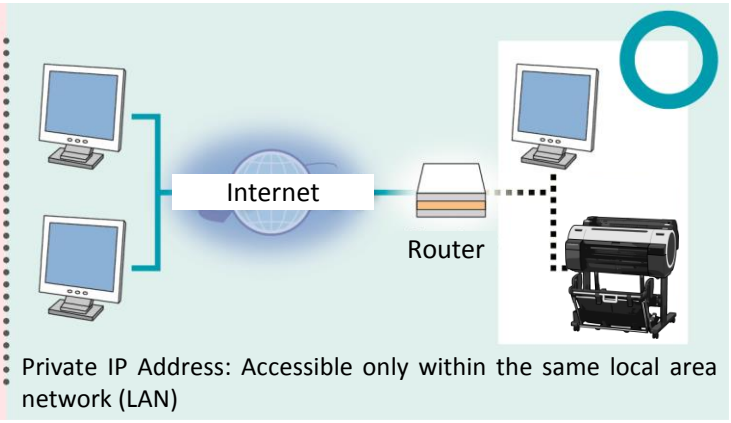
In general, Canon recommends that you use a private IP address for your LFP. An IP address that falls within the ranges listed below is a private IP address. Please check that your LFP’s IP address is a private one.

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 verify your LFP’s IP address

Menu key
↓
[Set. ／ Adj.]
↓
[Interface Setup]
↓
[TCP／IP]
↓
[IPv4]
↓
[IPv4 Setting]
↓
[IP Address]

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

How to check IP address for Specific Models

Menu Key
↓
[Interface Setup]
↓
[TCP／IP]
↓
[IP Setting]
↓
[IP Address]

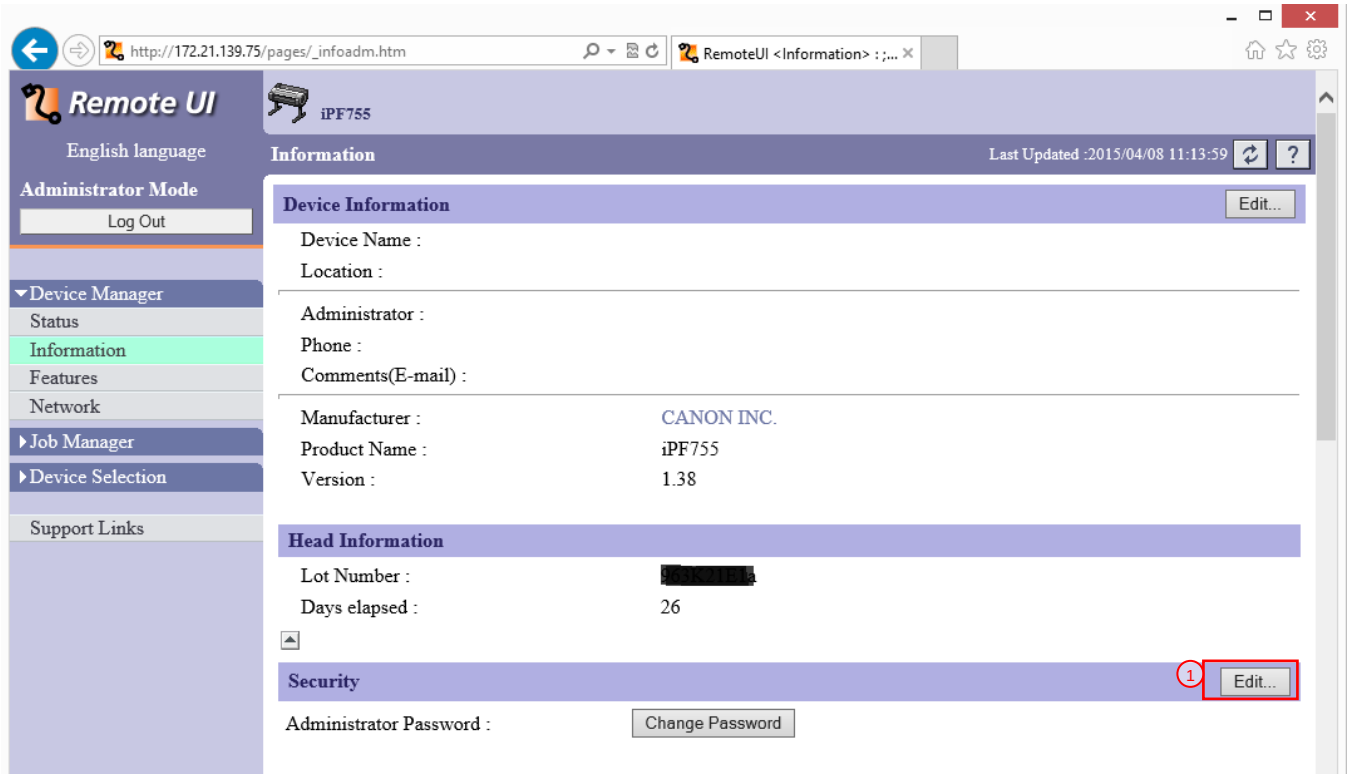
Note: For more information about how to verify the IP address of your LFP, please refer to the user manual included with your machine.

