kyoceradocumentsolutions.com

Firmware Upgrade Tool User Guide

2024.2
Ver.2.0

Contents

1. Preface

1.1 About This Document

This document contains a firmware update procedure that uses the “Firmware Upgrade Tool” application software to update the firmware of the product you are using.

1.2 Legal and Safety Information

- Unauthorized copy pf all of part of this guide is prohibited.
- The information in this guide is subject to change without notice.
- This document explains operations using operations performed in Windows 10 as an example.
- We are not responsible for any failures or damages that may occur resulting from conditions or usage procedures not contained in this document.

1.3 About Trade Names

- Microsoft, Windows and Windows Server are registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.
- Mac and macOS are trademarks of Apple Inc., registered in the U.S. and other countries.
- Linux is the registered trademark or trademark of Linus Torvalds in the U.S. and other countries.
- All other brands and product names are registered trademarks or trademarks of their respective companies. The designations ™ and ® will not be used in this guide.

1.4 About the Firmware Upgrade Tool

Firmware is software that controls a product and it is built into the product. By updating the firmware, improvements can be made to the product’s security and operations can be stabilized. We recommend using this application to update the product’s firmware so that you can continue to use the product safely.

1.5 System Requirements

Operating System：	Windows	Windows 11
		Windows 10
		Windows Server 2022
		Windows Server 2019
		Windows Server 2016
	Mac	macOS 14 Sonoma
		macOS 13 Ventura
		macOS 12 Monterey
	Linux	Ubuntu 22.04 LTS
		CentOS Stream 9
		OpenSUSE Leap 15.5
Memory Capacity:	At least 2 GB	
Execution Environment:	Requires “Visual C++ Redistributable Package” (only for Windows)	
Network:	Wired network connection recommended	

2. Firmware Update

Caution

- A network connection is required during the firmware update.
- The firmware cannot be restored to an earlier version once it has been updated.
- Do not turn off the product or disconnect the network cable during the firmware update. Additionally, the product cannot be used during the firmware update.
- Make sure that the HTTP/HTTPS port number is not blocked by a firewall or virus scanner.

2.1 Firmware Update Preparation

Perform the following before using this tool to update the firmware.

- Access the support site for your region and download the firmware file to your computer.
- Confirm the setting details of the protocol (SNMPv1/v2c, SNMPv3), and confirm that HTTP and HTTPS is enabled, for the product that is going to have its firmware updated.

  Confirm the setting details from Command Center RX. For details, refer to the Command Center RX User Guide.
- Confirm the user name and password for the Administrator that is registered on the product that is going to have its firmware updated.

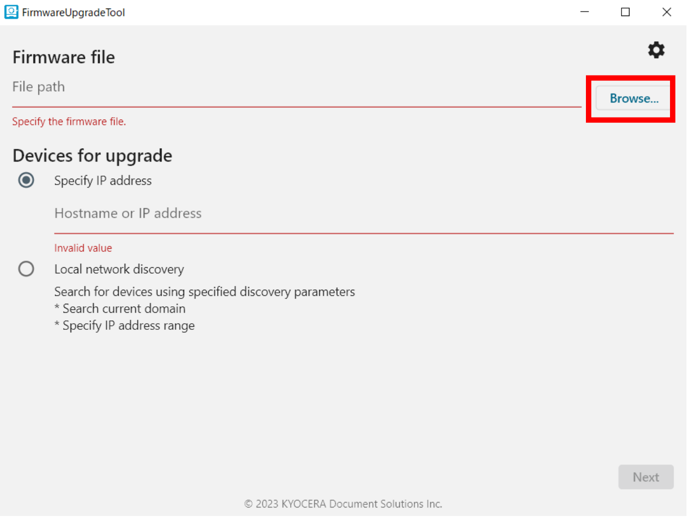
Note

Confirm the user name and password for the Administrator, not for the Machine Administrator. Refer to the Operation Guide for details on the user name and password for the Administrator.

