Useful Tips for Reducing the Risk of Unauthorized Access for MFPs for Office (imageRUNNER ADVANCE/ Color imageRUNNER/imageRUNNER Series) and MFPs for Production Printing (imageRUNNER ADVANCE PRO/imagePRESS Series)

Important: **System administrators are advised to read this manual.**

Overview and Use of this Guide

Objectives

This guide provides additional information related to the Canon MFPs for Office (imageRUNNER ADVANCE/Color imageRUNNER/imageRUNNER Series) and MFPs for Production Printing (imageRUNNER ADVANCE PRO/imagePRESS 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 purchasing Canon products. This document is an outline of instruction manual for protecting your multifunction copier/printer (hereinafter referred to as MFP) for the office (imageRUNNER ADVANCE/Color imageRUNNER/imageRUNNER series) or for production printing (imageRUNNER ADVANCE PRO/imagePRESS series) from unauthorized access via external networks.
System administrators are advised to read through the document before use. For the imagePRESS Server/ColorPASS/imagePASS/imagePRESS CR Server, see "To Protect Your Printers From Unauthorized Access".

Preface

In recent years, a number of functions equipped with MFPs is increasing. In addition to conventional functions such as copying, faxing, and printing, many functions for users who access MFPs using several types of protocols via network are now available.
Canon MFPs are no exception, providing a variety of convenient functions such as the Remote UI function that uses HTTP protocol, and the file sharing function that uses SMB/WebDAV protocol.
This document describes some points to prevent unauthorized access from external networks when using Canon MFPs.

Key points for preventing unauthorized access from external networks

1. **Using Private IP Addresses**
2. **Restricting Communication with Firewalls**
3. **Protecting MFP Data with Passwords**
4. **Limiting Usage of the Remote UI**
5. **Setting SSL Encrypted Communication**

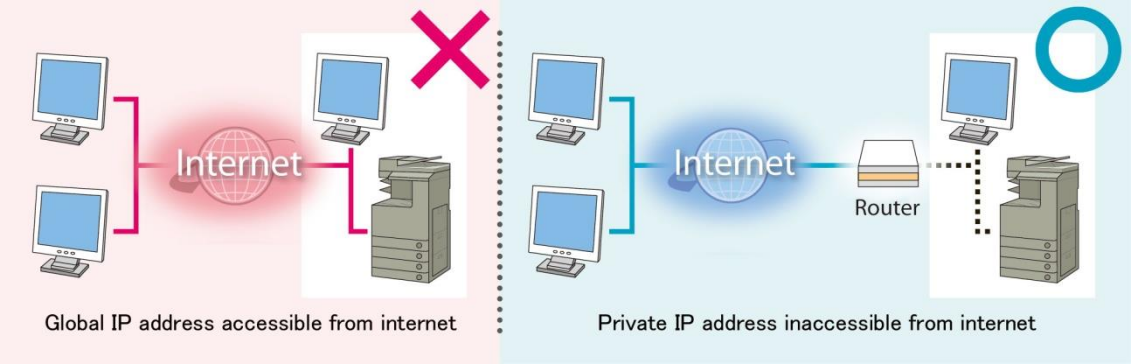
Using Private IP Addresses

An IP address is a numeric code assigned to a device on a network. There are two types of IP addresses: **Global IP Address**, which is used for the Internet connection, and **Private IP Address**, for local networks such as a company intranet. When an MFP is given a global IP address, it is accessible to anonymous users on the Internet. This raises the possibility of information leakage due to unauthorized access by third parties. On the other hand, access to an MFP with a private IP address is limited to authorized users on an internal network exclusive to one company or other LAN (local area network).

In principle, when you use an MFP, assign a private IP address. The private IP address has to be in one of the following ranges. Check that your MFP has a private IP address.

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 MFP is given a global IP address, the MFP is not likely to cause immediate information leakage, provided that an environment such as a firewall that blocks out access from other networks is constructed. When you want to set a global IP address on your MFP, consult with your network administrator in the company.

