Useful Tips for Reducing the Risk of Unauthorized Access for Fiery Controllers: imagePRESS Server/ ColorPASS/ imagePASS

IMPORTANT To administrators: Please read this document.

Overview and Use of this Guide

Objectives

This guide provides additional information related to the Canon Fiery Controllers: imagePRESS Server/ ColorPASS/ imagePASS, 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 using Canon products.
This document describes an example of measures to prevent unauthorized access to Fiery Controllers: imagePRESS Server/ ColorPASS/ imagePASS from the outside. Please read this document before using the products.

Introduction

Canon imagePRESS Server/ ColorPASS/ imagePASS products realize not only processing of a variety of data, but various convenient functions including Network Scanning function and sending print data using Hot Folder. In order for you to use these functions at ease and safely, the following describes points to be noted to prevent unauthorized access from the outside.

Points to be noted to prevent unauthorized access from the outside

1. **Use Private IP address**
2. **Restrict communication with firewalls**
3. **Configure Windows system password ***
4. **Configure Windows update ***
5. **Install Antivirus protection ***
6. **Manage Fiery Password**
7. **Configure IP filtering**

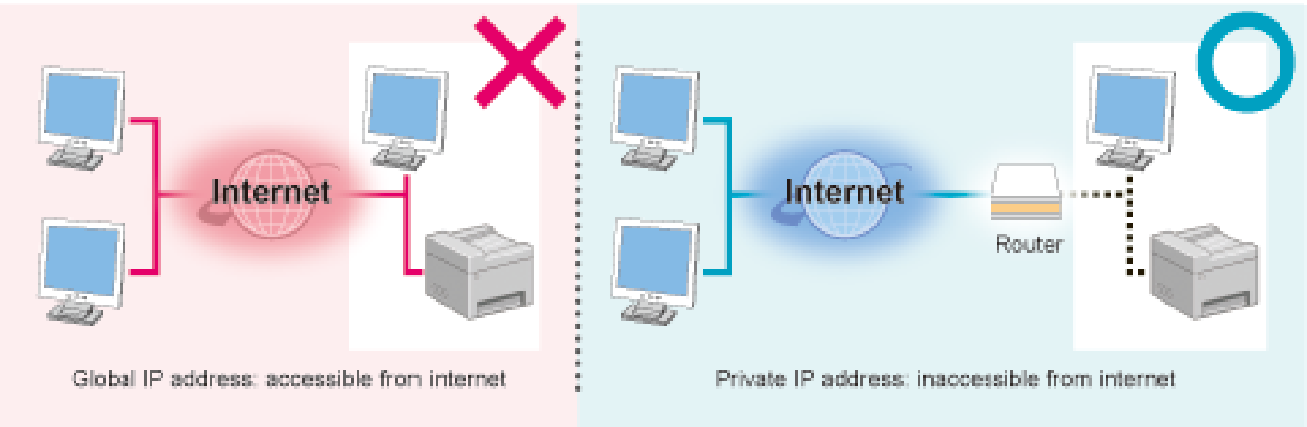
Note: An asterisk (*) indicates that a section only is applicable to a Windows-based server only.

1. Use Private IP address

An IP address is a numeric code assigned to a device on the network. There are two types of IP addresses: **Global IP Address**, which is used for the Internet connection, and **Private IP Address**, for local networks such as a company intranet. When a Fiery Controller is given a global IP address, it is 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 the Fiery Controller with a private IP address is limited to authorized users on an internal network exclusive to one company or other LAN (local area network).
In principle, when you use the Fiery Controller, assign a private IP address. The private IP address has to be in one of the following ranges. Check that your Fiery Controller has a private IP address.

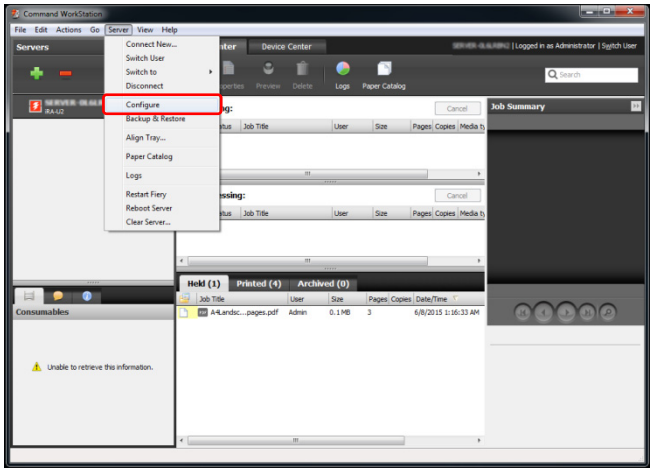
Private IP address ranges:

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

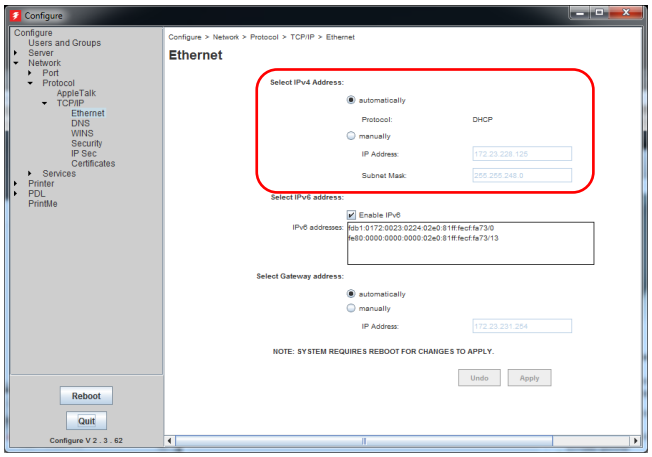


■ Steps to configure IP address

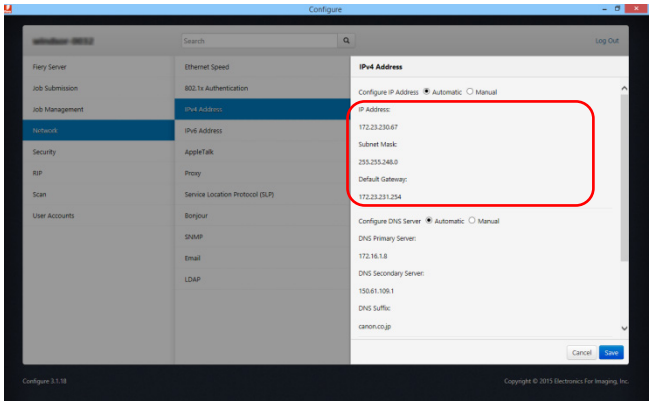
From Command WorkStation, under "Server," select "Configure."



<When using Configure v2.x>
Select "Network" > "Protocol" > "TCP/IP" > "Ethernet."



<When using Configure v3.x>
Select "Network" > "IPv4 Address."



2. Restrict communication with firewalls

A firewall is a system that prevents access by outside networks, and attacks and intrusions to the local network. You can block access from outside network that appears to be dangerous by restricting communication in your network environment from specified outside IP addresses. Configuring a password for each user account ensures the network security in an environment you use. You can also filter IP addresses with functions provided by Fiery controllers.

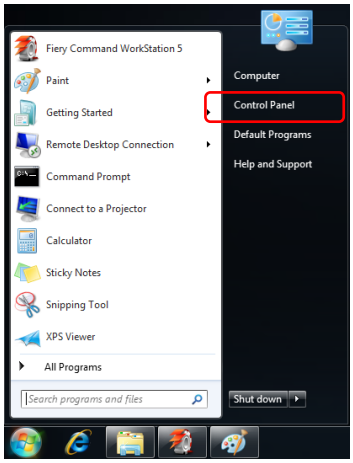
3. Configure Windows system password (Windows-based server only)

Configuring a password for each user account ensures the network security in an environment you use.

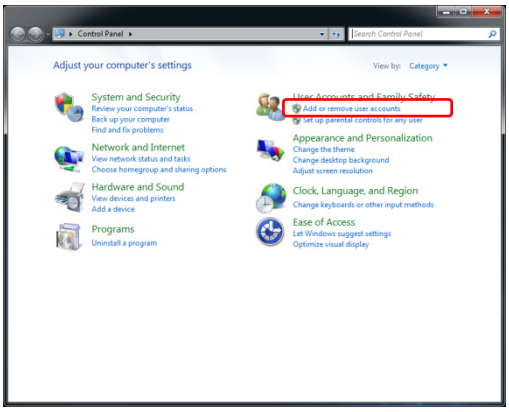
■ Steps to configure

*Connect a monitor/ keyboard/ mouse directly to Fiery Controller for operation.
*The following describes the steps to be performed for Canon imagePASS-U1. The screen may be different, depending on the model.