2.2 Update Product Firmware

1. **Start up Firmware Upgrade Tool.**
2. **Click [Accept] on the “LICENSE AGREEMENT” screen.**

3. **Click [Browse], and select the firmware file you downloaded to your computer.**


FirmwareUpgradeTool

Firmware file

File path

Browse...

Specify the firmware file.

Devices for upgrade

● Specify IP address

Hostname or IP address

Invalid value

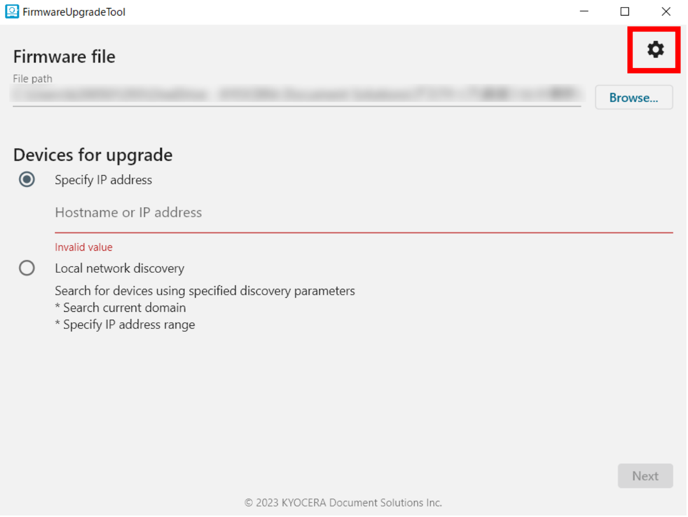
○ Local network discovery

Search for devices using specified discovery parameters
* Search current domain
* Specify IP address range

Next

© 2023 KYOCERA Document Solutions Inc.

4. **Click ⚙.**


FirmwareUpgradeTool

Firmware file

File path

Browse...

Devices for upgrade

● Specify IP address

Hostname or IP address

Invalid value

○ Local network discovery

Search for devices using specified discovery parameters
* Search current domain
* Specify IP address range

Next

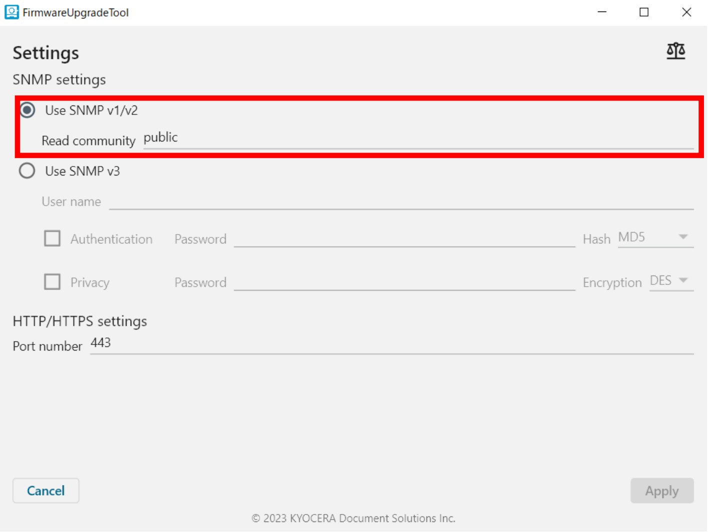
© 2023 KYOCERA Document Solutions Inc.