- Verifying IP Addresses for the imageRUNNER ADVANCE Series Machines and Some imagePRESS Series Machines

[Settings/Registration]

↓

[Preferences]

↓

[Network]

↓

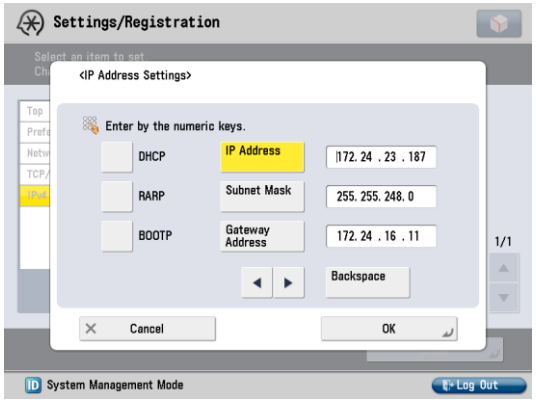
[TCP/IP Settings]

↓

[IPv4 Settings]

↓

[IP Address Settings]



✓ For information about how to verify IP addresses of your MFP, see user manuals provided with your machine.

- Verifying IP Addresses for the Color imageRUNNER/imageRUNNER/imagePRESS Series Machines

[Settings/Registration]

↓

[System Settings]

↓

[Network Settings]

↓

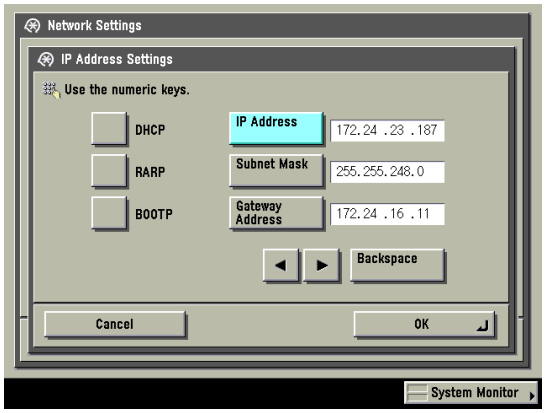
[TCP/IP Settings]

↓

[IPv4 Settings]

↓

[IP Address Settings]



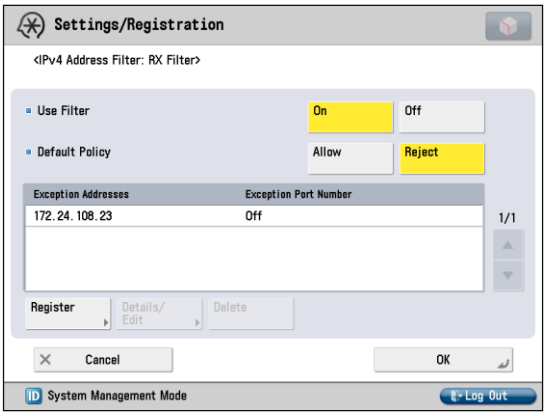
✓ For information about how to verify IP addresses of your MFP, see user manuals provided with your machine.

Restricting Communication with Firewalls

A firewall is a system that prevents access by outside networks, as well as attacks against and intrusions into the network of an organization. You can block access from outside networks that appears to be dangerous by using the firewall of Canon MFPs to restrict communication from specified outside IP addresses.

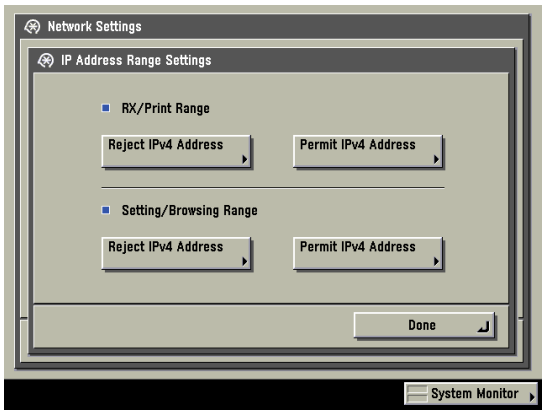
- Firewall Settings Screen of the imageRUNNER ADVANCE Series Machines and Some imagePRESS Series Machines

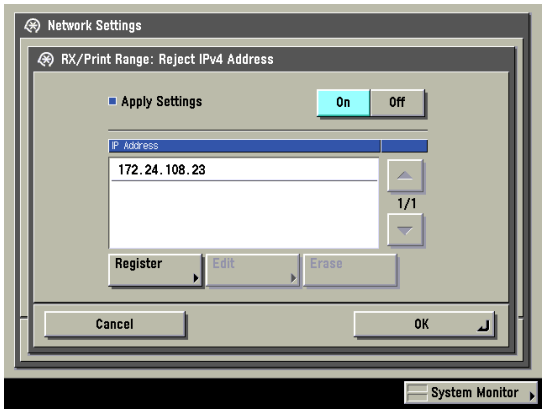
✓ For information about how to set the firewall settings, see user manuals provided with your machine.



