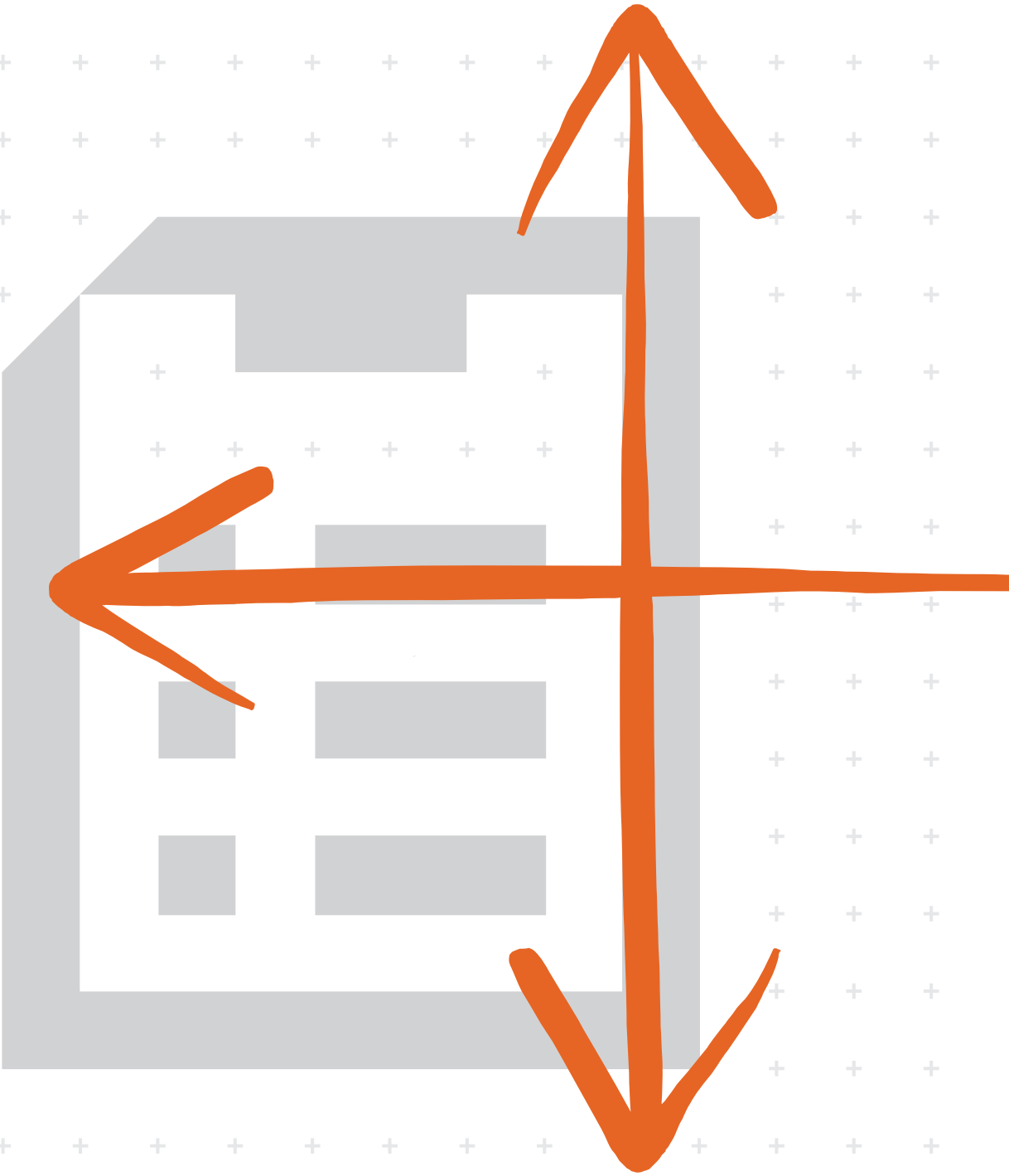
kyoceradocumentsolutions.com

KYOCERA Net Viewer
User Guide

2023.07
KNVUGKDEN660



Legal notes

Unauthorized reproduction of all or part of this guide is prohibited.

The information in this guide is subject to change without notice.

We cannot be held liable for any problems arising from the use of this product, regardless of the information herein.

Regarding trademarks

Microsoft®, Windows®, and Active Directory® are registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

All other brand and product names herein are registered trademarks or trademarks of their respective companies.

