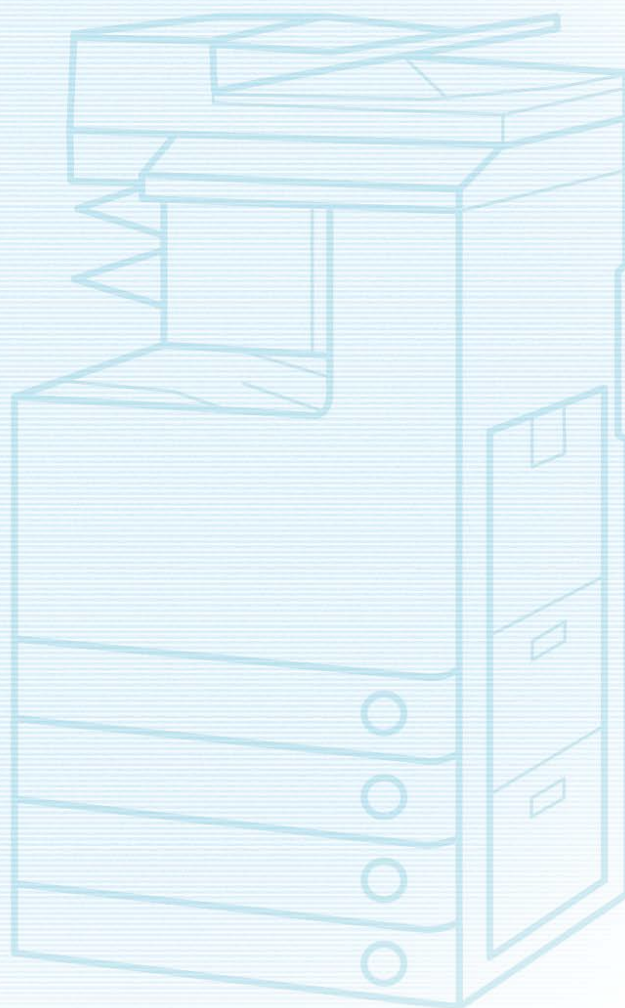




Useful Tips for Reducing the Risk of Unauthorized Access for MFPs for Office (imageFORCE / imageRUNNER ADVANCE DX/ imageRUNNER ADVANCE/imageRUNNER Series) and MFPs for Production Printing (imagePRESS/imagePRESS Lite Series)

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 (imageFORCE/imageRUNNER ADVANCE DX/imageRUNNER ADVANCE/imageRUNNER Series) and MFPs for Production Printing (imagePRESS/imagePRESS Lite 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 (imageFORCE/imageRUNNER ADVANCE DX/imageRUNNER ADVANCE/imageRUNNER series) or for production printing (imagePRESS/imagePRESS Lite 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 key points for preventing unauthorized access from external networks when using Canon MFPs.

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

Key points for preventing unauthorized access from external networks

1. Using MFP in an Environment with Access Control
2. Using Private IP Addresses
3. Restricting Communication with Firewalls
4. Securing the Communication Using Security Protocols
5. Managing MFP Information with Passwords
6. Limiting Usage of the Remote UI
7. Updating the Firmware
8. Detecting Unauthorized Firmware Modifications
9. Using the Audit Log
10. Managing MFPs According to a Security Policy

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 MFP in an Environment with Access Control

The risk of information leaks or malicious attacks increases when MFPs, destination computers, or wireless LAN routers are accessed directly.

Make sure to install and use such devices in a locked room where access control is implemented, so that the devices cannot be accessed by the general public.

