Instructions for setting security on our products

2025.02
SECURITYKDGEEN01

Contents

1 Purpose of This Guide 1
Purpose of this guide 2

2 Configuring the Correct Network Construction 3
Configuring the correct network construction 4

3 Changing the Machine Administrator and Administrator Accounts 6
Changing the Machine Administrator and Administrator accounts 7

4 Restricting Network Access with IP Filters 8
Restricting network access with IP filters 9

5 Closing Unused Ports 10
Closing unused ports 11

1 Purpose of This Guide

Purpose of this guide 2

Purpose of this guide

This guide aims to enhance the security of MFP and Printer products and helps users to:

- Set up their MFPs and Printers to make sure they can safely use the devices and protect against security threats such as cyberattacks and data breaches.
- Safeguard their business and personal data or information stored in their MFPs or Printers by correctly following the procedures that help enhance security described in guides that come with the product.

Make sure to carefully read this guide and follow the instructions described in the following chapters.

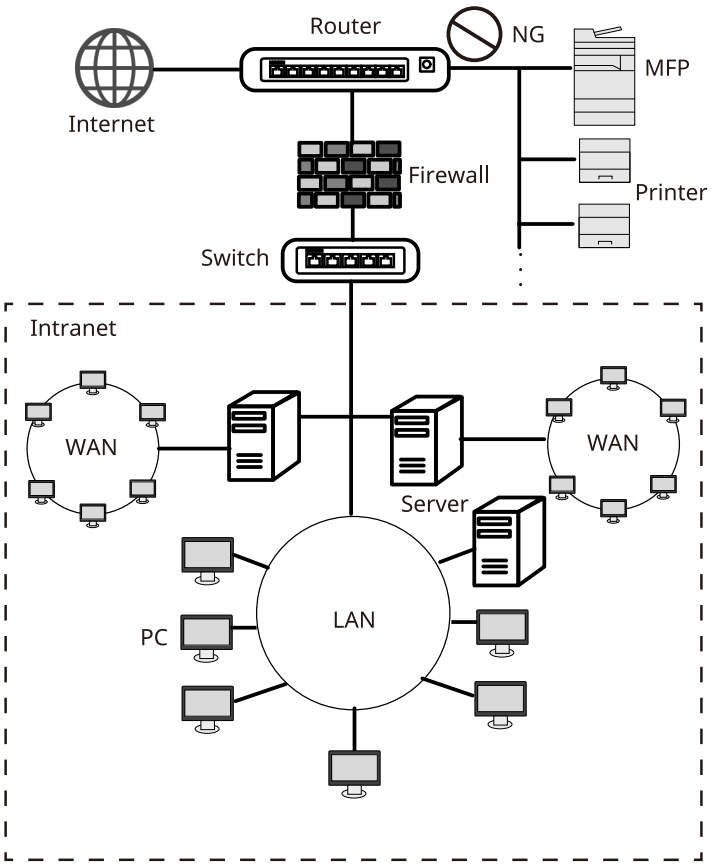
2 Configuring the Correct Network Construction

Configuring the correct network construction 4

Configuring the correct network construction

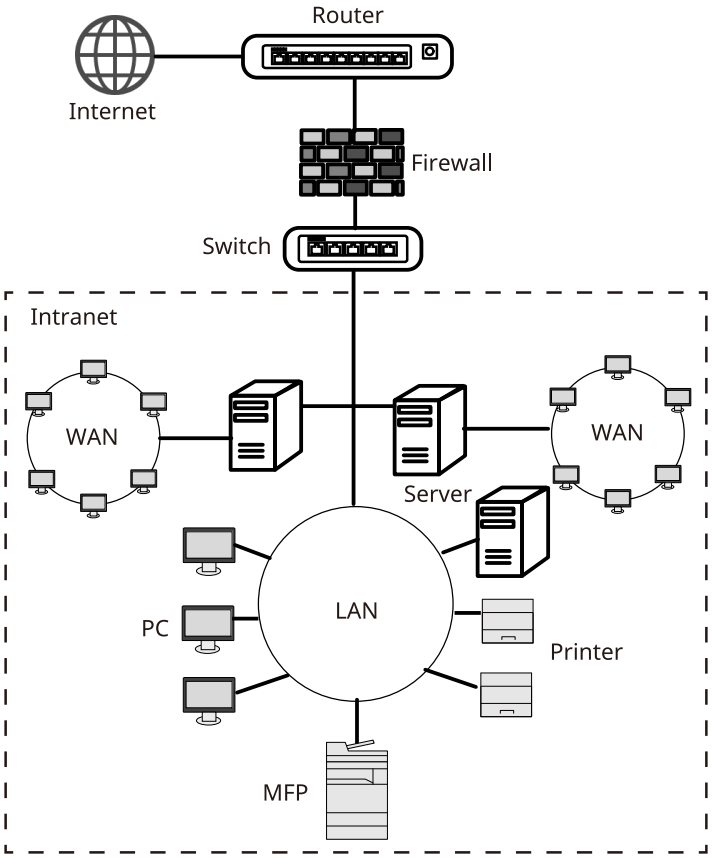
Assign a local IP address to the product, which is connected to an internal network (LAN) with firewall/routers protection, separated from an external network. *Figure-1: Incorrect product connection on network* shows that products are connected directly to the Internet. Such incorrect connections will result in the leakage of information assets or unauthorized use of products.