- IP Address Range Settings Screen of the Color imageRUNNER/ imageRUNNER/imagePRESS Series Machines

✓ For information about how to set the IP address range settings, see user manuals provided with your machine.





Protecting MFP Data with Passwords

Even if your MFP is hacked, the possibility of information leakage can drastically be reduced by password protection. You can protect various data on your MFP with a password. This section provides just some examples, and you can set passwords on other functions and data files. Set a password as necessary.

✓ For information about how to set a password on a function, see user manuals provided with your machine.

✓ You can set a password from the Remote UI or from the control panel of the machine.

NOTE

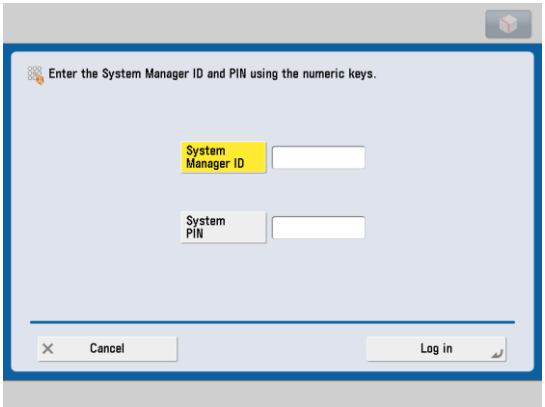
The Remote UI (User Interface) is preinstalled software in the machine that enables you to access the machine's functions by using a web browser. For example, the Remote UI enables you to access the machine to check machine status, execute jobs, and specify various settings. You can manage the machine from a computer connected to the network without having to perform operations on the machine itself. When you enter the machine's IP address into your web browser, the Remote UI's portal page is displayed on your computer screen.

✓ For information about how to use the Remote UI, see user manuals provided with your machine.

- Various Screens of the imageRUNNER ADVANCE Series Machines and Some imagePRESS Series Machines