Using Private IP Addresses

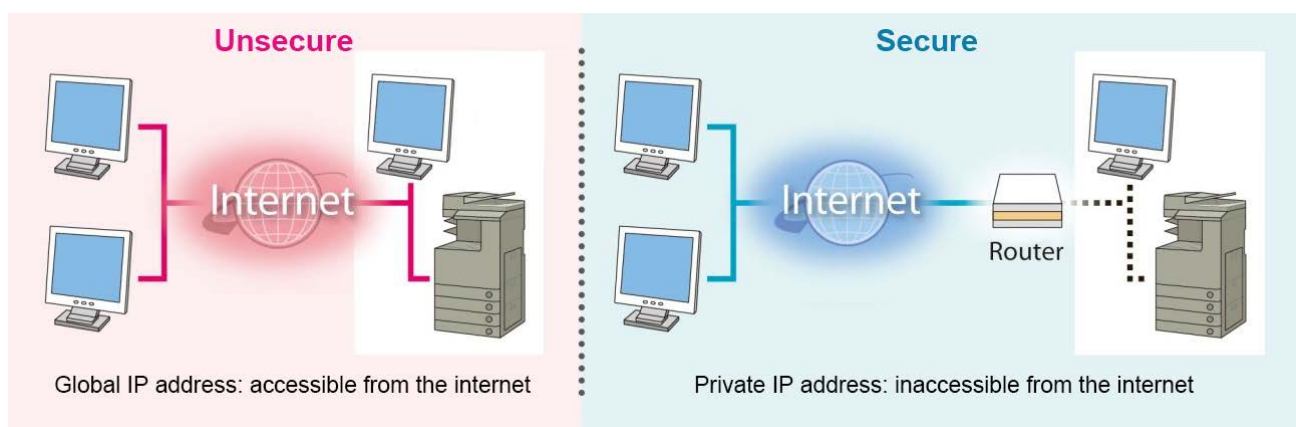
An IP address is a numeric code assigned to a device on a network. There are two types of IP addresses:

"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 an 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 an 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 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

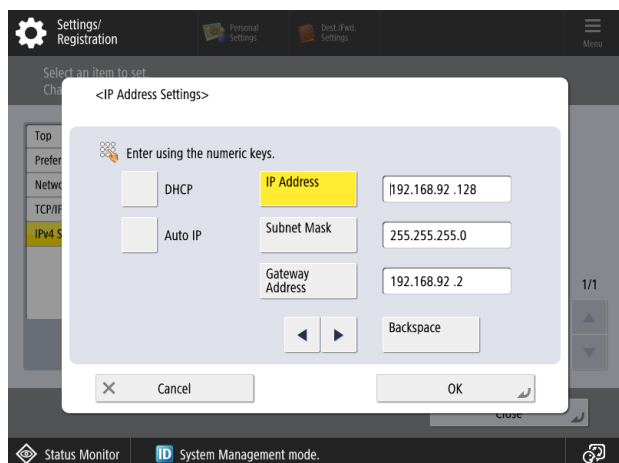


NOTE

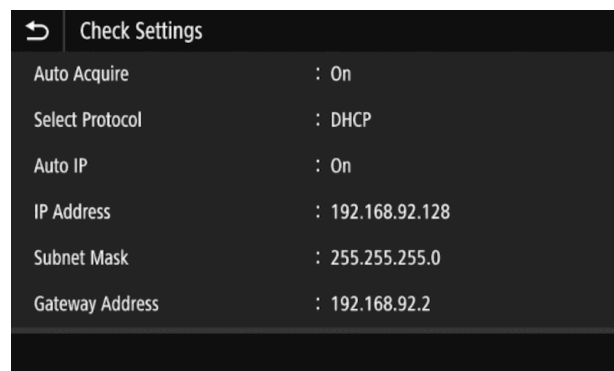
Even if your MFP is assigned a global IP address, you can limit the risk of unauthorized access through such means as establishing a firewall to prevent access from an external network. Consult with a corporate network administrator when setting a global IP address for your MFP.

■ Example of Screen for Checking the IP Address

Control Panel of the Machine



Control Panel of the Machine



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

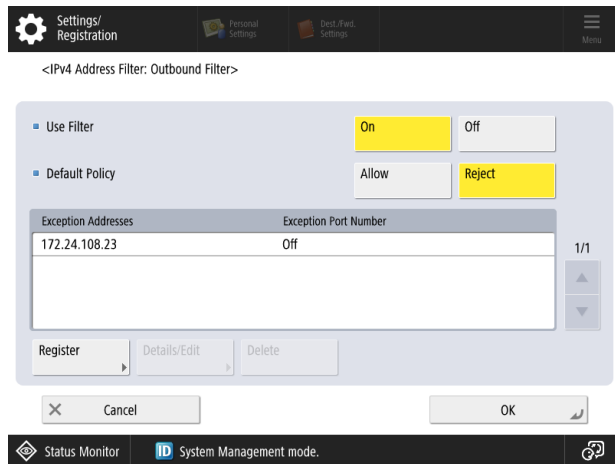
Restricting Communication with Firewalls

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 wireless LAN router also has a similar function. Make sure to set a password on your wireless LAN router, and be careful when changing the settings. IP addresses can also be filtered using functions employed in a Canon MFP.

