

# Firmware Upgrade Tool User Guide



---

# Contents

<b>1. Preface .....</b>	<b>3</b>
1.1 About This Document .....	3
1.2 Legal and Safety Information.....	3
1.3 About Trade Names.....	3
1.4 About the Firmware Upgrade Tool.....	3
1.5 System Requirements .....	4
<b>2. Firmware Update .....</b>	<b>5</b>
2.1 Firmware Update Preparation .....	5
2.2 Update Product Firmware.....	5
<b>3. Troubleshooting .....</b>	<b>14</b>

---

# 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 of all or 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. All other brands and product names are registered trademarks or trademarks of their respective companies. The designations <sup>™</sup> and <sup>®</sup> 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 8.1, Windows 10, Windows 10 Anniversary Update, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022
Memory Capacity:	At least 2 GB
Execution Environment:	Microsoft .NET Framework 4.8 or later
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.

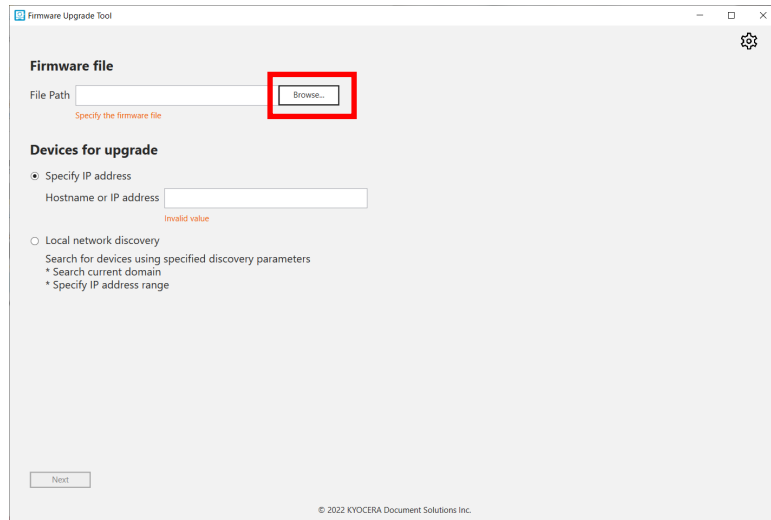
### Note

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.

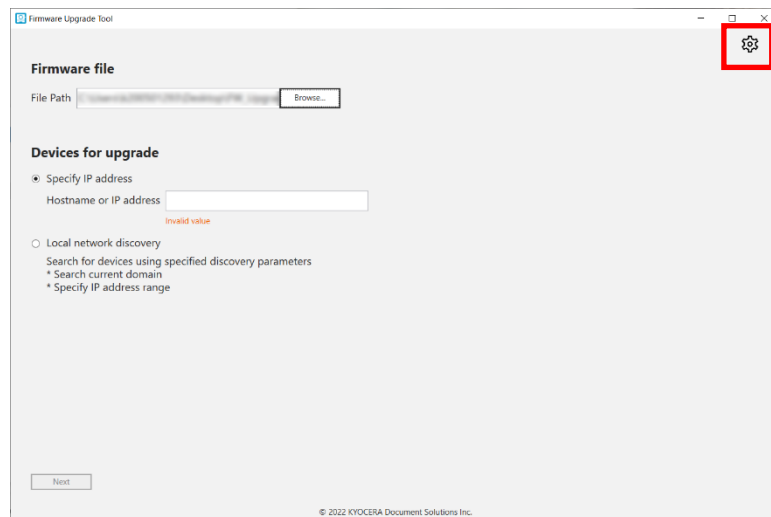
### 2.2 Update Product Firmware

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.**



**4. Click .**



---

**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.

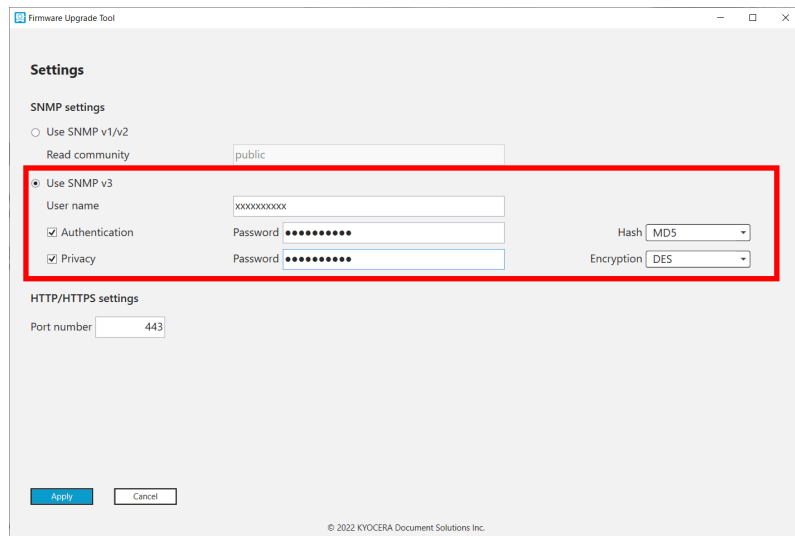
The screenshot shows the 'Firmware Upgrade Tool' settings window. The 'SNMP settings' section is highlighted with a red box. It contains the following options:

- Use SNMP v1/v2: Read community: public
- Use SNMP v3: User name: [empty], Authentication: , Privacy: , Hash: MD5, Encryption: DES

Below the SNMP settings is the 'HTTP/HTTPS settings' section with 'Port number' set to 443. At the bottom are 'Apply' and 'Cancel' buttons. The copyright notice '© 2022 KYOCERA Document Solutions Inc.' is visible at the bottom right.

## 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.



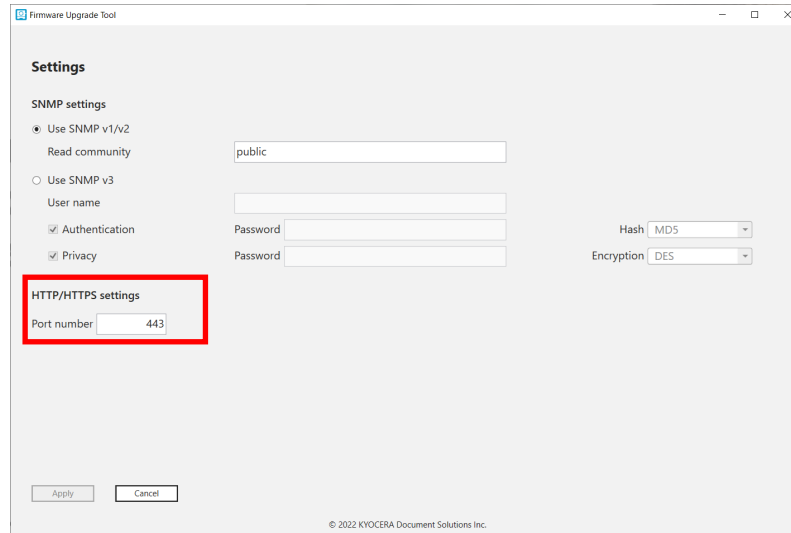
The screenshot shows the 'Settings' window of the 'Firmware Upgrade Tool'. The 'SNMP settings' section is expanded to show 'Use SNMP v3' selected. The 'Read community' field contains 'public'. The 'User name' field contains 'xxxxxxxxxx'. The 'Authentication' checkbox is checked, and the 'Password' field contains '\*\*\*\*\*'. The 'Hash' dropdown menu is set to 'MD5'. The 'Privacy' checkbox is checked, and the 'Password' field contains '\*\*\*\*\*'. The 'Encryption' dropdown menu is set to 'DES'. The 'HTTP/HTTPS settings' section shows the 'Port number' field set to '443'. At the bottom, there are 'Apply' and 'Cancel' buttons. The copyright notice '© 2022 KYOCERA Document Solutions Inc.' is visible at the bottom right.



**6. (Only when the computer you're using is already using port 443)  
Specify the HTTP/HTTPS port number.**

**Note**

Normally, there is no need to change the port number from "443".