5. Set the protocol (SNMPv1/v2c, SNMPv3) information for the product that is going to have its firmware updated.

If SNMPv1/v2c is set to On in Command Center RX

1. Select “Use SNMP v1/v2”.

2. In “Read community,” input the SNMPv1/v2c community name.



FirmwareUpgradeTool

Settings

SNMP settings

● Use SNMP v1/v2

Read community: public

○ Use SNMP v3

User name

□ Authentication Password Hash MD5

□ Privacy Password Encryption DES

HTTP/HTTPS settings

Port number: 443

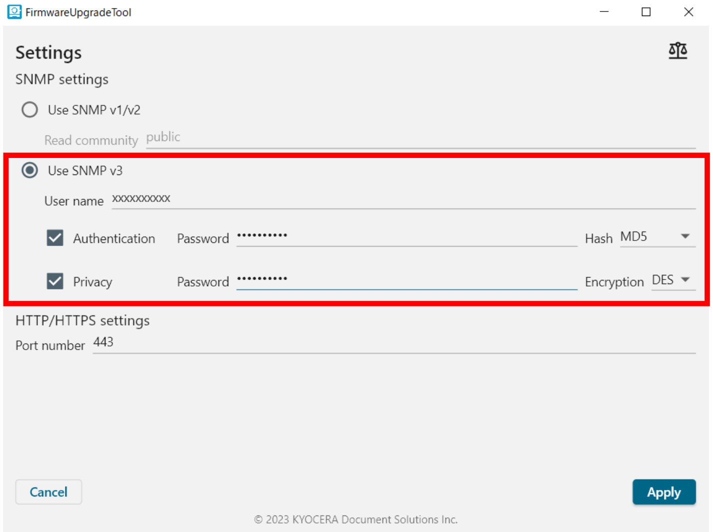
If SNMPv3 is set to On in Command Center RX

1. Select “Use SNMP v3”.

2. In “User Name,” input the SNMPv3 user name.

3. If “Authentication” is set to On in Command Center RX, select “Authentication” and input your password, then select the authentication algorithm from the “Hash” dropdown menu.

4. If “Privacy” is set to On in Command Center RX, select “Privacy” and input your password, then select the encryption algorithm from the “Encryption” dropdown menu.



Settings

SNMP settings

○ Use SNMP v1/v2

Read community public

● Use SNMP v3

User name xxxxxxxxxx

☑ Authentication Password •••••••••• Hash MD5

☑ Privacy Password •••••••••• Encryption DES

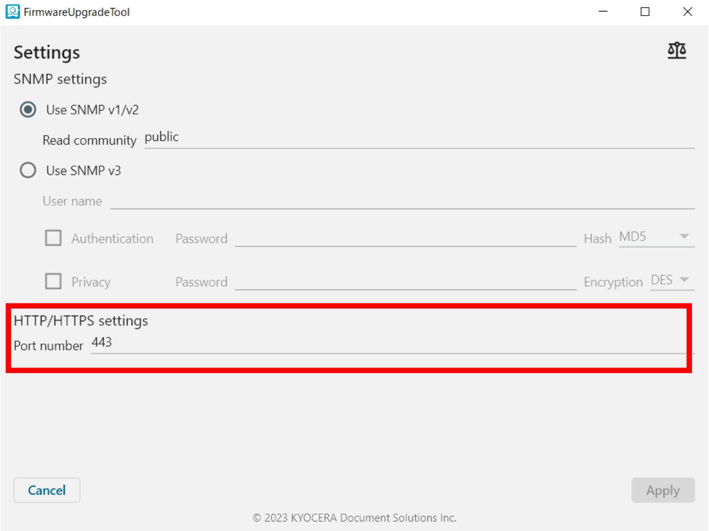
HTTP/HTTPS settings

Port number 443

© 2023 KYOCERA Document Solutions Inc.

6. **If you are using a Windows or Mac computer and port 443 is already in use, specify the HTTP/HTTPS port number.**

Note
Normally, there is no need to change the port number from “443”.



Settings

SNMP settings

● Use SNMP v1/v2

Read community public

○ Use SNMP v3

User name

□ Authentication Password Hash MD5

□ Privacy Password Encryption DES

HTTP/HTTPS settings

Port number 443

© 2023 KYOCERA Document Solutions Inc.