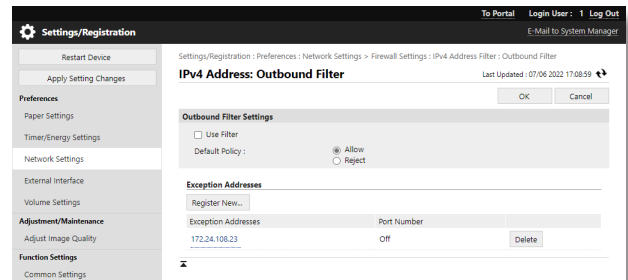
■ Example of Screen for Firewall Settings

Control Panel of the Machine



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

Remote UI



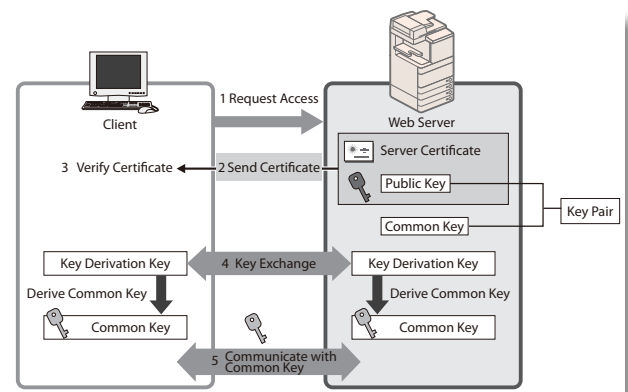
Securing the Communication Using Security Protocols

When connecting an MFP to a network via a wireless LAN router (access point), use a security protocol such as WPA2 or WPA3. The security protocol to use is configured in the wireless LAN router. For information on the security standards supported by the wireless LAN router you are using and how to configure them, see the manual of the wireless LAN router or contact the manufacturer.

Another effective method for improving security when users access an MFP via a browser is to enable encrypted communication. By installing a server certificate to the MFP, encrypted communication can be performed with TLS. TLS communication uses a server certificate and public key to generate a common key that can only be used by the user and the MFP. Set the TLS version to 1.2 or later.

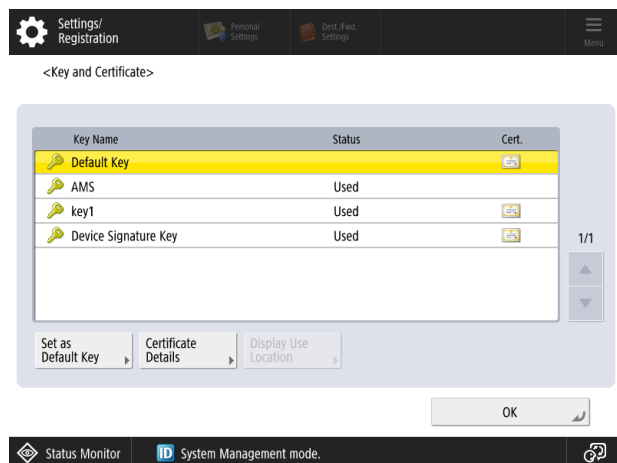
The structure of TLS communication (right-hand figure)

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.

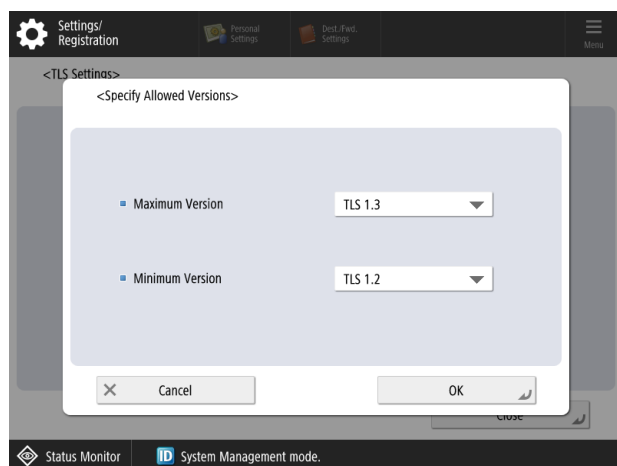
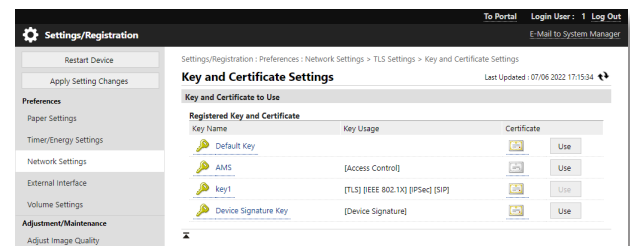


