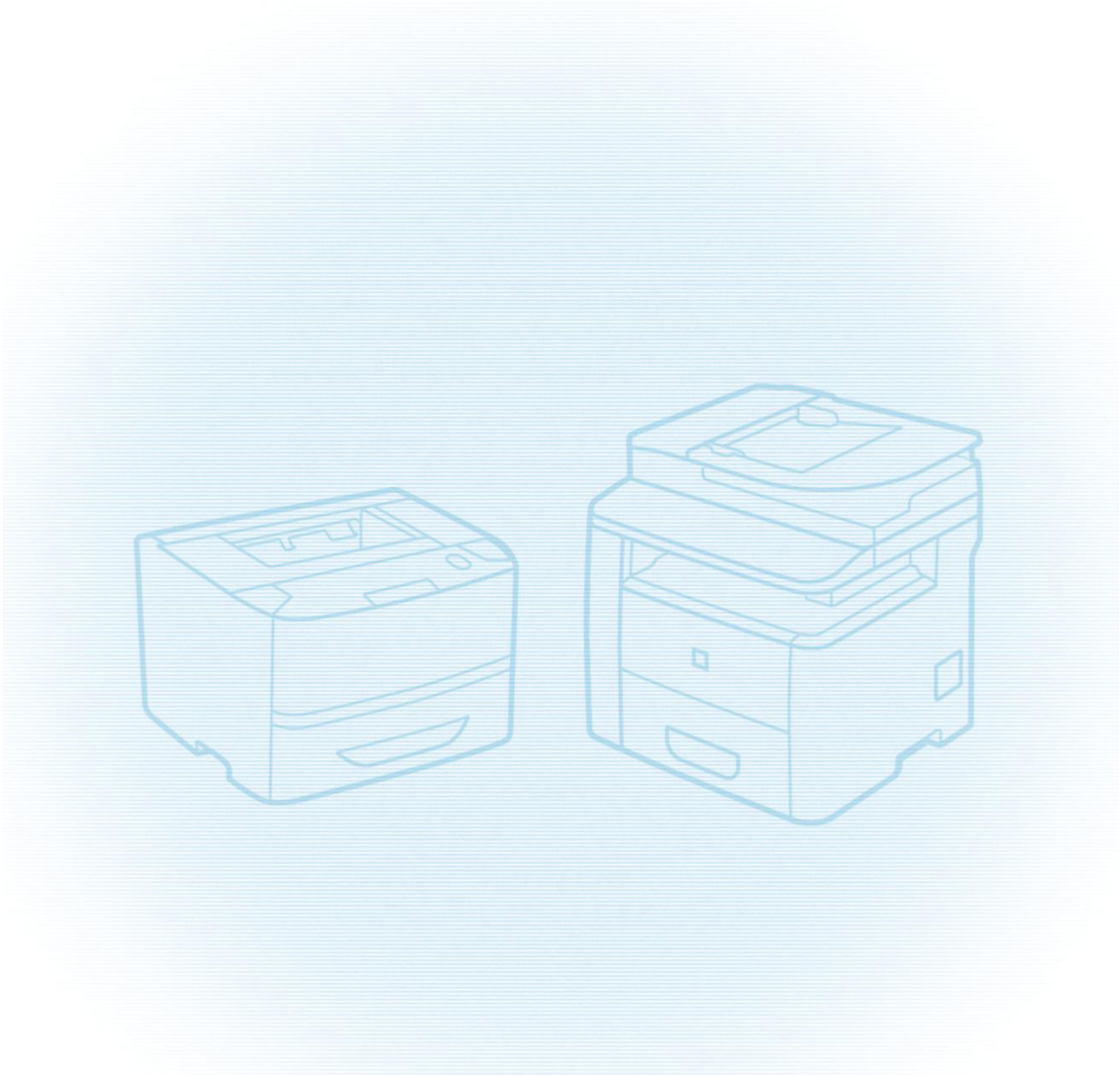
Useful Tips for Reducing the Risk of Unauthorized Access for Laser Beam Printers and Small-Office MFPs (LBP and MF series)

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



Overview and Use of this Guide

Objectives

This guide provides additional information related to the Canon Laser Beam Printers and Small-Office MFPs, 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 outlines how to protect laser-beam printers (hereinafter referred to as printers) and small-office multifunction printers (hereinafter referred to as MFPs) from being accessed by an unauthorized third-party on an external network. Printer and MFP users and system administrators are advised to read through this document before use.

