To Our Customers

Fuji Xerox Co., Ltd.

How to set your Fuji Xerox multifunction device to ensure information security

In order to use Fuji Xerox multifunction devices/machines more securely, we request that you change the system administrator passcode. Changing the system administrator passcode can help prevent unauthorized third parties with malicious intent (i.e., changing settings) from accessing your device.

If you are directly connecting Fuji Xerox multifunction devices to the internet (when devices are placed outside a firewall), we also recommend that you set IP access restrictions to prohibit unauthorized access from external networks, in addition to changing the system administrator passcode. Setting IP access restrictions can help prevent unauthorized access by third parties, whose intentions are malicious (i.e., viewing job history and accessing device folders).

In addition, by setting the device authentication, you can place authentication controls by using the user information registering in the multifunction devices. This allows the use of devices only to users who have been successfully authenticated. However, users are required to either enter their user IDs from the device panel or to use an IC card when using the devices. Please contact your sales representative for details.

Please set the following to prevent unauthorized access to multifunction devices:

- Change the system administrator passcode (to prevent unauthorized access to the system administrator screen)
- Set IP access restrictions (restrict access to specific PCs)
- Set device authentication (restrict access to authenticated users)

1. Changing the System Administrator Passcode

① Log in with the system administrator's ID and passcode.

② Press the [Tools] button, and select [System Administrator's Passcode] in [Authentication / Security Settings] > [System Administrator Settings].

③ Select [New Passcode], use the displayed keyboard to enter a passcode using 4 to 12 characters, and press the [Save] button.

④ Select [Retype Passcode], use the displayed keyboard to enter the same passcode you entered in (3), and press the [Save] button.

⑤ Press the [Save] button, and select [Yes] to confirm your entry.

This completes the procedure for changing the passcode.

You can also change the system administrator ID

The system administrator ID can be set in [System Administrator's Login ID] in [Authentication / Security Settings] > [System Administrator Settings]. (See the screen on the right.)

<Caution>

If you are using an application that links with multifunction devices, such as ApeosWare Management Suite, it is also necessary to change settings in the application.

1
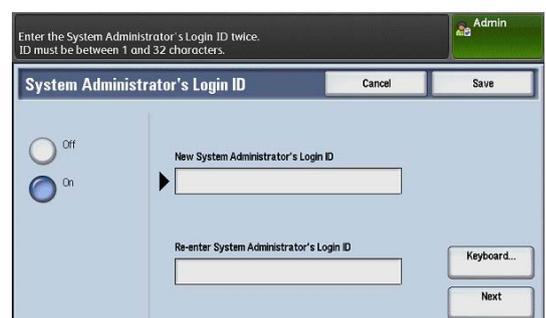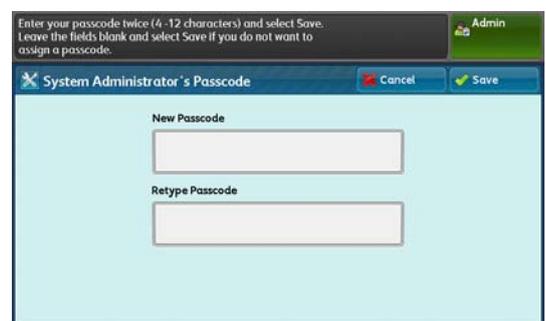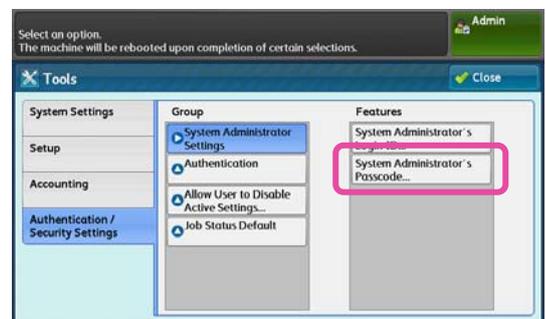
2. Setting IP Address Restrictions

① Start Internet Explorer, and enter the IP address of the device as the URL to display the CentreWare Internet Services screen.

② Select the [Properties] tab, and enter the system administrator's ID and passcode.