7. **If you are using a Linux computer and port 10443 is already in use, specify the HTTP/HTTPS port number.**

8. **Click [Apply].**

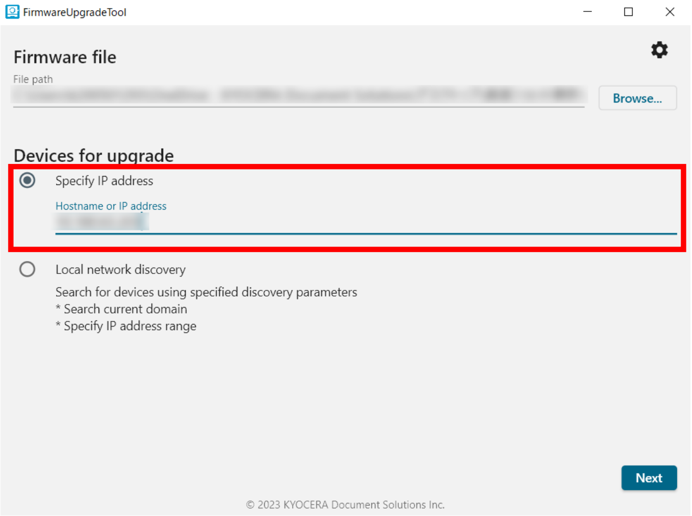
Note
Click [Cancel] if you want to cancel the change to the settings.

9. Select the product to have its firmware updated.

If specifying the product with an IP address or host name

1. Select “Specify IP address”.

2. Input the product’s IP address or host name.



FirmwareUpgradeTool

Firmware file

File path

[redacted]

Browse...

Devices for upgrade

● Specify IP address

Hostname or IP address

[redacted]

○ Local network discovery

Search for devices using specified discovery parameters
* Search current domain
* Specify IP address range

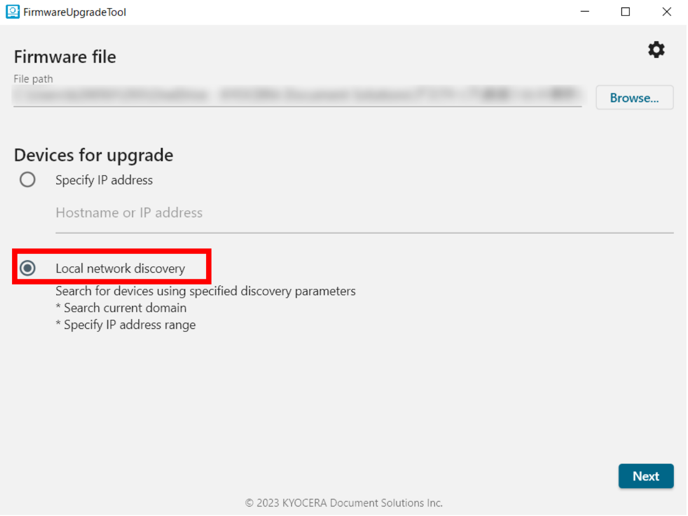
Next

© 2023 KYOCERA Document Solutions Inc.

3. Click [Next] and proceed to step **10**.

If specifying the product by searching for it over the network

1. Select “Local network discovery”.



FirmwareUpgradeTool

Firmware file

File path

[redacted]

Browse...

Devices for upgrade

○ Specify IP address

Hostname or IP address

● Local network discovery

Search for devices using specified discovery parameters
* Search current domain
* Specify IP address range

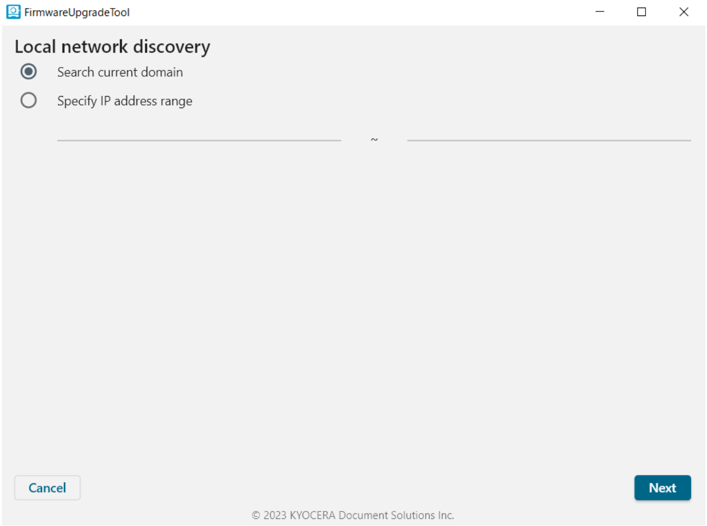
Next

© 2023 KYOCERA Document Solutions Inc.

