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.

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.

Key points for preventing unauthorized access from external networks

1. **Using the Device in an Environment with Access Control**
2. **Using Private IP Addresses**
3. **Restricting Communication with Firewalls**
4. **Secure the communication using security protocols**
5. **Managing printer/MFP information with passwords**
6. **Updating the Firmware**
7. **Detecting Unauthorized Firmware Modifications**
8. **Using the Audit Log**

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 the Device in an Environment with Access Control

Any direct access to your devices, such as printers, MFPs, connected computers, and Wi-Fi routers, increases the risk of information leakage and vulnerability to malicious attacks.

Locate and use your device in a lockable space where access is controlled, to prevent use by unspecified persons.

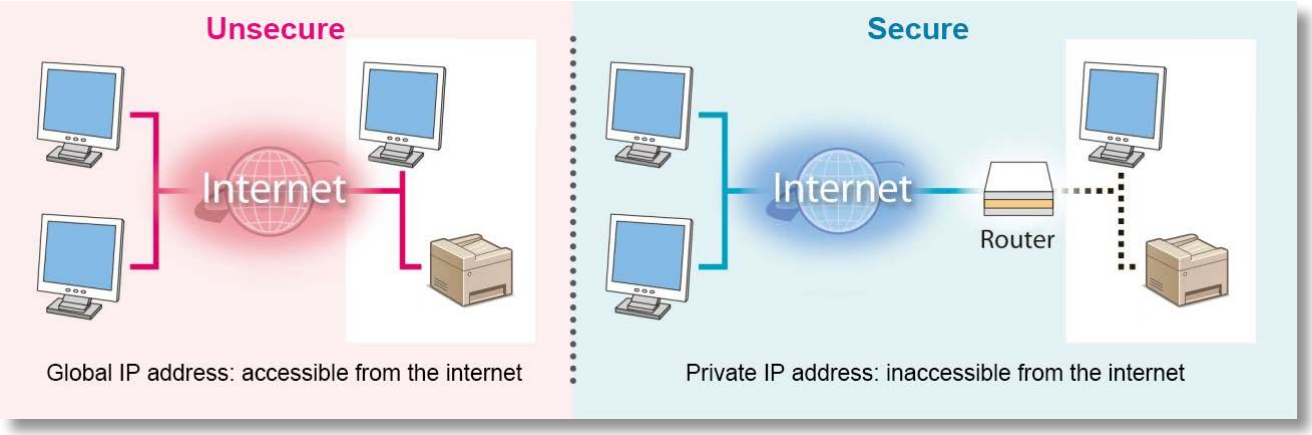
Using Private IP Addresses

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

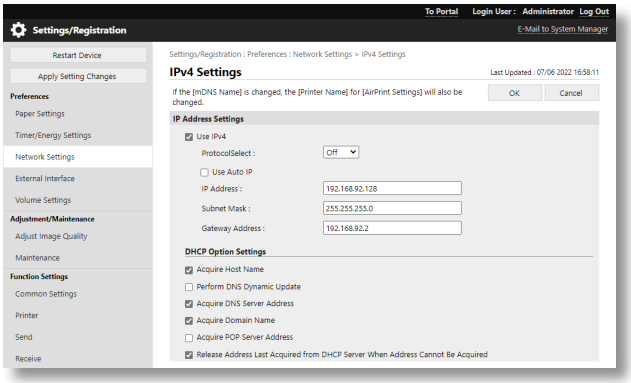
- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255



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



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

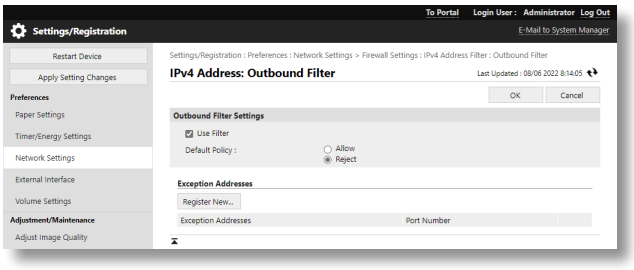
Restricting Communication with Firewalls

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.

Your Wi-Fi router has the same function. Be sure to set a password to your Wi-Fi router, and use caution when changing the setting.

Functions on Canon printers and MFPs also allow IP address filtering.

■ Example of Screen for Firewall Settings



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

Secure the communication using security protocols

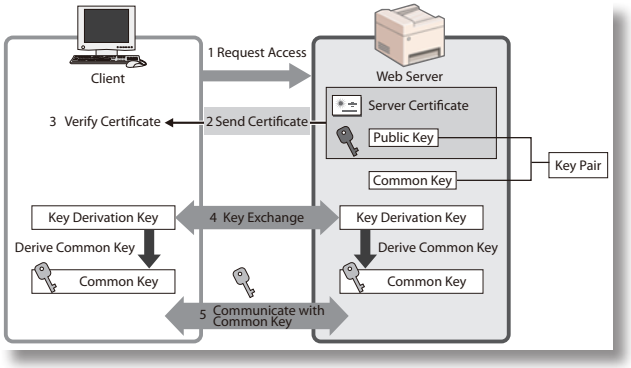
When connecting your printer or MFP to a network via a wireless LAN router (access point), be sure to connect using a safe security standard, either WPA2 or WPA3.
Set the security standard you are using on the wireless LAN router. For details on security standards your wireless LAN router supports and how to set them, refer to the manual for the wireless LAN router or inquire with the manufacturer.