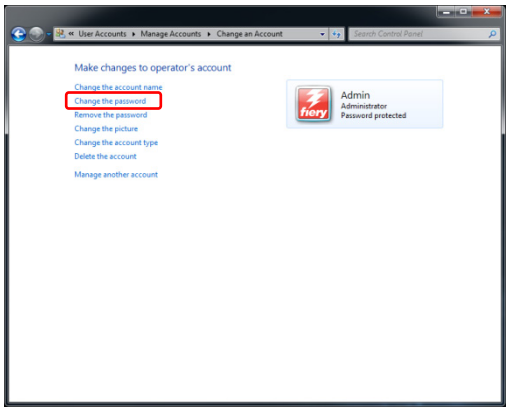
From the "Start" menu, select "Control Panel."



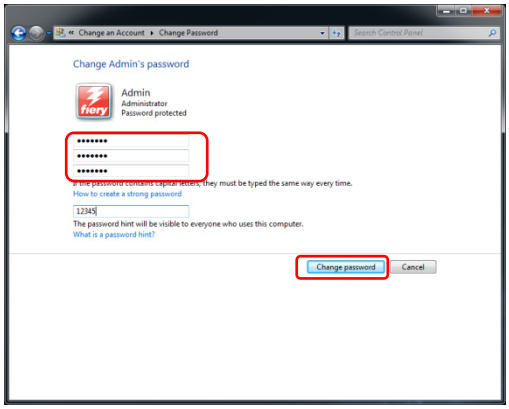
Select "Add or remove user accounts."



Select an account to which you want to make a change, and click "Change the password."



Enter a password, and click "Change Password."



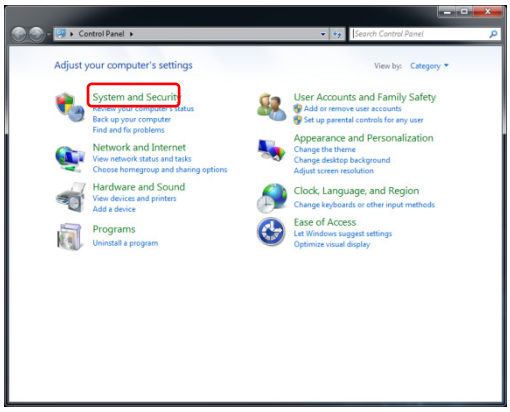
4. Configure Windows Update (Windows-based server only)

If the Windows Operating System of your Fiery controller is Windows 7 FES (For Embedded System) or later, configure and use Automatic Updates features in Windows to notify when important updates are available for your Fiery controller.

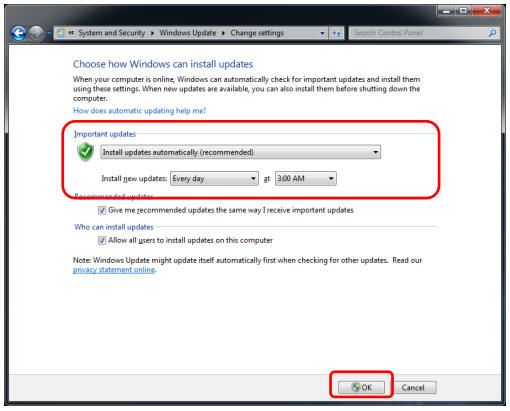
■ Steps to configure

* Connect a monitor/ keyboard/ mouse directly to Fiery Controller for operation.
* The following describes the steps to be performed for Canon imagePASS-U1. The screen may be different, depending on the model.

From the "Start" menu, select "Control Panel" and then "System and Security."



Select "Windows Update" and then "Change settings." Choose your Windows Update settings. Once you made your choice, click OK button to confirm the changes.



5. Install Antivirus protection (Windows-based server only)

To protect against viruses, scan the Fiery controller periodically with antivirus software. Make sure that you start the antivirus software only when the Fiery controller is Idle and not receiving jobs. This prevents errors that may result if the antivirus software acts while Fiery controller attempts to process a job. Use antivirus software to scan files sent to the Fiery controller outside the usual print scenarios, including files copied to the Fiery controller from removable media or a shared network directory. Configure and use Automatic Updates features in Windows to notify when important updates are available for your Fiery controller.

Note: Contact your authorized service/support center for antivirus applications supported for Fiery controllers.