③ Select [Security] > [IP Filtering] in the menu on the left of the screen.
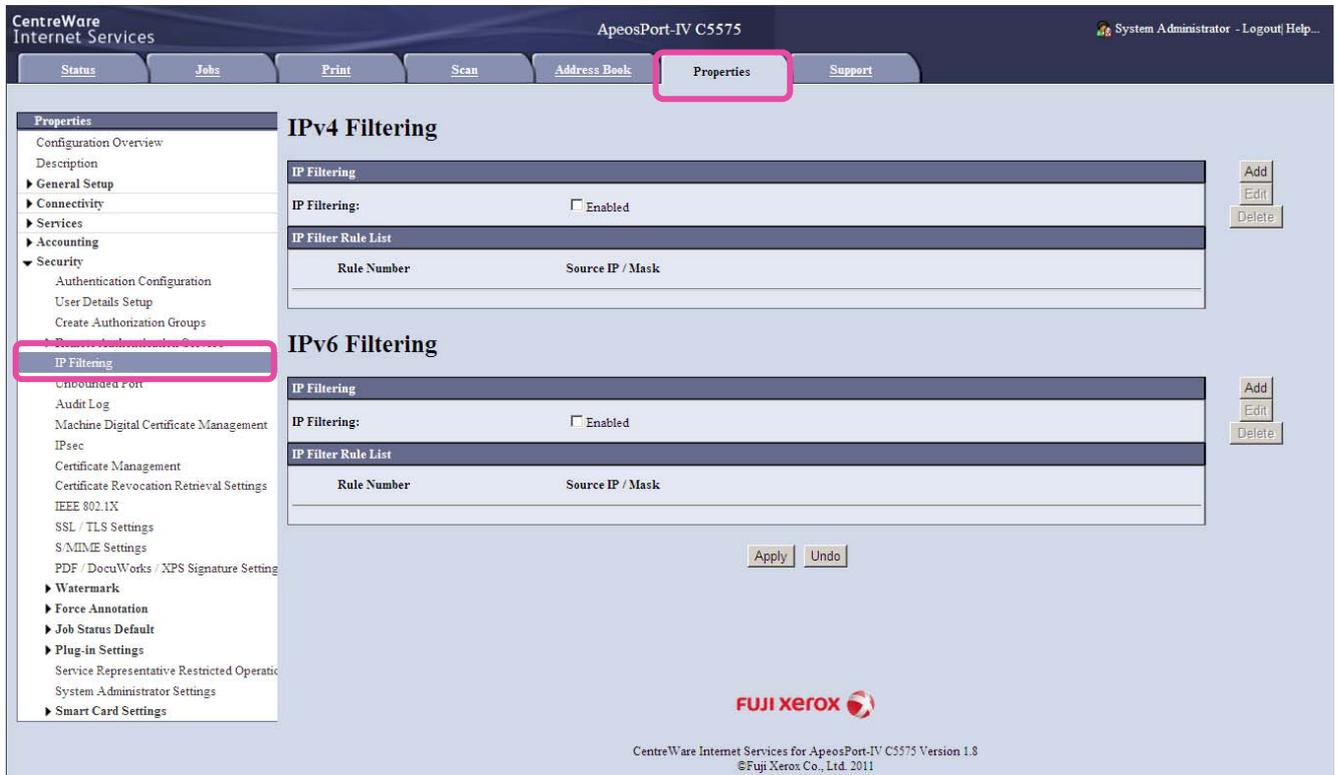
The steps below assume an IPv4 environment.

④ Press the [Add] button.

⑤ screen similar to that on the right on displayed. Enter the contents of [Source IP Address] and [Source IP Mask], and press the [Apply] button.

<Example 1> To allow access from a single IP address (192.168.10.1):
Source IP Address: 192.168.10.1
Source IP Mask: 32

<Example 2> to allow access from multiple IP addresses (192.168.10.1 to 192.168.10.255):
Source IP Address: 192.168.10.1
Source IP Mask: 24

<Note>
- Source IP Address

  Add the IPv4 addresses to allow access from in the format xxx.xxx.xxx.xxx. xxx refers to a number between 0 and 255.
- Source IP Mask

  Add the mask address of the IPv4 addresses to allow access from using a number between 0 and 32. If you set this address mask, the IP class is ignored, and the value of the address mask is used.

⑥ Select the [IP Filtering] check box under [IP Filtering – Ipv4].

⑦ Press the [Apply] button.

You can set device authentication to manage authentication using user information registered in multifunction devices. This allows the use of devices only to users who have been successfully authenticated. However, users are required to either enter their user IDs from the device panel or to use an IC card when using the devices. Please contact your sales representative for details.

Setting Device Authentication

Enable the authentication mode of the device to identify users that use the device.

1   Press the <Log In/Out> button.
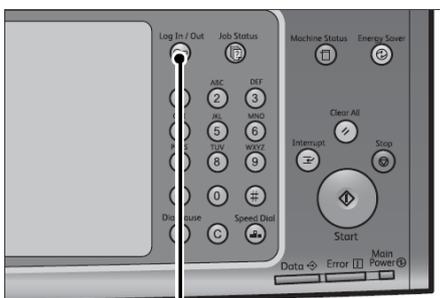
<Log In/Out> button

2   Enter the System Administrator ID, and select [Enter].
It is recommended that you change the System Administrator's ID and Passcode immediately after installing the device.   The <Log In/Out> button lights up while the user is authenticated.