Preface

In recent years, printers and MFPs are increasingly connected to a network, enabling such useful functions as printing and management through Remote UI, while MFPs also allow the sending of scanned data.

This document describes various methods to help prevent printers and MFPs connected to a network from being accessed by an unauthorized third party from an external network.

Additionally, this document describes how to set up the machine using Remote UI. Depending on the model of printer or MFP, as well as the functions incorporated in the machine, you may be able to adjust these settings from the device's operation panel. Setting procedures and illustrations described here are examples provided for reference and may differ from those of your machine. For more information, please refer to the user manual provided with your device.

Methods for preventing unauthorized access from external networks

1. **Use Private IP Addresses**
2. **Restrict communication by using firewalls**
3. **Protect MFP data with passwords**
4. **Set SSL Encrypted Communication**
5. **Note: Precautions when Using Remote UI**

NOTE

Remote UI (User Interface) is preinstalled software that enables users to access the machine's functions using a Web browser. For example, Remote UI enables users to access the machine to check its status, execute jobs, and specify various settings. The machine can also be managed from a computer connected to a network without having to operate the machine directly. Users can access the Remote UI's portal page from a computer screen by entering the device's IP address into a Web browser.

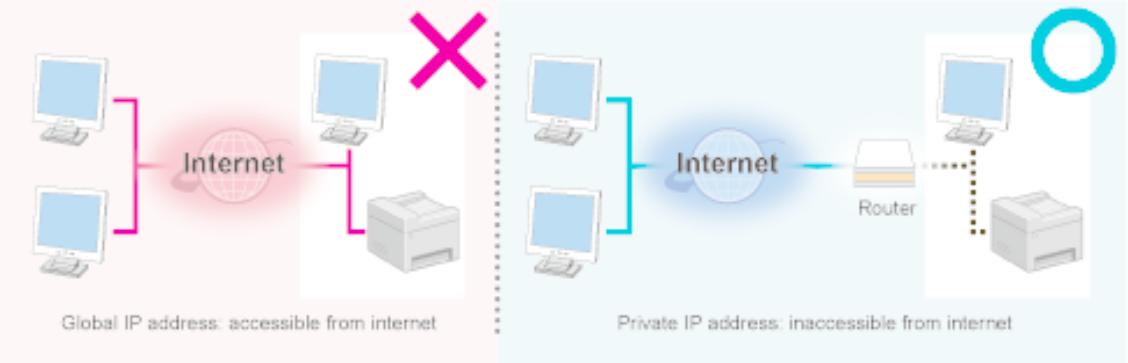
✓ For information about how to use Remote UI, please see the user manual provided with the machine.

Use Private IP Address

An IP address is a numeric code assigned to a device on a network. There are two types of IP addresses: **Global IP Addresses**, which are used for an Internet connection, and **Private IP Addresses**, which are used for local networks such as on a company intranet. When a printer or MFP is assigned a global IP address, the device becomes 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 a printer or MFP with a private IP address is limited to authorized users on an internal network exclusively used by a company or other LAN (local area network). In principle, when using a printer or MFP, we recommend that users employ a private IP address. The private IP address has to fall within one of the following ranges. Please check that your printer or 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 a printer or MFP is assigned a global IP address, users can limit the risk of access by an unauthorized third party through such means as establishing a firewall to prevent access from an external network. Please consult with a corporate network administrator when setting a global IP address for your printer or MFP.

- Verify IP address

Start Remote UI and login as an administrator

↓

[Settings/Registration]

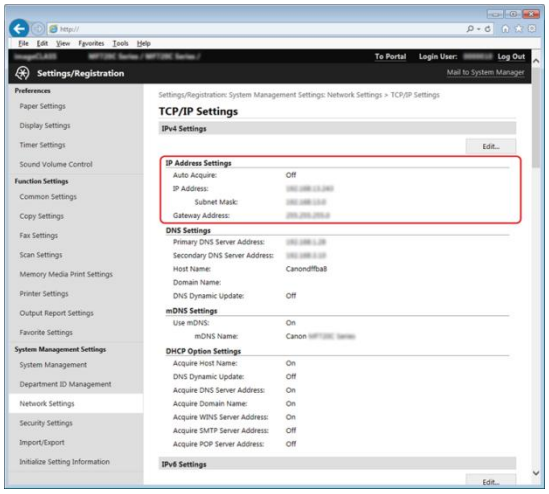
↓

[Network]

↓

[TCP/IP Settings]

✓ For information about how to verify the IP address of your printer or MFP, please see the user manual provided with the machine.