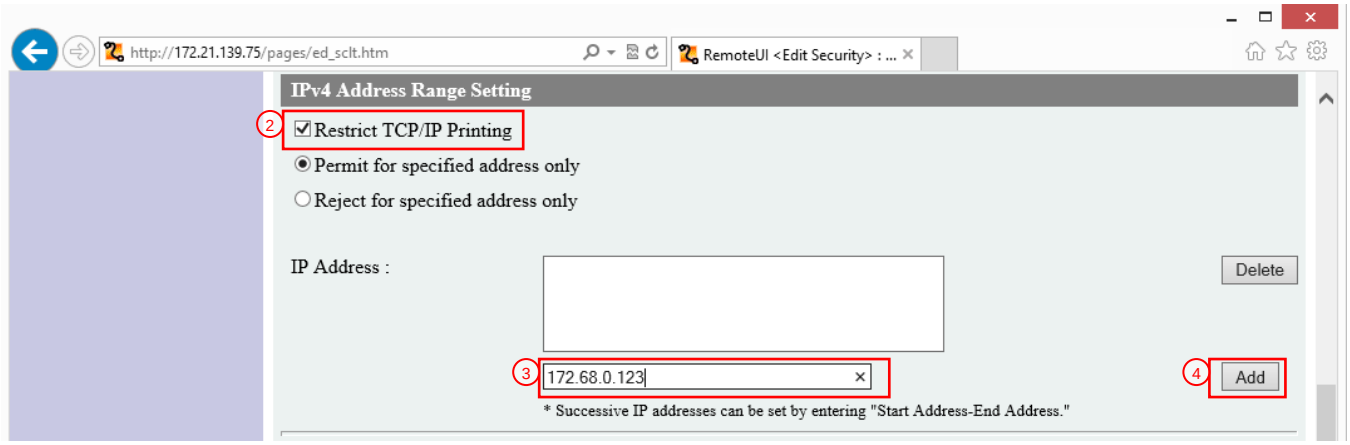
RESTRICT COMMUNICATION BY USING FIREWALLS

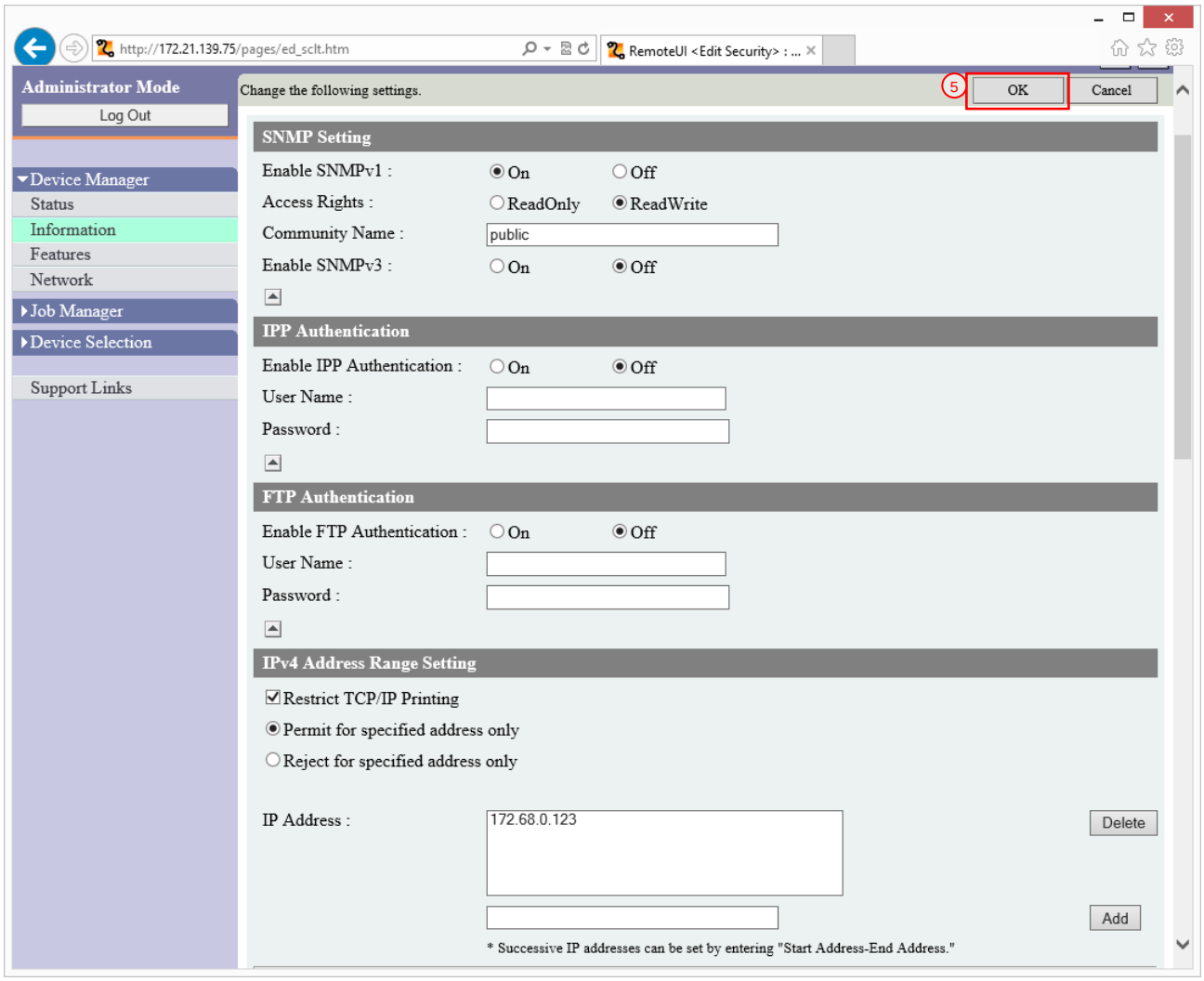
A firewall is a system that prevents not only access by external networks, but also attacks on and intrusions to a local network. Firewalls can block potentially dangerous unauthorized access from external networks by restricting specified external IP addresses from accessing a network environment. IP addresses can also be filtered using functions included in a Canon LFP.

