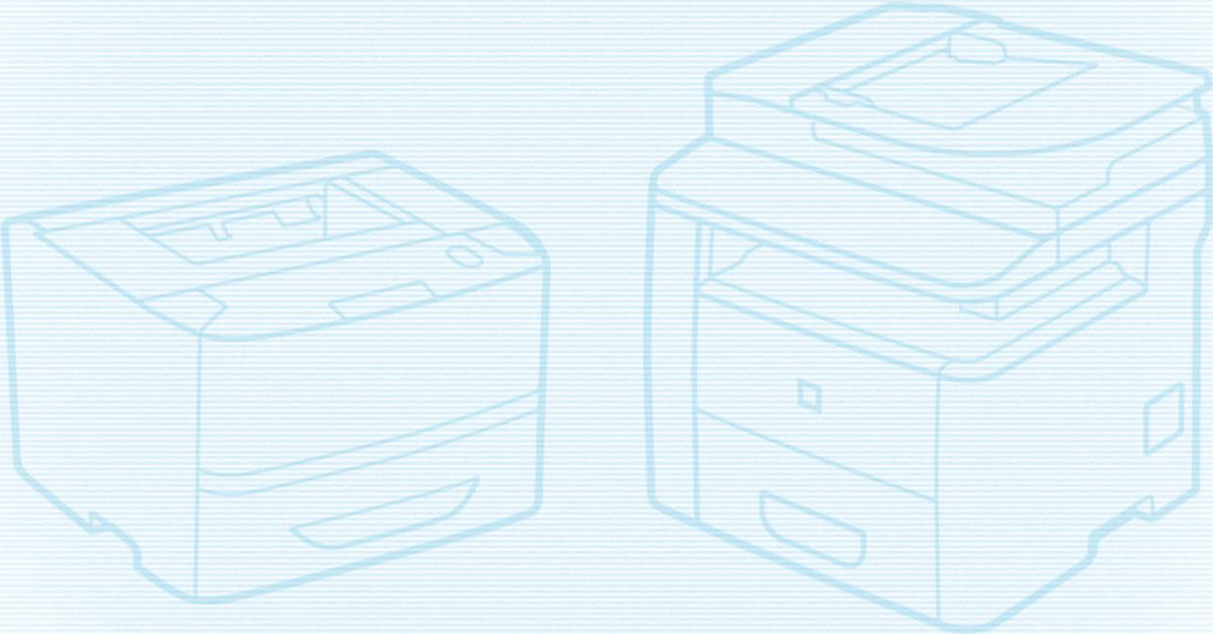
Useful Tips for Reducing the Risk of Unauthorized Access for LBP and Small Office MFPs (LBP and MF/X series)

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 LBP 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/MFPs have become able to connect to a network to provide various convenient functions. This document describes key points for preventing unauthorized access from outside when using a printer/MFP in a network environment.

Key points for preventing unauthorized access from external networks

1. **Using Private IP Addresses**
2. **Restricting Communication with Firewalls**
3. **Setting SSL (TLS) Encrypted Communication**
4. **Managing printer/MFP information with passwords**
5. **Updating the Firmware**
6. **Detecting Unauthorized Firmware Modifications**

Screenshots of the Remote UI are used in this document. You may also be able to configure some settings from the control panel of the machine, depending on the model of your machine.

Functions described in this document may not be supported, depending on the model of your machine. For details on the printer and MFP operations/settings required for each key point, see the user manual of your machine.

NOTE

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

Cautions Using the Remote UI:
Do not access other websites while the Remote UI is open in a Web browser. Also make sure to close the Web browser if you step away from your computer while changing settings with the Remote UI, or when you finish changing the settings.

Using Private IP Addresses

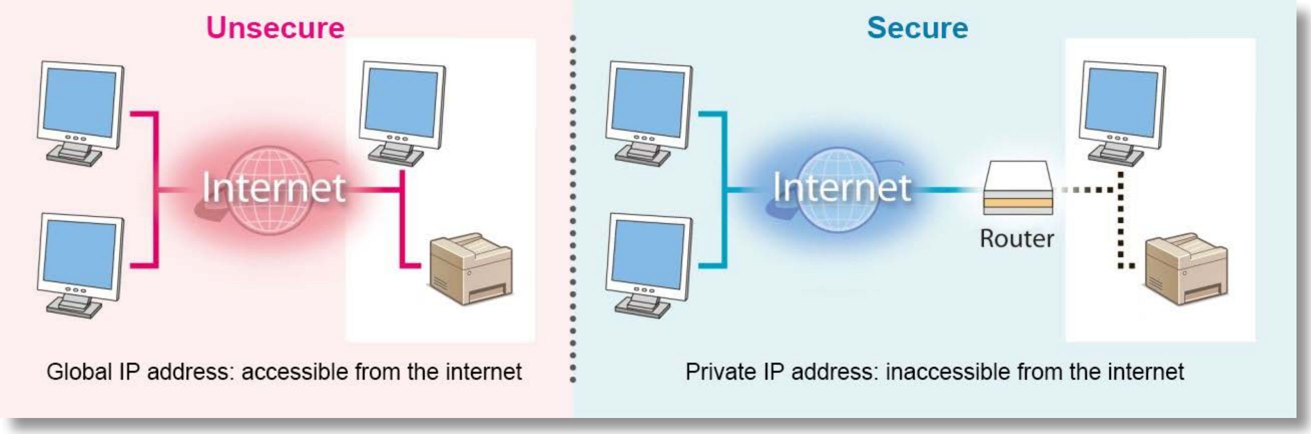
An IP address is a numeric code assigned to a device on a network. There are two types of IP addresses: "**Global IP Addresses**", which are used for an Internet connection, and "**Private IP Addresses**", which are used for local networks such as on a company intranet. When a printer/MFP is assigned a global IP address, it 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/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 you use a printer/MFP, assign a private IP address. The private IP address has to be in one of the following ranges.