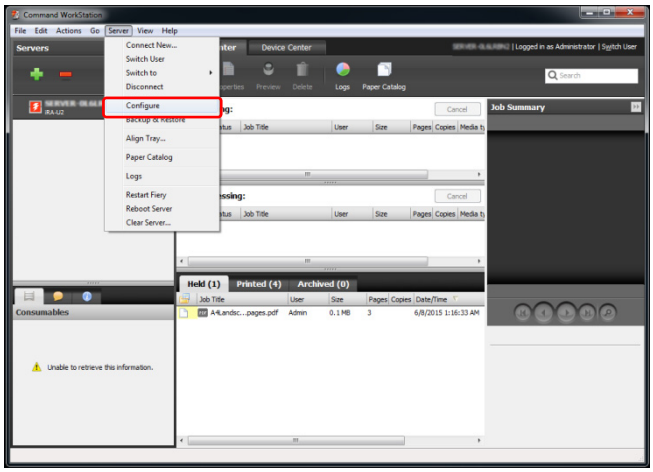
6. Manage Fiery Password

When you create a user in Configure in User Accounts, you can set a password for the user. Set passwords for the Administrator (default user in the Administrators group) and Operator (default user in the Operators group) in Configure in Security. This prevents unauthorized access. You can also set a password for the Administrator during initial setup with the Fiery Setup Wizard.

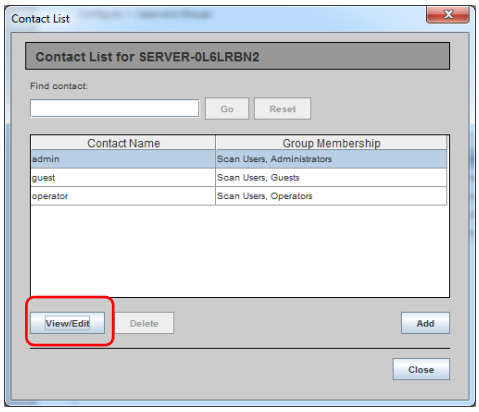
We strongly recommend that you change passwords periodically to protect the Fiery controller from unauthorized changes. Choose a password that is longer than 15 characters and includes some symbols rather than only alphanumeric characters.

■ How to change password

From Command WorkStation, under "Server," select "Configure."

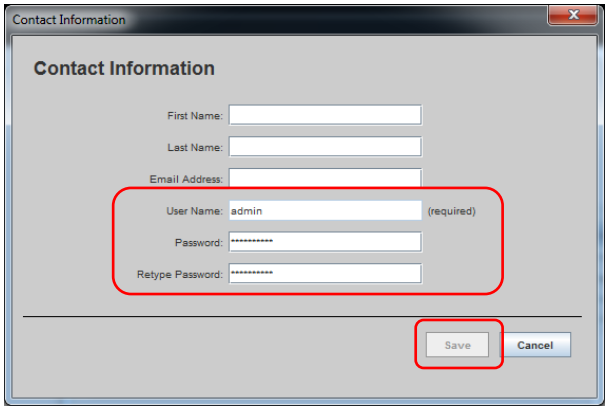


<When using Configure v2.x>
Under "Users and Groups," click "Contact List." Select a user to which you want to change a password, and then click "View/Edit."

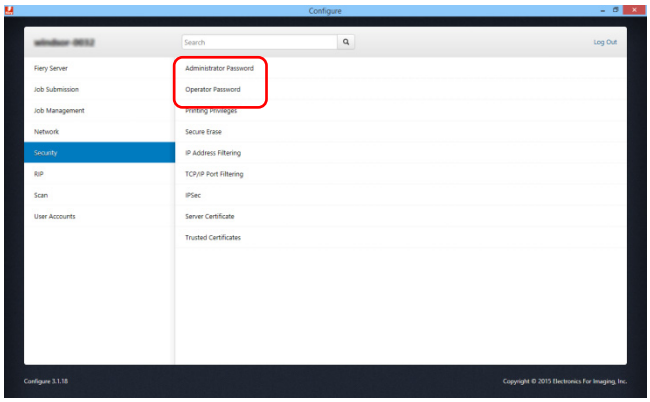


Make necessary changes and click "Save" button.

Note: After you change the password, you need to reboot the Fiery controller for the changes to take effect.

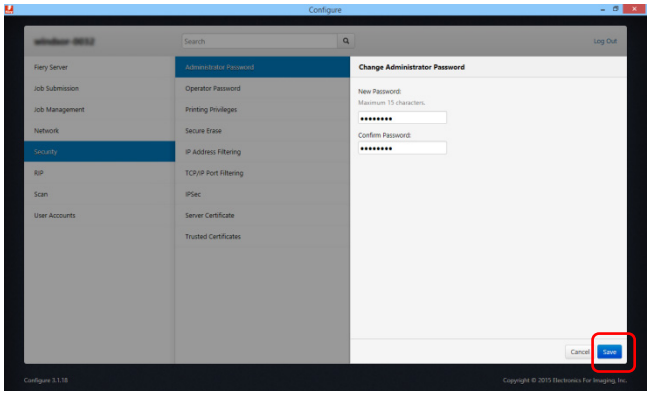


<When using Configure v3.x>
Under "Security", select a user to which you want to change a password.