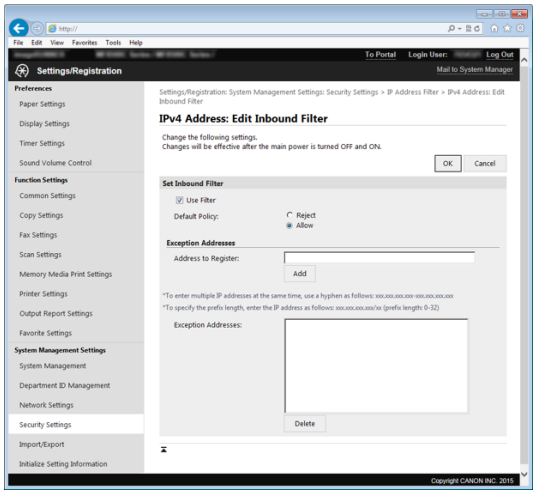


Restrict communication by using firewalls

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 employed in a Canon printer or MFP.

- Printer and MFP IP Address Filtering Screen

✓ For information about how to filter an IP address, please refer to the user manual provided with the machine.



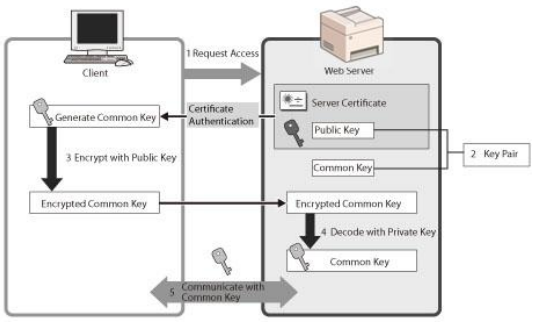
Set SSL Encrypted Communication

By installing a server certificate, users can ensure that communication with the printer or MFP is safe and encrypted when accessing the device via a Web browser. SSL communication creates a common key that can only be used by the user and the machine, and is generated using a server certificate and public key. Doing so will help prevent data interception and theft.

✓ Some models are not equipped with an SSL communication feature. We recommend that such models only be used in environments that cannot be accessed from an external network.

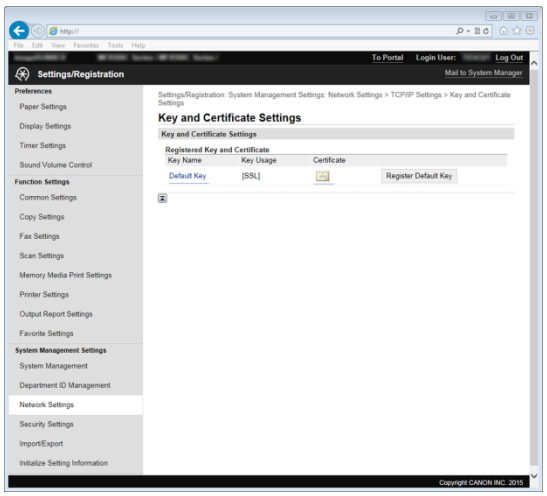
The structure of SSL communication (see figure on right)

1. When a user accesses a 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, a unique common key is encrypted on the computer.
4. The encrypted common key is sent to the machine.
5. The private key on the machine is used to decode the encrypted common key.
6. As a result, the user's computer and the machine both possess the common key and can send/receive data using the common key.



- SSL Settings Screen

✓ For information about how to set SSL communication, please see the user manual provided with your machine.↓



Protect MFP data with passwords

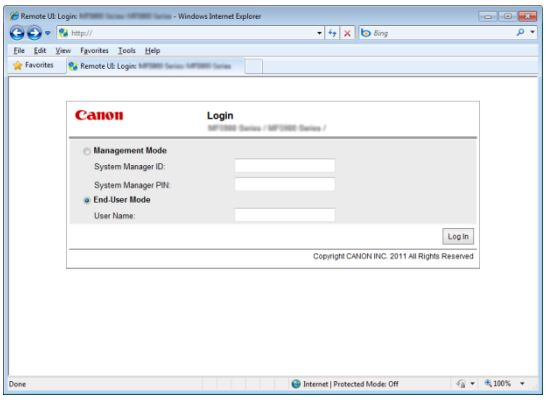
Even if your printer or MFP is hacked, the possibility of information leakage can be drastically reduced by password protection. Users can protect various types of data on a printer or MFP by using a password. This section provides examples for setting passwords for functions and data files. Please set a password when considered necessary.