**7. Click [Apply].**

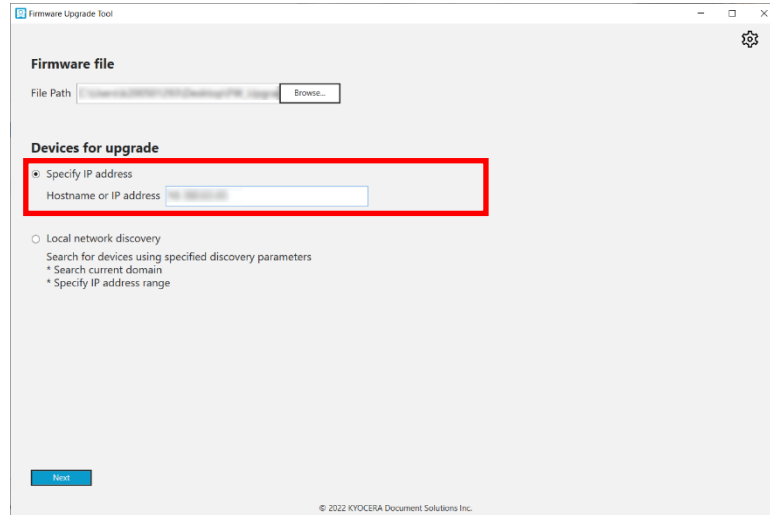
**Note**

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

## 8. Select the product to have its firmware updated.

### If specifying the product with an IP address or host name

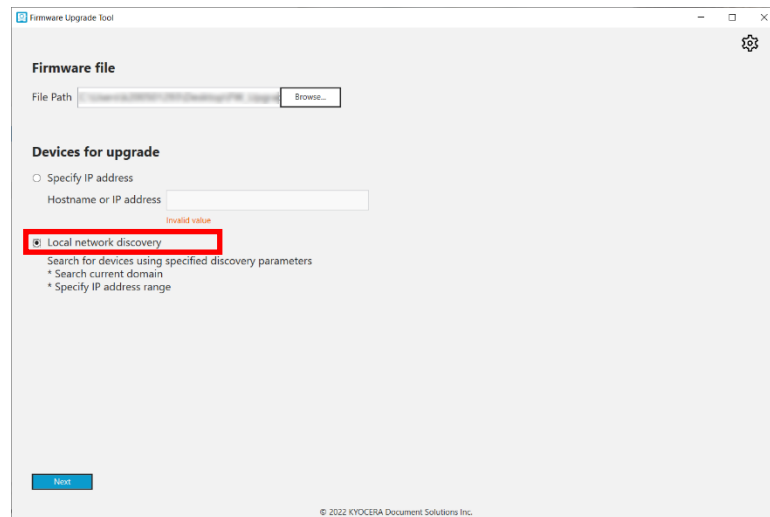
1. Select “Specify IP address”.
2. Input the product's IP address or host name.



3. Click [Next] and proceed to step 9.

### If specifying the product by searching for it over the network

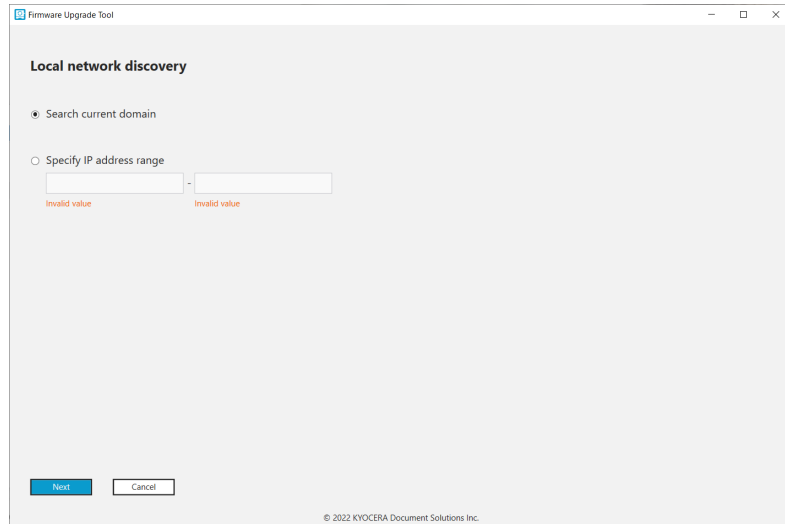
1. Select “Local network discovery”.



2. Click [Next].

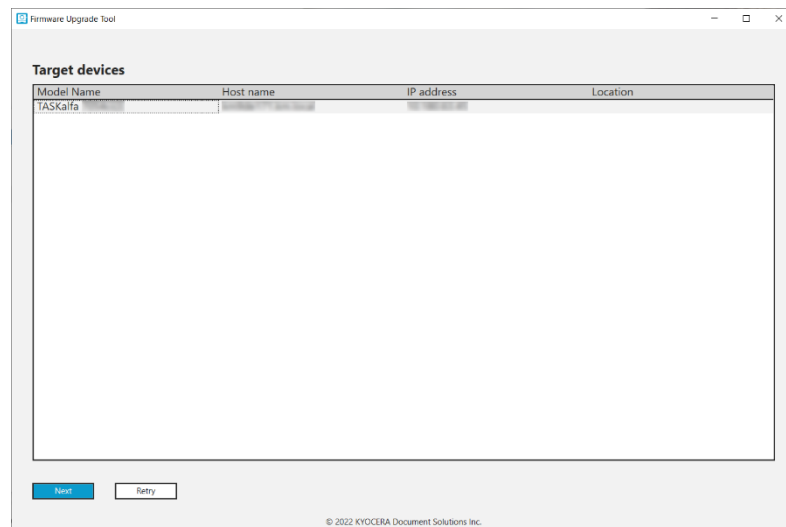
3. Do one of the following:

- 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.