Make necessary changes and click "Save" button.

Note: After you change the password, you need to reboot the Fiery controller for the changes to take effect.

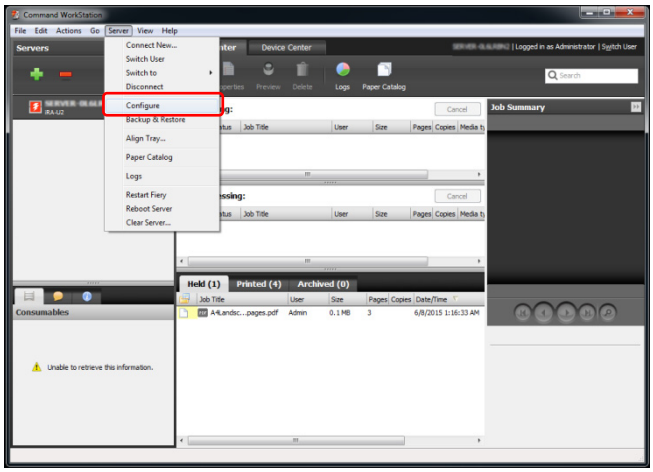


7. Configure IP filtering

By restricting the range of IP addresses that are allowed to access imagePRESS Server/ ColorPASS/ imagePASS, you can prevent unrestricted access from the network. This ensures the network security in an environment you use.

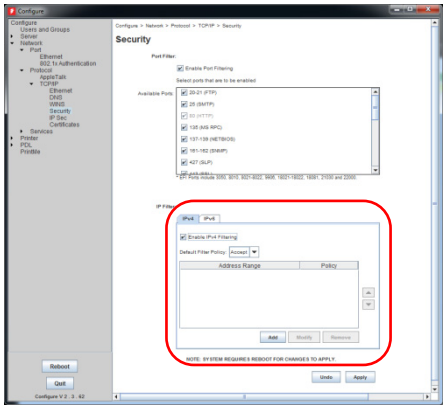
■ Steps to configure

From Command WorkStation, under "Server," select "Configure."



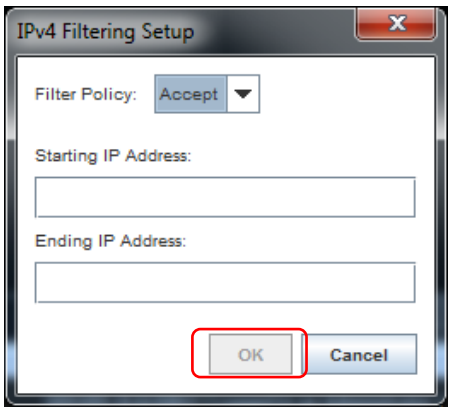
<When using Configure v2.x>
Select "Users and Groups" > "Network" > "Protocol" > "TCP/IP" > "Security." In "IP Filter," select "Add" to control access to the Fiery server.

Note: After you make changes, you need to reboot the Fiery controller for the changes to take effect.

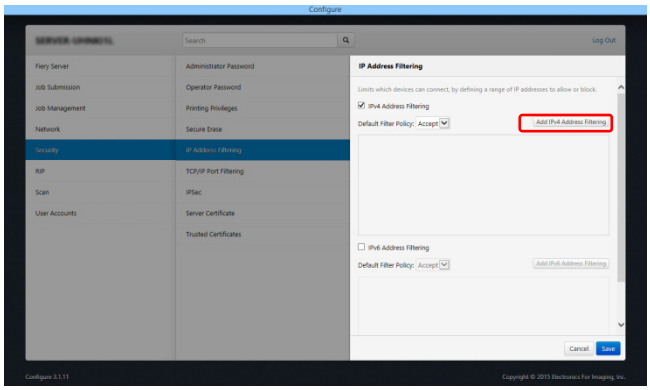


Create a range of IP addresses for filtering and specify the filter policy for the IP address range. Click "OK" button when finished.

Note: After you make changes, you need to reboot the Fiery controller for the changes to take effect.



<When using Configure v3.x>
Select "Security" > "IP Address Filtering" > "Add IPv4 Address filtering."



Create a range of IP addresses for filtering and specify the filter policy for the IP address range. Click "Add" button when finished.

Note: After you make changes, you need to reboot the Fiery controller for the changes to take effect.