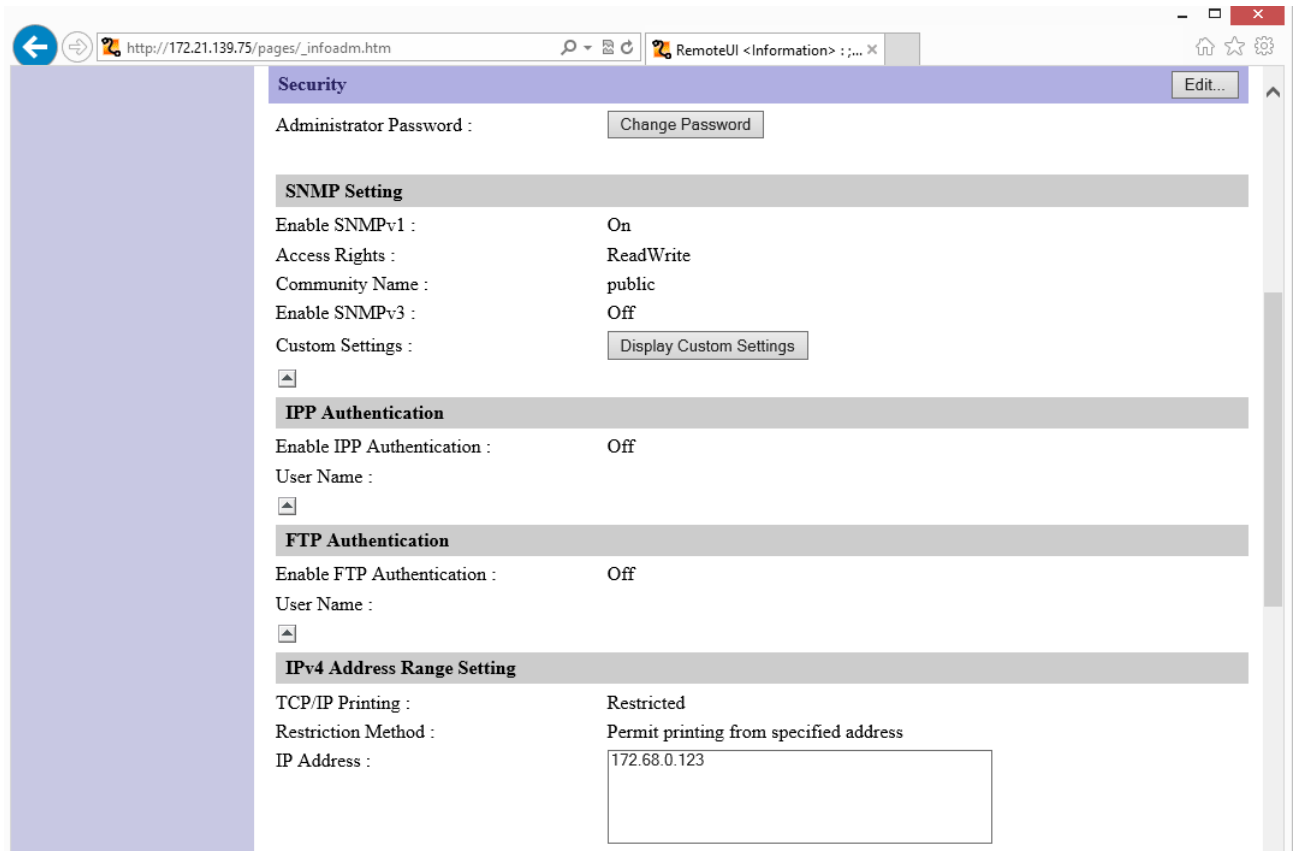
■ IP Address Range Setting Screens (imagePROGRAF Series)

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.






http://172.21.139.75/pages/ed_sclt.htm
RemoteUI <Edit Security> : ...
Administrator Mode
Log Out
Device Manager
Status
Information
Features
Network
Job Manager
Device Selection
Support Links
Change the following settings.
5
OK
Cancel
SNMP Setting
Enable SNMPv1 : On Off
Access Rights : ReadOnly ReadWrite
Community Name : public
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 : 172.68.0.123
Delete
Add
* Successive IP addresses can be set by entering "Start Address-End Address."


http://172.21.139.75/pages/_infoadm.htm
RemoteUI <Information> : ;...
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 : 172.68.0.123

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.

PROTECT 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: - Depending on the printer model, **your LFP may not employ a default password**. Please set a password.

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

- 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.)

- For the iPF5100 / iPF510 / iPF610 / iPF605, use Remote UI to set a system administrator password. The LFP's operation panel does not include screens enabling passwords to be set or input.

NOTE

You can protect your LFP by making use of its password functionality. It is important that passwords are properly managed to ensure the security of your machine. Please note the following when managing your passwords.

- Change the default password.
- Periodically change your password.
- Avoid passwords that are easy to guess.
- Don't share your password with others.

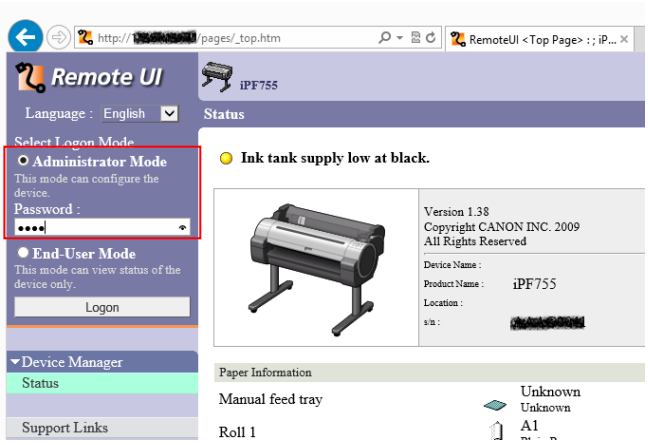
■ Password Setting Screens (imagePROGRAF Series)

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 input screen