4. Click [Next].

5. Select the product to have its firmware updated.

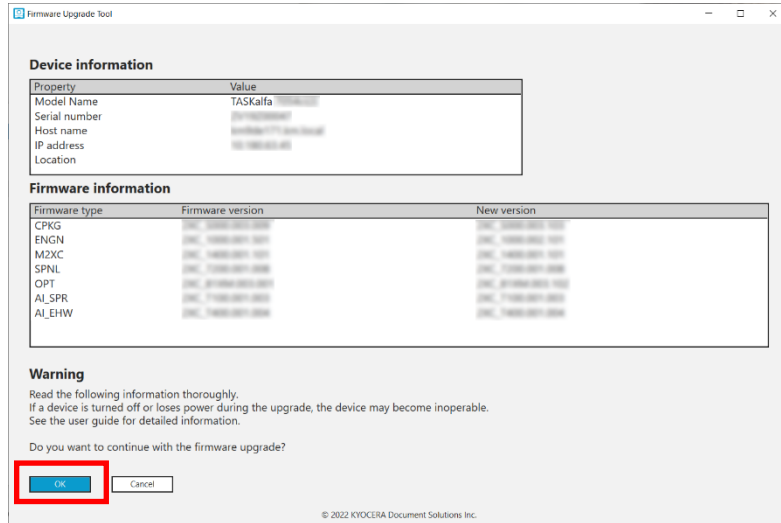


6. Click [Next].

**Note**

Click [Retry] to retry the search.

## 9. Click [OK].



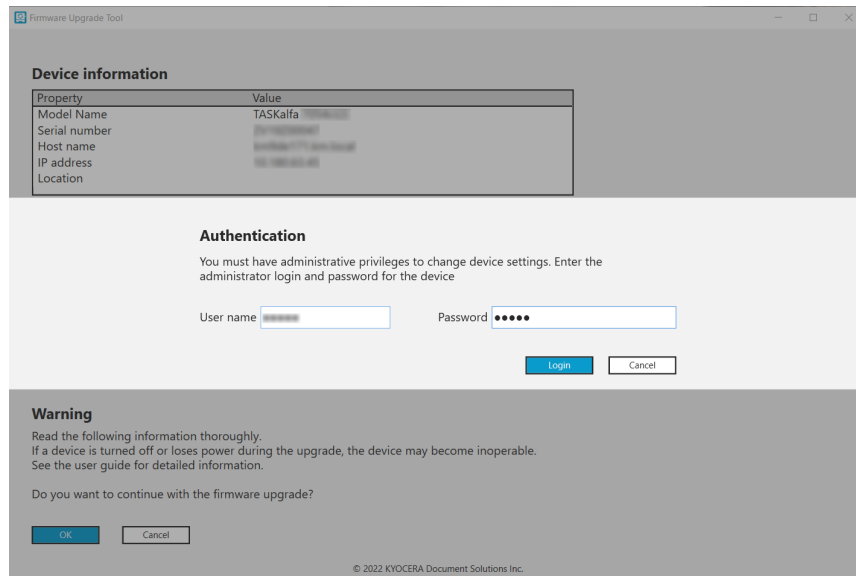
### Caution

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.

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



---

## 11. 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 10. Confirm the correct user name and password.

## 12. Click [Exit].

## 3. Troubleshooting

Message	Corrective Actions
Warning You do not have permission to access this host. Please check your settings and try again.	<ul style="list-style-type: none"><li>• Check the host name or IP address you entered is correct.</li><li>• 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.</li></ul>
Warning Devices not found. Search for devices on your local network	
Error Upgrade failed. Reason: Cannot verify installed version.	<ul style="list-style-type: none"><li>• 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.)</li></ul> <p>If it has been updated, ignore this error and click [Exit].</p> <p>If it has not been updated, check the network is not disconnected and the product is turned on, and then update the firmware again.</p> <ul style="list-style-type: none"><li>• If the problem persists, contact your service representative.</li></ul>
Error Upgrade failed. Reason: Master file version error	
Error Upgrade failed. Reason: Cannot write firmware file to device.	