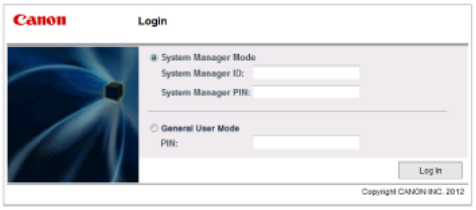
Control Panel of the Machine

- Password input screen for the System Manager



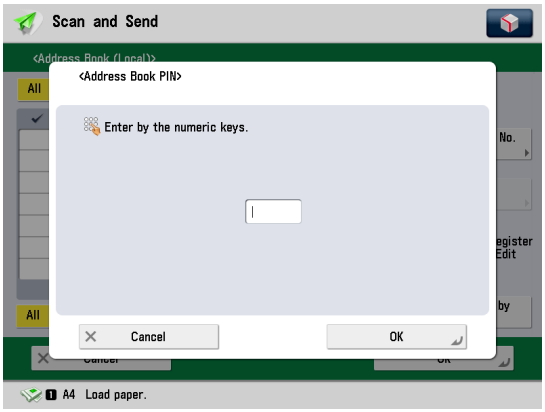
Remote UI

- Password input screen for the System Manager



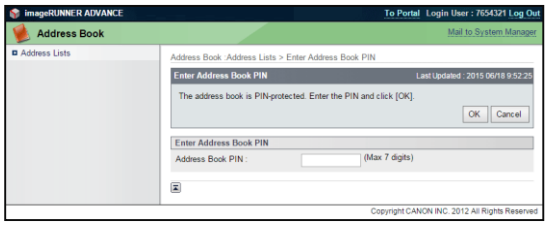
Control Panel of the Machine

- Password input screen to access Address Book



Remote UI

- Password input screen to access Address Book

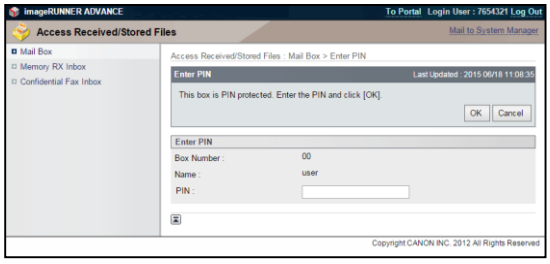


Control Panel of the Machine

- Password input screen to access inbox

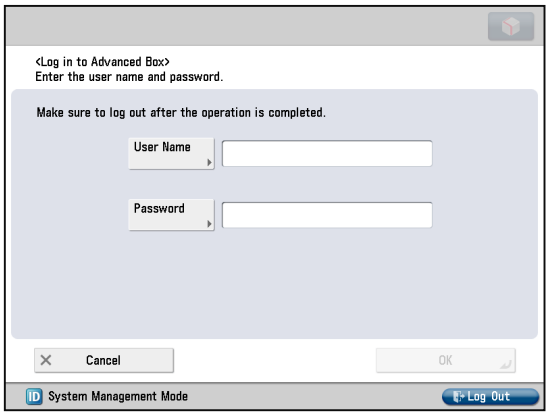
Remote UI

- Password input screen to access inbox



Control Panel of the Machine

- Password input screen to access Advanced Box



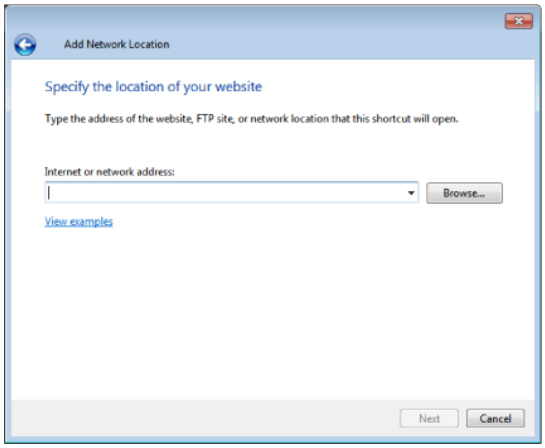
SMB

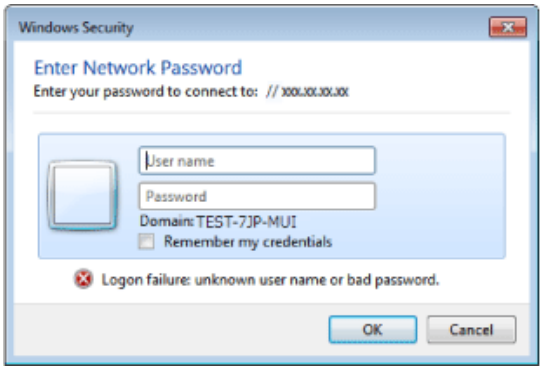
- Password input screen to access Advanced Box

When accessing the SMB server, enter the host name or IP address of the machine followed by "\share" or "\users", then "\folder name".

WebDav

- Password input screen to access Advanced Box





When accessing the WebDAV server, enter the URL in the following format:

http(s)://<IP address or host name of the machine>/<"share" or "users">/<folder name>

NOTE

Although MFPs are password protected, it is essential to manage passwords for security measures. Take the following points into consideration when managing passwords:

✓ Make sure to change the default password.

✓ Change the passwords regularly.

✓ Avoid passwords that others can easily guess.

✓ Do not let others know your password.

Limiting Usage of the Remote UI

The Remote UI now has a function that restricts usage of the Remote UI, to enhance its security.

✓ Several settings, such as changing the default PIN for system manager settings, are required to use the Remote UI.

✓ Access to the Remote UI by general users can be restricted. A PIN or password is required for both the administrator and general users.