■ Example of Screen for TLS Settings

Control Panel of the Machine



Remote UI



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

NOTE

It is recommended that [Communication Operational Policy] is enabled in the security policy settings in order to enhance security.

* For information about [Communication Operational Policy], see the user manuals of your machine.

Managing MFP Information with Passwords

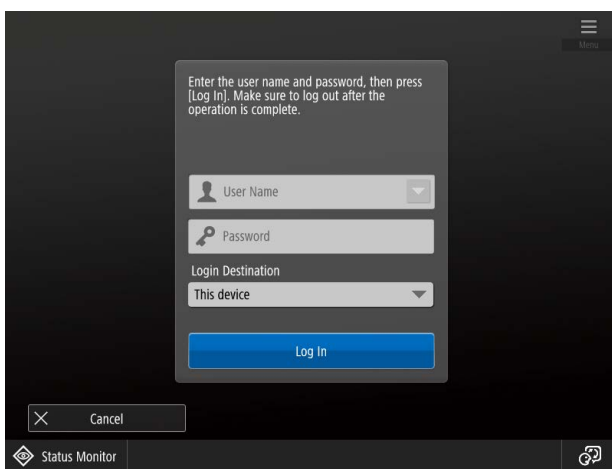
Even if your MFP is accessed by malicious third parties without authorization, the possibility of information leakage can drastically be reduced by password protection. You can protect various types of data on your MFP with a password. This section provides some examples of the functions and information 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 control panel of the machine or from the Remote UI.

■ Example of Screen for Password Input

Control Panel of the Machine

Password input screen for user login

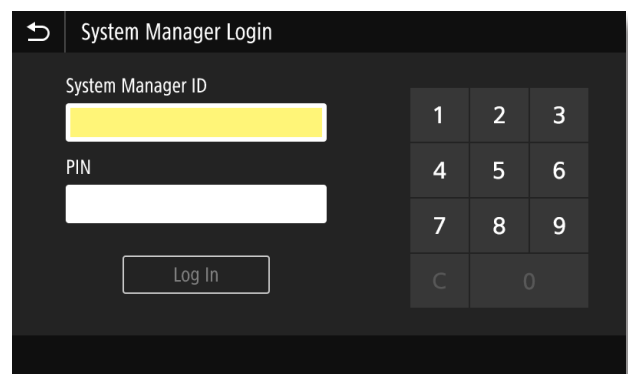


The screenshot shows a dark-themed control panel interface. At the top, a message reads: "Enter the user name and password, then press [Log In]. Make sure to log out after the operation is complete." Below this, there are three input fields: "User Name" with a user icon, "Password" with a key icon, and "Login Destination" with a dropdown menu currently set to "This device". A blue "Log In" button is at the bottom of the input area. At the very bottom of the screen, there is a "Cancel" button with an 'X' icon and a "Status Monitor" icon.

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

Control Panel of the Machine

Password input screen for the System Manager



The screenshot shows a dark-themed control panel interface titled "System Manager Login". It features a "System Manager ID" field with a yellow highlight and a "PIN" field. To the right of these fields is a numeric keypad with buttons for digits 1-9, 0, and a "C" (clear) button. A "Log In" button is positioned below the PIN field.

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.
- Avoid passwords that others can easily guess.
- Do not let others know your password.

Limiting Usage of the Remote UI

The Remote UI has a function that restricts usage of the Remote UI.