By setting encrypted communication, you can Increase the security of communication with the MFP when accessing the MFP via a Web browser. Using a server certificate on your MFP enables TLS encrypted communication. With TLS communication, a common key that can only be used by the user and the MFP is generated using the server certificate and public key. Be sure to set TLS that is version 1.2 or higher.

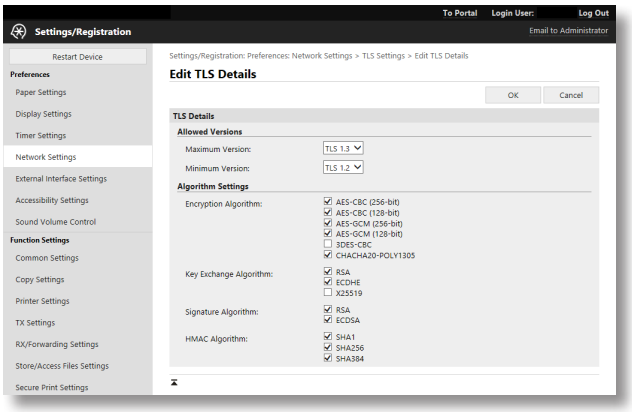
* Some models do not support TLS encrypted communication. For non-supported models, it is recommended to use them in an environment where connection from an external network is not possible.

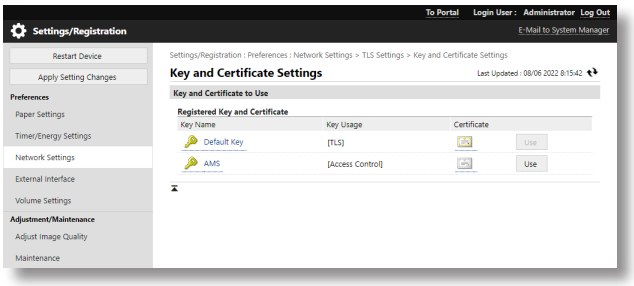
The structure of TLS communication (right-hand figure)

1. When the user accesses the machine from their computer, the server certificate for 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.



■ Example of Screen for TLS Settings





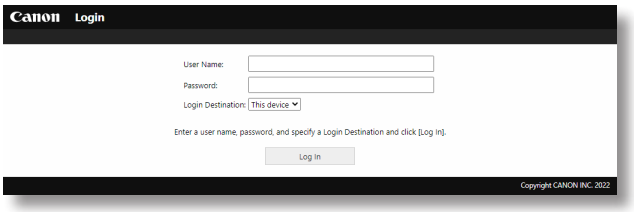
* The screens may differ depending on the model of your machine.

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



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

NOTE

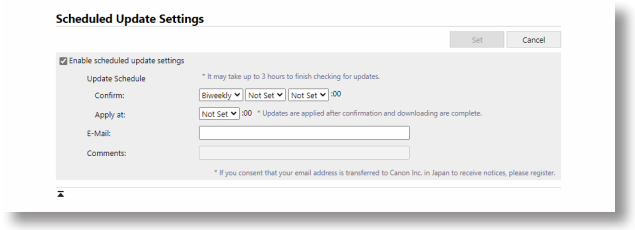
While MFPs have functionality for password protection, managing passwords is an important security measure.
Be sure to manage passwords referring to the following.

- Always change initial passwords
- Avoid setting passwords that are easy to guess by third parties
- Avoid carelessly revealing passwords to third parties

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

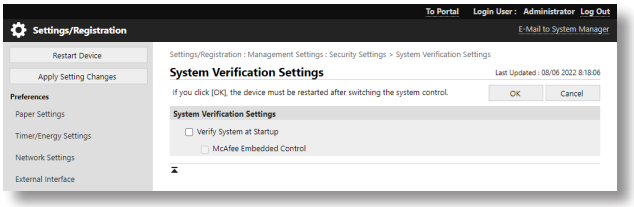


* The screens may differ depending on the model of your machine.

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



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

Using the Audit Log

You can use logs to check/analyze how the printer/MFP is used. Logs record information such as the operation date/time, user name, type of operation, type of function, and operation result.

* The log types and the log retrieval methods may differ depending on the model of your machine.

Log Type

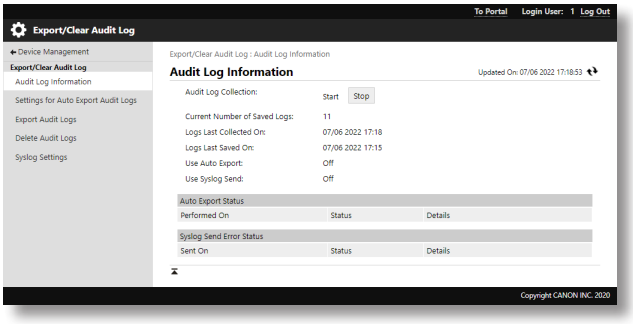
- User Authentication Log
- Job Log
- Transmission Log
- Advanced Box Save Log
- Mail Box Operation Log
- Mail Box Authentication Log
- Advanced Box Operation Log
- Machine Management Log
- Network Authentication Log
- Export/Import All Log
- Mail Box Backup Log
- Application/Software Management Screen Operation Log
- Security Policy Log
- Group Management Log
- System Maintenance Log
- Authenticated Print Log
- Setting Synchronization Log
- Log for Audit Log Management

Log Retrieval Method

- Automatic Exporting (Automatically Exporting to the Specified Folder of an SMB Server)
- Manual Exporting (Exporting from the Remote UI)
- Continuous Sending (Sending to a Syslog/SIEM Server)

■ Example of Screen for Log Settings

Remote UI



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

USRM3-1641-02