2. Click [Next].

3. Do one of the following:

    - If searching from all products on the network, select “Search current domain”.
    - If searching from a filtered list of all products on the network, select “Specify IP address range” and input the IP addresses.



FirmwareUpgradeTool

Local network discovery

● Search current domain

○ Specify IP address range

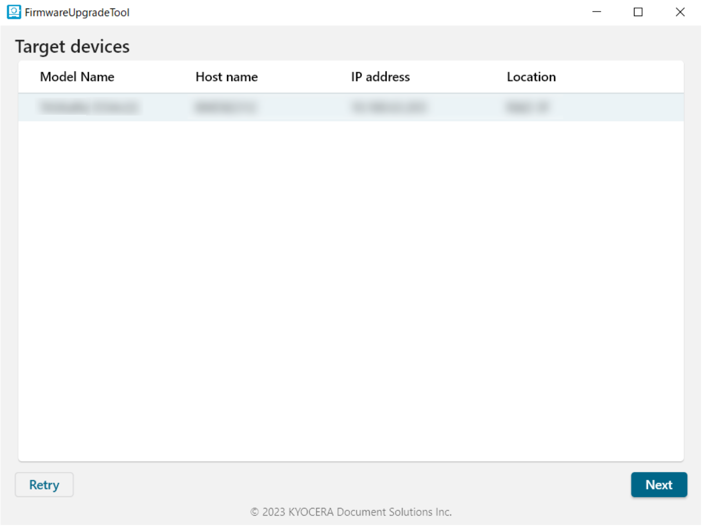
~

Cancel Next

© 2023 KYOCERA Document Solutions Inc.

4. Click [Next].

5. Select the product to have its firmware updated.



FirmwareUpgradeTool

Target devices

Model Name	Host name	IP address	Location
[redacted]	[redacted]	[redacted]	[redacted]

Retry Next

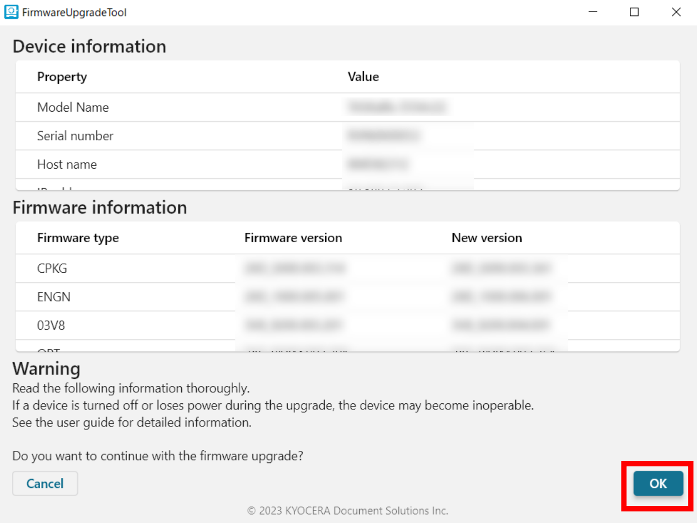
© 2023 KYOCERA Document Solutions Inc.

6. Click [Next].

Note

Click [Retry] to retry the search.

10. Click [OK].



Device information

Property	Value
Model Name	[redacted]
Serial number	[redacted]
Host name	[redacted]

Firmware information

Firmware type	Firmware version	New version
CPKG	[redacted]	[redacted]
ENGN	[redacted]	[redacted]
03V8	[redacted]	[redacted]

Warning

Read the following information thoroughly.
If a device is turned off or loses power during the upgrade, the device may become inoperable.
See the user guide for detailed information.

Do you want to continue with the firmware upgrade?