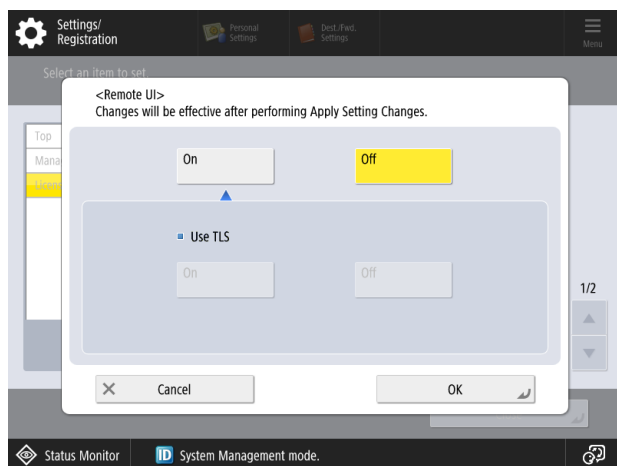
- Several settings, such as changing the default PIN for system manager settings, are required to use the Remote UI.

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

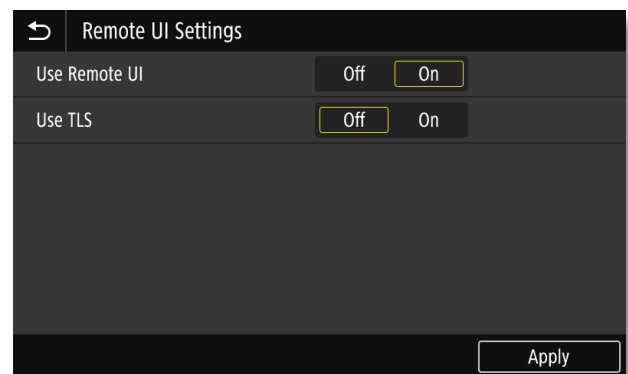
You can also use two-factor authentication, which requires a one-time password to be entered in addition to a password.

■ Example of Screen for Enabling/Disabling the Remote UI

Control Panel of the Machine



Control Panel of the Machine

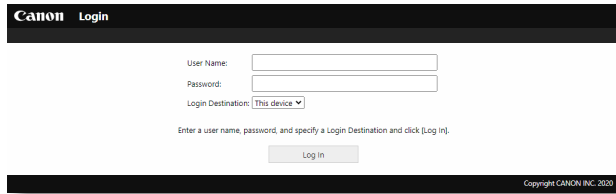


* The screens may differ depending on the model of your machine.

■ Example of Screen for Remote UI Login Screen

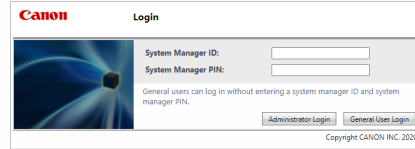
The login screen shown may differ from the screens below, depending on your machine or settings.

Login screen 1

A screenshot of a Canon login screen. At the top, it says "Canon Login". Below this, there are input fields for "User Name:", "Password:", and "Login Destination:" with a dropdown menu currently showing "This device". Below the input fields, there is a small instruction: "Enter a user name, password, and specify a Login Destination and click [Log In].". At the bottom, there is a "Log In" button. The footer says "Copyright CANON INC. 2020".

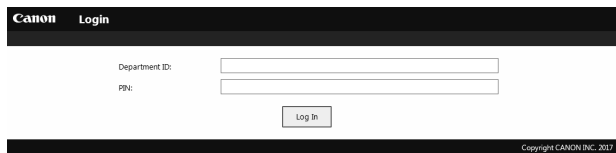
Whether you are an administrator or general user, the screen prompts you to enter a user name and password.

Login screen 2

A screenshot of a Canon login screen. At the top, it says "Canon Login". Below this, there is a graphic of a blue sphere with a black cube. To the right of the graphic, there are input fields for "System Manager ID:" and "System Manager PIN:". Below these, there is a small instruction: "General users can log in without entering a system manager ID and system manager PIN.". At the bottom, there are two buttons: "Administrator Login" and "General User Login". The footer says "Copyright CANON INC. 2020".

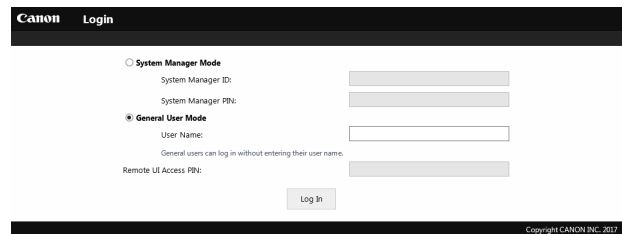
The screen prompts the administrator to enter the System Manager ID and System PIN, or general users to enter their PIN.