- Remote UI On/Off Screen of the imageRUNNER ADVANCE Series Machines and Some imagePRESS Series Machines

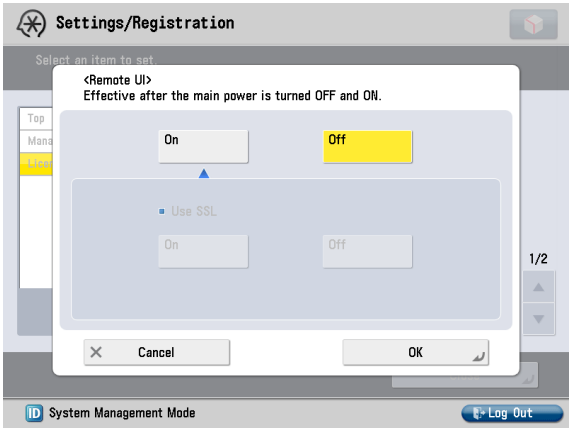
[Management Settings]

↓

[License/Others]

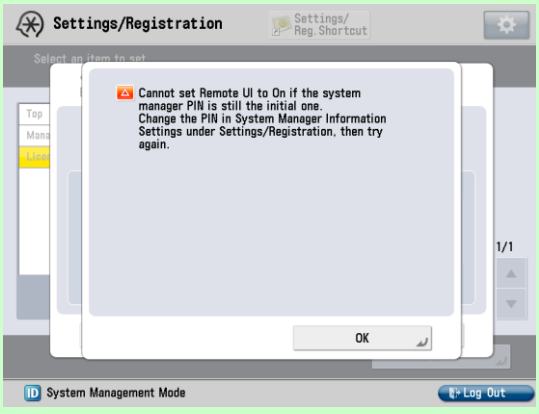
↓

[Remote UI On/Off]



NOTE

If the default PIN for system manager settings has not been changed, the following warning screen is displayed when changing settings:

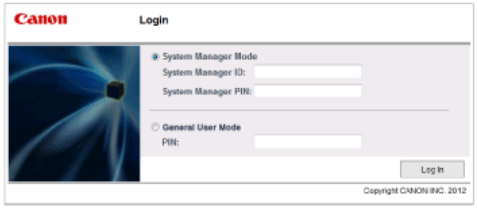


* The screen displayed may differ from the one above, depending on your machine.

- Remote UI Login Screen of the imageRUNNER ADVANCE Series Machines and Some imagePRESS Series Machines

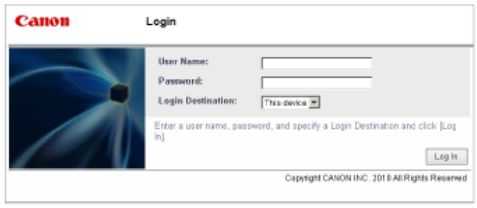
The login screen shown may differ from the screens below, depending on your machine or settings.

Login screen 1



The screen prompting the administrator to enter the System Manager ID and System PIN, or general users to enter their PIN is displayed when accessing the Remote UI.

Login screen 2



Whether you are an administrator or general user, the screen prompting you to enter a user name and password is displayed when accessing the Remote UI.

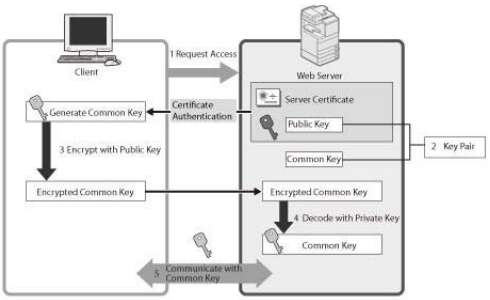
***Consult with your authorized Canon dealer for more information on using this function with your machine.**

Setting SSL Encrypted Communication

You can perform safe encrypted communication when the user is accessing your MFP via a Web browser by installing a server certificate to the machine. With SSL communication, a common key that can only be used by the user and the machine is generated using the server certificate and public key. Doing so will help prevent data interception and theft.

✓ For information about how to set SSL communication, see user manuals provided with your products.

The structure of SSL communication (right-hand figure)



1. When the user accesses the machine from their computer, the server certificate for SSL and the public key for the server are requested.
2. The certificate and the public key are sent to the user's computer from the machine.
3. Using the public key received from the server, encrypt the uniquely generated common key on the computer.
4. Send the encrypted common key to the machine.
5. Use the private key on the machine and decode the encrypted common key.
6. Now, the user's computer and the machine both possess the common key and can send/receive data using the common key.

- SSL Settings Screen of the imageRUNNER ADVANCE Series Machines and Some imagePRESS Series Machines

[Preferences]

↓

[Network]

↓

[TCP/IP Settings]

↓

[SSL Settings]

↓

[Key and Certificate]

↓

Default Key

(Pre-installed key pair and server certificate)

↓

[Set as the Default Key]