Figure -1: Incorrect product connection on network



Connect the products to the outside of the Internet through a firewall as shown in *Figure-2: Correct product connection on network*.

Figure-2: Correct product connection on network



3 Changing the Machine Administrator and Administrator Accounts

Changing the Machine Administrator and Administrator accounts 7

Changing the Machine Administrator and Administrator accounts

It is important to change the product's default password to a new password to stay protected from unauthorized external access. To be able to safely use this product, make sure to correctly change the default Machine Administrator and Administrator accounts by referring to the procedures described in the Operation Guide.

NOTE

The setup procedures for changing the default login password and other settings may defer depending on the model. Refer to the following guide that corresponds with this product:

➡ **Operation Guide**

Administrator Privileges Overview

This machine is shipped with two default users registered one with Machine Administrator privileges, and another with Administrator privileges. The user with Machine Administrator privileges and the user with Administrator privileges can configure important settings for the machine. The differences in the privileges are as follows:

User Privilege	Can Do	Cannot Do
Machine Administrator	Can only login from the machine.	Cannot login from the product's embedded web server.
	Can configure the product's network settings, security settings such as user registration and the machine's security level.	
Administrator	Can login from the machine or from other devices.	Cannot set the machine's security level.
	Can configure the product's network settings and security settings such as user registration.	

Password Policy and User Account Lockout

You can prohibit the setting and use of passwords that do not comply with the password policy. Setting the Password Policy makes it more difficult to break the password.

You can also prohibit and lock the use of a user account if an incorrect password is entered repeatedly to login using that account.

For information on how to set the Password Policy and User Account Lockout, refer to the following guide that corresponds with this product:

➡ **Operation Guide**

4 Restricting Network Access with IP Filters

Restricting network access with IP filters 9

Restricting network access with IP filters

Use the IP filter to specify IP addresses that are allowed or prohibited access. By limiting the IP addresses that can access the product, you can prevent external intrusions to your product and internal network. For details on how to set IP filter, refer to our product's embedded web server user guide.

5 Closing Unused Ports

Closing unused ports 11

Closing unused ports

Check the services and protocols used in your environment and turn off any unused ports (protocols) by referring to *Table-1: List of port settings*. This will prevent unauthorized access and attacks to the ports.

Set the desired protocols to [Off] from the system menu through the product's operation panel or embedded web server.

NOTE

For details on how to close the unused ports (protocols), refer to the following guides:

- **Operation Guide**
- **Our product's embedded web server user guide**

Table-1: List of port settings

Port	Protocol	Setting Value
21	FTP	FTP Server (Reception)
80	HTTP	HTTP
139	NetBIOS Session Service	NetBEUI*1
445	CIFS	NetBEUI*1
137	NetBIOS Name Service	NetBEUI*1
138	NetBIOS Datagram Service	NetBEUI*1
139	NetBIOS Session Service	NetBEUI*1
443	HTTPS/IPPS	HTTPS
515	LPD	LPD
631	IPP	IPP
5358	WSD-Print	WSD Print
5358	WSD-Scan*2	WSD Scan
9090	KM-WSDL	Enhanced WSD
9091	KM-WSDL (SSL/TLS)	Enhanced WSD(TLS)
9070	WS-Transfer	All WSD-related ports (WSD Print, WSD Scan, Enhanced WSD, and Enhanced WSD(TLS))
3702	WS-Discovery	All WSD-related ports (WSD Print, WSD Scan, Enhanced WSD, and Enhanced WSD(TLS))
9061	Enhanced RFB (SSL/TLS)	Enhanced VNC(RFB) over TLS
9062	RFB	VNC(RFB)
9063	RFB (SSL/TLS)	VNC(RFB) over TLS
9080	REST	REST
9081	REST (SSL/TLS)	REST over TLS
9095	eSCL*2	eSCL
9096	eSCL (SSL/TLS)*2	eSCL over TLS

Port	Protocol	Setting Value
9100	PortPrint lp1	Raw*1
9101	PortPrint lp2	Raw*1
9102	PortPrint lp3	Raw*1
9103	PortPrint lp4	Raw*1
68	DHCPv4 client	DHCP
161	SNMP	SNMP
500	ISAKMP	IPsec*1
4500	NAT-Traversal	IPsec*1
5353	Multicast DNS (Bonjour)	Bonjour
5355	LLMNR*3	—

*1 This setting allows you to close multiple ports (protocols).
*2 This port is only available for MFP products.
*3 This port is always open.