Table of Contents

Chapter 4 Device

Chapter 5 Account

Chapter 6 Host

1 Product overview

The **KYOCERA Net Viewer** application lets you organize and monitor network device information.

Documentation

This guide provides instructions on how to use the features and settings of the application.

Features and options may vary depending on your device.

This guide is intended for system administrators and all other users.

Conventions

The following conventions may be used in this guide:

- **Bold text** is used for menu items and buttons
- Screen, text box, and drop-down menu titles are spelled and punctuated exactly as they are displayed on the screen
- *Italics* are used for document titles
- Icons are used to draw your attention to certain pieces of information. Examples:

This is a NOTE icon. This indicates information that is useful to know.

This is a CAUTION icon. This indicates important information that you should know, including such things as data loss if the procedure is not done properly.

System requirements

Refer to the *Release Notes* or *ReadMe* that accompany this product.

2 Getting started

Organize and monitor network device information with different features that are available through default and custom views. To get started, log in, and then set up a workspace by discovering devices on your network.

Starting and logging in

1. Open the application.
2. Do either of the following:
   - If you have administrator rights, then you may be required to provide login information.

     The application opens the last saved workspace.

   - If you do not have administrator rights or if this is the first time that you opened the application, then do the following:

     Your network administrator may need to set up your login information.

     a. Specify the location of your workspace folder, and then select **OK**.
     b. Add devices to your workspace. For more information, see *Device Discovery*.

When you select **File** > **Close window**, the application continues to run in the system tray.

Workspaces

Collect and view device information and settings. The workspace data displays in the device list or map, and in the navigation pane of the screen.

A workspace is identified with login information. When a user opens the application, the last workspace from the user history automatically opens. When the user closes the application, the workspace is automatically saved. You need only one workspace, but you can also define additional workspaces for different devices in multiple locations.

Adding a new workspace

1. Go to **File** > **New workspace**.
2. Select **Yes**.

3 Specify the location of the workspace folder.

4 Select **OK**.
The application restarts.

Opening an existing workspace

A workspace created for an older version of the application is converted for the newer version and cannot be changed back.

1 Go to **File** > **Open workspace**.

2 Select **Yes**.

3 Specify the location of the workspace folder.

4 Select **OK**.
The application restarts.

Import and export workspaces

The file name extension of the workspace varies, depending on the import source.

Import source	File name extension
Version 4.x	.kv3
Version 5 or later	.kvx
KM-Net for Accounting	.xml

To reuse device data and UI information from an older version, import and convert the old workspace to the new workspace. When you share a workspace with another user, the application prevents other users including administrators from accessing the workspace to protect data integrity.

Importing a file to a new workspace

1 Go to **File** > **Import to new workspace**.

2 Browse for a file to import.

The file must have an extension of .kvx, .kv3, or .xml.

3 Specify the location of the workspace folder.

4 Select **OK**.

Exporting a workspace

1. Go to **File** > **Export** > **Workspace**.
2. Enter a file name, and then specify the export destination.
3. Select **Save** > **OK**.

Viewing or restoring recent workspaces

Only the last five workspaces appear in the list.

1. Go to **File** > **Open recent**.
2. Select a workspace from the list, and then select **Yes**.

The application restarts.

Device discovery

This feature lets you check networks for devices. If new devices are found, then the application updates its database with information about the device. You can manually discover single or multiple devices, or you can run discovery automatically according to a set schedule. It is also possible to exclude devices from being discovered.

When the application is launched for the first time, or when a new workspace is opened, the Add Devices wizard automatically launches.

Adding devices

1. Go to **Device** > **Discovery** > **Add devices**.
2. Select an option, and then select **Next**.

Express

Find devices in the local network using predefined communication settings.

Custom

a. Select from the following discovery options:

Option	Actions
On your local network Scans all devices in the local network using IPv4 and IPv6 addresses in your domain.	Select from the following local network discovery types: • IPv4 • IPv6
By IP address Scans for the device using a specific address in your domain.	Select from the following methods: • Enter an IPv4 or IPv6 address or host name, and then select **Add** to include the entry in the Selected targets list. • Select **Import** to use an IP address list. To remove an IP address or host name from the Selected targets list, select the IP address or host name, and then select **Remove**.
By IP address range Scans all devices within the designated IP address range in your domain.	Enter a starting and ending IPv4 or IPv6 address, and then select **Add** to include the entry in the Selected network segments list. To remove an IP address range from the Selected network segments list, select the range, and then select **Remove**.

b. Configure Communication settings, and then select **Next**.

c. Set a recurring schedule for discovery, or select **Next** to start immediately.