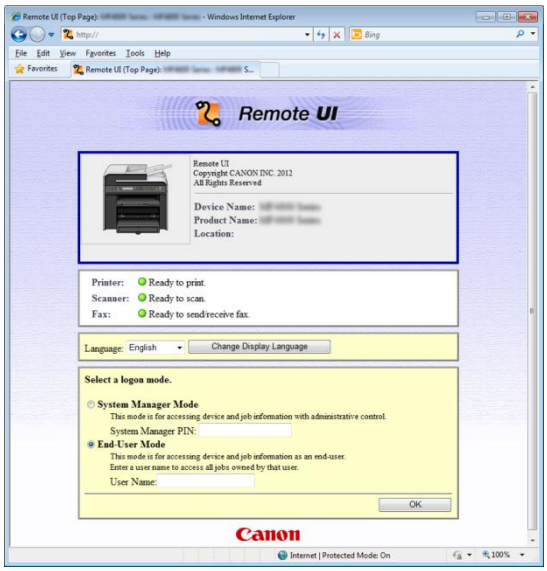
✓ For information about how to set a function password, please refer to the user manual provided with your machine.

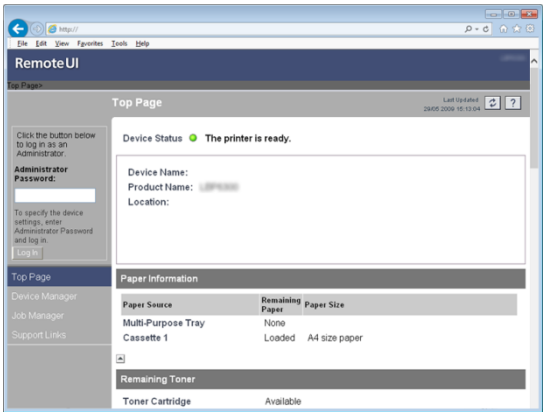
✓ Passwords can be set from Remote UI

- Various Screens

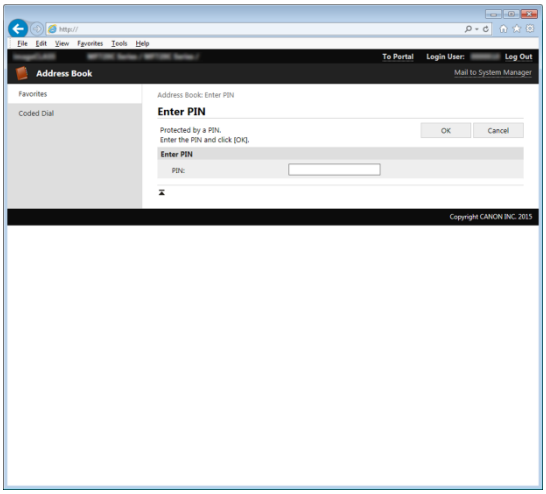
- Password input screen for a system manager

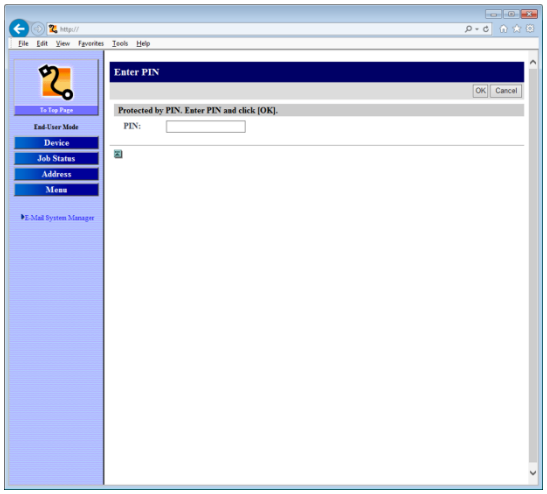






- Password input screen to access the address book





Note

- Precautions when Using Remote UI

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

Do not forget to close the web browser if you step away from the computer or after you finish changing settings.