Useful Tips for Reducing the Risk of Unauthorized Access for Inkjet Printer
Business Inkjet Printer

IMPORTANT If you are connecting your printer(s) to the network, read this document.

Overview and Use of this Guide

Objectives

This guide provides additional information related to the Canon Inkjet Printer / Business Inkjet Printer, 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

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 inkjet printers and business inkjet printers (“printers”) against unauthorized access via the network. If you are using printers in the network environment or if you are an administrator, Canon recommends that you read through this document before use.

Introduction

These days, by connecting your printers to the network, you can enjoy various useful functions including printing via the network.
Introduced below are the points to protect your printers from unauthorized access when you use them in the network environment.

The setting procedures or illustrations given in this document are examples, and they may differ from the ones of your printer. For specific details, refer to the Instruction Manual of your printer.

Points to protect your printers against unauthorized access:

1. Use a private IP address.
2. Use a firewall or Wi-Fi router to limit communication.
3. Set the password to your printer.
4. Note: Precautions when Using Remote UI

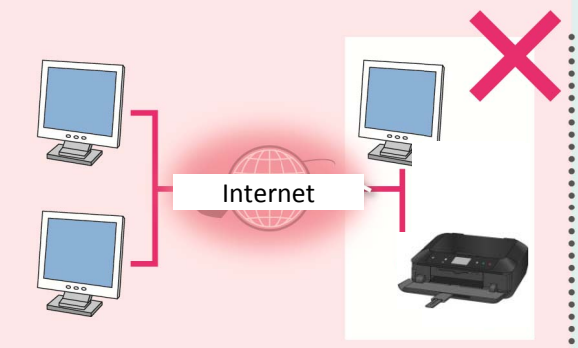
Using Private IP Address

An IP address is a number that is assigned to each device on the network. An IP address that is used to connect to the Internet is called “global IP address,” while an IP address within a local area network (LAN) is called “private IP address.” If a printer uses a global IP address, it can be accessed by the general public, which will increase risk of information leakage by unauthorized access from outside. If a printer uses a private IP address, then it can only be accessed by users on the same local area network (LAN) as the printer is connected to.

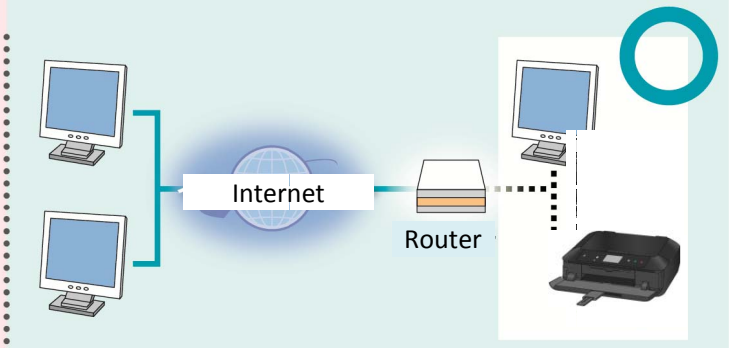
In general, Canon recommends that you use a private IP address for your printer. An IP address within the ranges listed below is a private IP address. Check if your printer’s IP address is a private one.

Range of the private IP address:

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



[Global IP Address] Accessible from outside



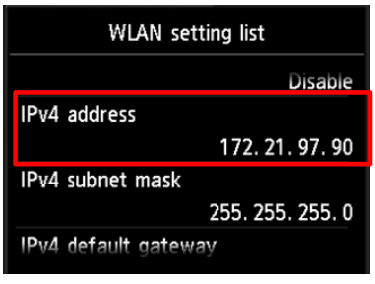
[Private IP Address] Accessible only within the local area network (LAN)

MEMO

Even if your printer uses a global IP address, you can reduce risk of unauthorized access by blocking access from outside using the firewall, etc.

How to check your printer’s IP address (Example)

Setup
↓
[Device settings]
↓
[LAN settings]
↓
[Confirm LAN settings]
↓
[WLAN setting list]



Note: For specific procedures for checking the IP address, refer to the Instruction Manual of your printer.

Using a Firewall or Wi-Fi Router to Limit Communication

Firewall is a system to protect against unauthorized access from outside and to prevent network attacks or hacking. By restricting communication with a certain external IP address, you can block suspicious access from outside.

Home-use Wi-Fi routers have similar functions. Be cautious when you change their settings.

Setting the Password to Your Printer

By utilizing the password functionality, you can protect various information of your printer and significantly reduce risk of information leakage in case of malicious access to the printer.

Note: - If a default password has been set, change it.

- **No password is set by default** depending on the printer model. Set the password.
- Some printer models do not have the password functionality.
- For specific procedures for setting the password, refer to the Instruction Manual of the printer.

MEMO

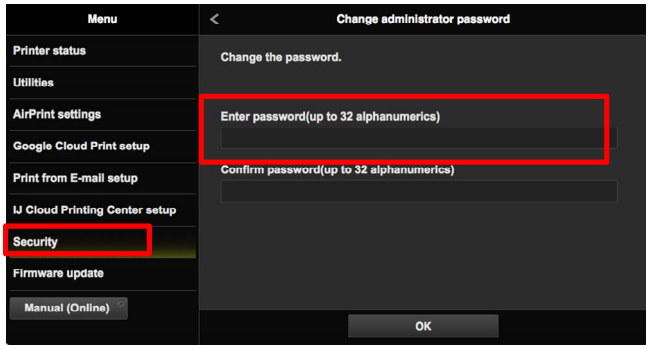
Printers have the password functionality for printer protection. What is important for your security is the proper use of the password. Keep the following in your mind in using the password:

- Always set the password.
- Change the password periodically.
- Avoid using an easy-to-guess password.
- DO NOT tell the password to others.

Screen Examples

Remote UI

The screen to set the password you will see at login to the Remote UI:



MEMO

Remote UI (User Interface) is the software that lets you access to the printer from a web browser in hand. You can check and change various printer settings using Remote UI without coming to the printer. When you enter the printer IP address or host name in the web browser, you will see the portal page of Remote UI.

Note: For details of Remote UI operation, refer to the Instruction Manual of the printer.

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.

Revision history:

January 1, 2023. The UI displays have been updated.