Login screen 3

A screenshot of a Canon login screen. At the top, it says "Canon Login". Below this, there are input fields for "Department ID:" and "PIN:". Below the input fields, there is a "Log In" button. The footer says "Copyright CANON INC. 2017".

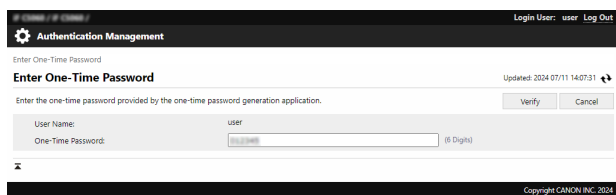
When Department ID Management is set, the screen prompts you to enter the Department ID/PIN.

Login screen 4

A screenshot of a Canon login screen. At the top, it says "Canon Login". Below this, there are two radio buttons: "System Manager Mode" and "General User Mode". The "General User Mode" is selected. Below the radio buttons, there are input fields for "System Manager ID:", "System Manager PIN:", "User Name:", and "Remote UI Access PIN:". Below the input fields, there is a "Log In" button. The footer says "Copyright CANON INC. 2017".

When Department ID Management is not set, the screen prompts the administrator to enter the System Manager ID and System PIN, or general users to enter their PIN .

Login screen 5

A screenshot of a Canon login screen. At the top, it says "Authentication Management". Below this, there is a section titled "Enter One-Time Password". Below this, there is a small instruction: "Enter the one-time password provided by the one-time password generation application.". Below the instruction, there are input fields for "User Name:" (with the value "user") and "One-Time Password:". Below the input fields, there are "Verify" and "Cancel" buttons. The footer says "Copyright CANON INC. 2024".

If two-factor authentication is set, you will be requested to enter a one-time password after entering the user name and password.

Updating the Firmware

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

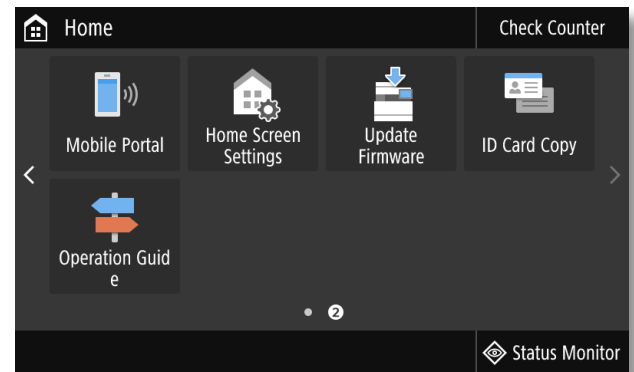
You can set the machine to periodically check for new firmware and automatically update the firmware.

■ Example of Screen for Firmware Update Settings

Control Panel of the Machine

The screenshot shows the 'Settings/Registration' screen with a 'Menu' icon in the top right. The title is '<Scheduled Update>'. There are two main sections: 'Scheduled Update Settings' and 'Update Schedule'. In the 'Scheduled Update Settings' section, there are two radio buttons: 'On' (selected) and 'Off' (highlighted in yellow). A note next to the 'Off' button states: 'Auto Update will be turned Off until all scheduled deliveries are sent.' The 'Update Schedule' section has a note: 'It may take up to 3 hours to finish checking for updates.' It includes a 'Confirm' dropdown set to 'Biweekly', a 'Set Day' dropdown, and a time field set to ':00'. Below this is an 'Apply at' field set to ':00' with a note: 'Updates are applied after confirmation and downloading are complete.' There are also fields for 'E-Mail' and 'Comments'. At the bottom, there is a disclaimer: 'If you consent that your email address is transferred to Canon Inc. in Japan to receive notices, please register.' and two buttons: 'Cancel' and 'OK'.

Control Panel of the Machine



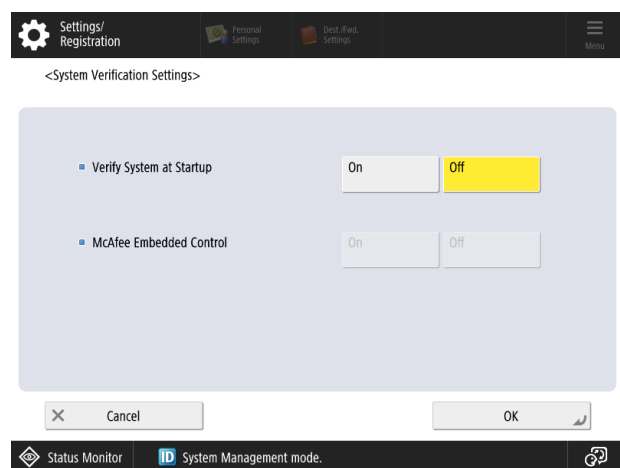
* The screens may differ depending on the model of your machine.