Check that your printer/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



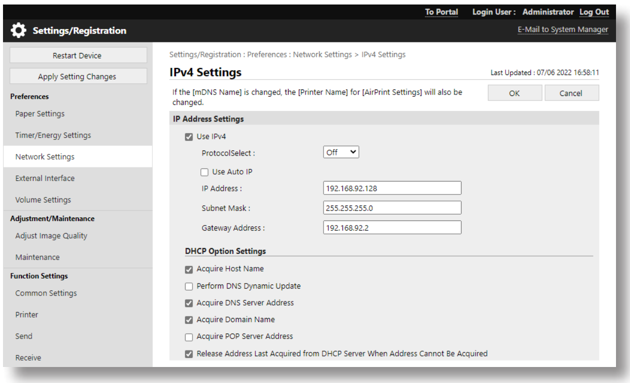
Global IP address: accessible from the internet

Private IP address: inaccessible from the internet

NOTE

Even if your printer/MFP is assigned a global IP address, you can limit the risk of unauthorized access through such means as establishing a firewall to prevent access from an external network. Consult with a corporate network administrator when setting a global IP address for your printer/MFP.

■ Example of Screen for Checking the IP Address



Settings/Registration : Preferences : Network Settings > IPv4 Settings

IPv4 Settings

Last Updated : 07/06 2022 16:58:11

If the [mDNS Name] is changed, the [Printer Name] for [AirPrint Settings] will also be changed.

IP Address Settings

☑ Use IPv4

ProtocolSelect : Off

☐ Use Auto IP

IP Address : 192.168.92.128

Subnet Mask : 255.255.255.0

Gateway Address : 192.168.92.2

DHCP Option Settings

☑ Acquire Host Name

☐ Perform DNS Dynamic Update

☑ Acquire DNS Server Address

☑ Acquire Domain Name

☐ Acquire POP Server Address

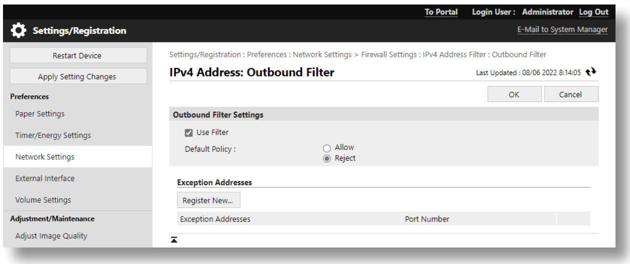
☑ Release Address Last Acquired from DHCP Server When Address Cannot Be Acquired

* The screens may differ depending on the model of your machine.

Restricting Communication with 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.

■ Example of Screen for Firewall Settings



Settings/Registration : Preferences : Network Settings > Firewall Settings : IPv4 Address Filter : Outbound Filter

IPv4 Address: Outbound Filter

Last Updated : 08/06 2022 8:14:05

Outbound Filter Settings

☑ Use Filter

Default Policy : ○ Allow ● Reject

Exception Addresses

Exception Addresses	Port Number

* The screens may differ depending on the model of your machine.

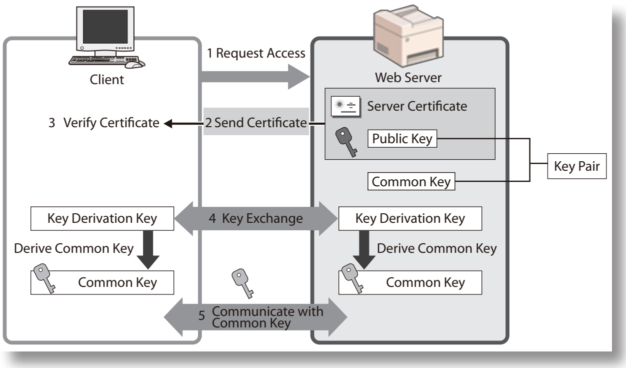
Setting SSL (TLS) Encrypted Communication

By installing a server certificate to a printer/MFP, you can ensure that communication with the printer/MFP is safe and encrypted by SSL (TLS) when accessing the printer/MFP via a Web browser. With SSL (TLS) communication, a common key that can only be used by the user and the printer/MFP is generated using the server certificate and public key. This helps prevent unauthorized access via external networks.