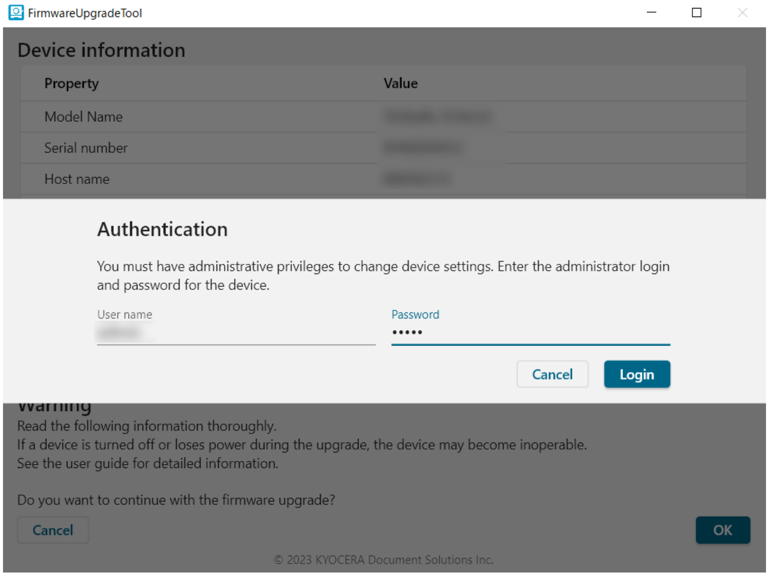
Caution

Do not turn off the product or disconnect the network cable during the firmware update. Additionally, the product cannot be used during the firmware update.

Note

If "WARNING: The device already has a new version installed." is displayed, the update is unnecessary as the product is already running the newest version of the firmware. Click [Cancel] and end the operation.

11. Input the user name and password for the Administrator registered to the product.



Device information

Property	Value
Model Name	[redacted]
Serial number	[redacted]
Host name	[redacted]

Authentication

You must have administrative privileges to change device settings. Enter the administrator login and password for the device.

User name: [redacted]

Password: •••••

Warning

Read the following information thoroughly.
If a device is turned off or loses power during the upgrade, the device may become inoperable.
See the user guide for detailed information.

Do you want to continue with the firmware upgrade?

12. Click [Login].

It will start the firmware update.
When the firmware update is finished, “Upgrade completed.” will be displayed.

Note

If “Authentication failed. Verify user name and password and try again.” is displayed after clicking [Login], there is an error in the user name or password that was entered in step 11. Confirm the correct user name and password.

13. Click [Exit].

3. Troubleshooting

Message	Corrective Actions
Warning You do not have permission to access this host. Please check your settings and try again.	· Check the host name or IP address you entered is correct. · Check the SNMP settings in the [Settings] screen match the protocol settings (SNMPv1/v2c, SNMPv3) on the product. You can check the product protocol settings in Command Center RX. For more information, refer to the Command Center RX User Guide. · Check the specified firmware file is compatible with your product. · Check the product's system menu or Command Center RX to confirm if this tool can be used. However, in some products, the permission settings may not be supported. For more information, refer to the Operation Guide or Command Center RX User Guide.
Warning Devices not found. Search for devices on your local network	
Error Upgrade failed. Reason: Cannot verify installed version.	· Check the firmware version of the product, and then check the firmware has been updated. (Refer to the Operation Guide for how to check the firmware version of the product.) If it has been updated, ignore this error and click [Exit]. If it has not been updated, check the following items and update the firmware again. · The network is not disconnected · The product is turned on · This application is not blocked by a firewall · If the problem persists, contact your service representative.
Error Upgrade failed. Reason: Master file version error	
Error Upgrade failed. Reason: Cannot write firmware file to device.	
Error Upgrade failed. Reason: This HTTP/HTTPS port number (#) has been used. Please specify another HTTP/HTTPS port number in Settings and try again.	The HTTP/HTTPS port number specified on the setting screen is already in use. Specify a port number that is not in use. **For Windows** You can find unused port numbers by using the "netstat" command in the command prompt. **For Mac** You can find unused port numbers by using the "netstat" command or "lsof" command in the terminal.

Message	Corrective Actions
	For Linux You can find unused port numbers by using the "ss" command or "lsof" command in the terminal.