Detecting Unauthorized Firmware Modifications

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

■ Example of Screen for Firmware Modification Detection Settings

Control Panel of the Machine



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

Using the Audit Log

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

Log Type

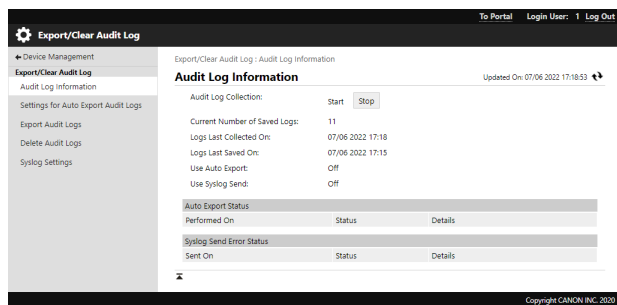
- User Authentication Log
- Job Log
- Transmission Log
- Advanced Box Save Log
- Mail Box Operation Log
- Mail Box Authentication Log
- Advanced Box Operation Log
- Machine Management Log
- Network Authentication Log
- Export/Import All Log
- Mail Box Backup Log
- Application/Software Management Screen 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.

Managing MFPs According to a Security Policy

Security policies including a basic policy and security measure standards for information security are defined by several organizations. Information devices, such as computers and MFPs, are expected to be operated under these policies.

Security Policy Settings

[Interface]

- **Wireless Connection Policy**
Prohibits wireless connections to prevent unspecified large amounts of access.
- **USB Policy**
Prohibits USB connections to prevent unauthorized connections and the retrieval of data.

[Authentication]

- **Authentication Operational Policy**
Ensures user authentication to avoid unauthorized operations by unregistered users.
- **Password Operational Policy**
Strictly limits the password operation method.
- **Password Settings Policy**
Makes passwords used for user authentication difficult to be guessed by third parties by setting a required level of complexity and an expiration period.
- **Lockout Policy**
Prevents users from logging in for a certain period of time when the login operation fails a certain number of consecutive times due to an incorrect password.

[Key/Certificate]

Protects important data by preventing weak encryption from being used and encrypting user passwords and keys inside specified hardware.

The machine enables the comprehensive management of multiple settings regarding a security policy, and setting changes can be limited to people in charge of information security.

[Network]

- **Communication Operational Policy**
Enables more secure communication by requiring signatures and certificates to be verified.
- **Port Usage Policy**
Prevents external infiltration by closing unused ports.

[Log]

Enables periodic auditing by requiring logs to be recorded.

[Job]

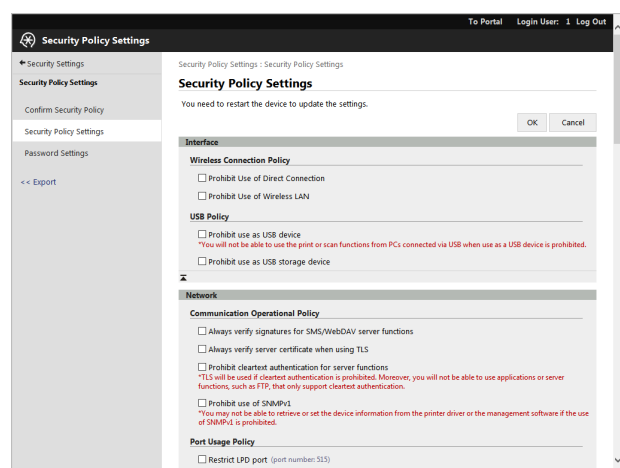
- **Printing Policy**
Prevents information leaks due to printing.
- **Sending/Receiving Policy**
Restricts destination operations when sending and the method for processing received data.

[Storage]

Prevents information leaks by deleting unnecessary data on the hard disk.

■ Example of Screen for Security Policy Settings

Remote UI



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