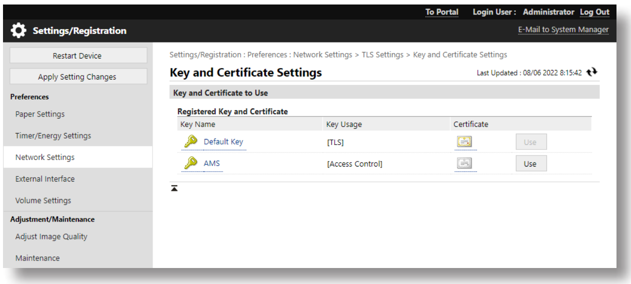
The structure of SSL (TLS) communication (right-hand figure)

1. When the user accesses the machine from their computer, the server certificate for SSL (TLS) is requested.
2. The certificate is sent to the user's computer from the machine.
3. The certificate received from the machine is verified on the user's computer.
4. The key is exchanged between the user's computer and the machine to establish a common key.
5. Now, the user's computer and the machine both possess the common key and can send/receive data using the common key.

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



■ Example of Screen for SSL (TLS) Settings



Settings/Registration : Preferences : Network Settings > TLS Settings > Key and Certificate Settings

Key and Certificate Settings

Last Updated : 08/06 2022 8:15:42

Key and Certificate to Use

Registered Key and Certificate

Key Name	Key Usage	Certificate	
Default Key	[TLS]		Use
AMS	[Access Control]		Use

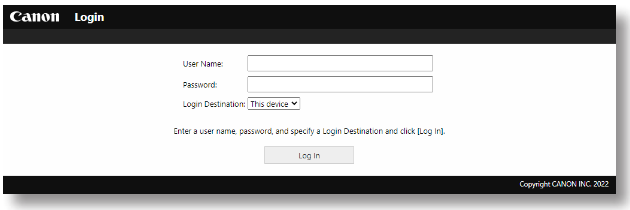
* The screens may differ depending on the model of your machine.

Managing printer/MFP information with passwords

Even if your printer/MFP is accessed by malicious third parties without authorization, the possibility of information leakage can drastically be reduced by password protection. You can protect various types of data on your printer/MFP with a password. This section provides some examples of the functions and information that can be protected by passwords. However, you can also set a password on other functions and information. Set a password on them as necessary.

* You can set a password from the Remote UI.

■ Example of Screen for Password Input



Login

User Name:

Password:

Login Destination: This device

Enter a user name, password, and specify a Login Destination and click [Log In].

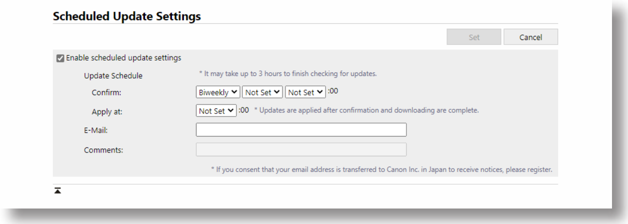
* The screens may differ depending on the model of your machine.

Updating the Firmware

The firmware is updated when functions are added or when problems with functions are fixed.

You can set the machine to periodically check for new firmware and automatically update the firmware.

■ Example of Screen for Firmware Update Settings



Scheduled Update Settings

☑ Enable scheduled update settings

Update Schedule * It may take up to 3 hours to finish checking for updates.

Confirm: Biweekly Not Set Not Set :00

Apply at: Not Set :00 * Updates are applied after confirmation and downloading are complete.

E-Mail:

Comments:

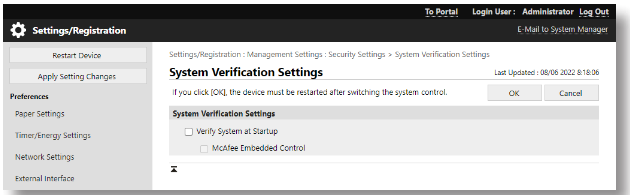
* If you consent that your email address is transferred to Canon Inc. in Japan to receive notices, please register.

* The screens may differ depending on the model of your machine.

Detecting Unauthorized Firmware Modifications

In order to further enhance the safety of firmware, you can set a printer/MFP to detect firmware modifications when the printer/MFP starts and while the printer/MFP is running.

■ Example of Screen for Firmware Modification Detection Settings



Settings/Registration : Management Settings : Security Settings > System Verification Settings

System Verification Settings

Last Updated : 08/06 2022 8:18:06

If you click [OK], the device must be restarted after switching the system control.

System Verification Settings

□ Verify System at Startup

□ McAfee Embedded Control

* The screens may differ depending on the model of your machine.

Canon