3   Select [Tools].

4
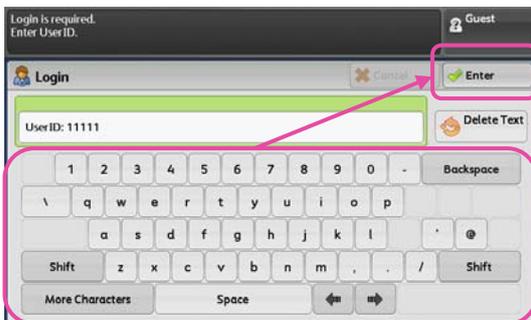
4 Select [Authentication / Security Settings], and select [Authentication].
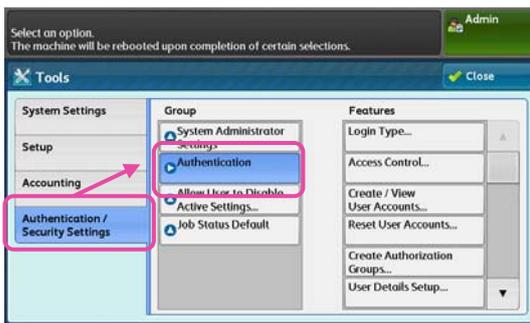


5 Select [Login Type].

6 Select [Login to Local Account], and select [Save].
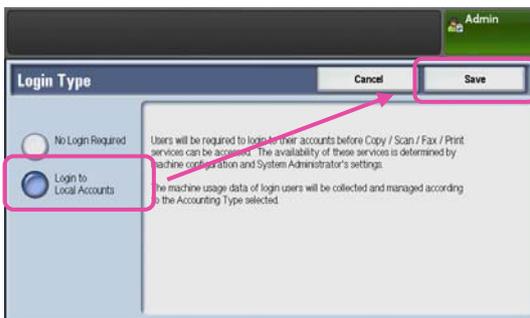
Requiring Administration

You can set whether to require a passcode to be entered when users perform authentication on the device panel. We recommend that you require passcodes to be entered in order to enhance security.

1   Press ▾ and select [Passcode Policy].
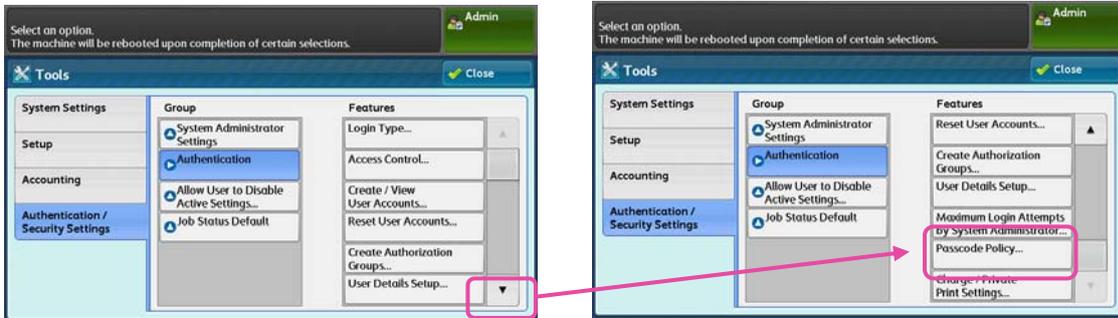
2   Select [Passcode Policy for Control Panel Login], and select [Change Settings].

3   Select [On], and select [Save].
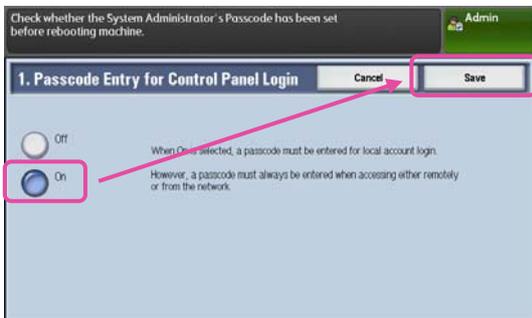
4   Select [Close].
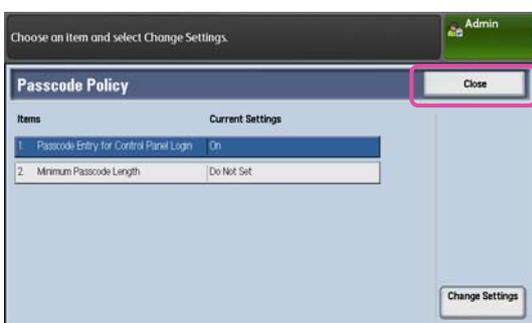
The following settings may also be required, depending on the usage environment for the multifunction devices.

　・Set accounting management

　・Register users and set function usage restrictions

However, users are required to either enter their user IDs from the device panel or to use an IC card when using the devices. Please contact your sales representative for details.