3 Confirm the details, and then select **Finish**.

Scheduling automatic device discovery

Set up a regular schedule for performing the discovery process. If devices are frequently added to or removed from the network, performing discovery on a regular basis keeps the device database up to date.

1. Go to **Device** > **Discovery** > **Automatic Discovery**.
2. In the Scheduled Discovery dialog box, do any of the following:
   - To create a new discovery mode, select **Add**. Set up a recurring schedule, and then select **Finish**.
   - To remove a discovery schedule, select **Delete**.
   - To edit an existing discovery mode, select **Properties**. Set up a recurring schedule, and then select **Apply changes**.
3. Select **Close**.

Excluding a device from discovery

For security purposes, you can exclude devices from the discovery process to remove them from view. Information about the exclude device is not deleted from the application.

1. From any Device view or Accounting devices view, select a device to exclude.
2. Right-click the selected device, and then select **Delete device**.

To add a deleted device, go to **Device** > **Discovery** > **Show excluded devices**, select one or more entries, and then select **Include device**.

User interface

The user interface displays information about your network devices, device accounts, and host computers where the device drivers are installed.

Main Menu

The main menu is located at the top of the window. Basic operations that affect the application are in this menu.

Toolbar

Each view displays a toolbar below the main menu. The toolbar contains icons for the most common tasks for each view, including managing and editing devices, accounts, and hosts. Move your mouse cursor over each icon to view its corresponding task.

My Views

My Views are lists or maps you can create from Default Views or other My Views. Customize the type of information you want to see using My Views,

which are organized in a tree structure that displays folders and My Views nodes.

When you select a custom view under My Views, the application displays the view (list or map) in the other pane. Create folders to organize and manage My Views.

To add information to My Views, go to the View menu and select **Add Dynamic View** or **Add Manual View Using Selection**.

Default Views

Default Views are read-only standard list or map views. When you select a particular default view, the application displays the view (list or map) in the other pane. Some Device view options are only available from list views and not map views.

List or map view

A list of devices, accounts, or hosts displays on the window depending on the selected view. This customizable list provides information that you can organize. Expand each row in any Device list view to display more information. A Map view is also available and displays your devices on a custom map background.

Identifying status icons

In the device or host list view, status icons provide information about the condition of each device. Select the triangle icon to expand the row and see a description of the condition.

Customizing list views

Customize your view to arrange the information of a device, account, or host list view saved under My Views. After customizing you view, select **Update View**. Changes made to Default Views are not saved after you leave the view.

Administrator login

For some devices, administrator authentication is required to access selected features. Available features may vary depending on your device. When you select a feature from a menu, you may be prompted to enter one of the following:

- Command Center administrator password
- Administrator login and password (with optional Use local authentication)
- Accounting administrator code
- Model-specific authentication:

Model	User name	Password
MA2001w MA2000w PA2001w PA2000w	Admin	Enter the Write community name in **Device** > **Advanced** > **Device network settings** > **SNMP v1/v2c**. • The default Write community name is set to **public**. To ensure that your device is securely accessed, change this default name. • If you have modified the Write community name or other SNMP settings for one or more devices, make sure to review the SNMP settings for the devices in other driver or utility applications.

Operations on multiple devices do not prompt for administrator login. Login options must be configured in the Login section of the Communication Settings dialog box.

Options

Configure the following optional settings for the application:

Option	Description
Mail settings	Sets the mail server, authentication, and sender information
Authentication	Sets or change local password for users without administrator rights on a computer
Default device polling settings	Specifies default device polling settings for new devices at specific time intervals
Trap	Configures settings for the trap server
Default account polling settings	Specifies account counter polling settings for new devices
Log management settings	Sets a schedule for clearing audit logs
Proxy settings	Selects proxy server settings for communication with devices on remote network

Editing mail settings

1. Go to **Edit** > **Options**.
2. Select **Mail settings**.
3. Do the following:
   a. In Host, enter the SMTP (email) server name.
   b. In Port, enter the port number.
4. If necessary, select **Require authentication**, and then enter the login information.
5. Enter the sender name and email address.
6. To test device connection to the SMTP server, select **Test connection**.

   - If an error occurs, correct the host name and port number, and then repeat Test connection.
   - Test connection does not check the validity of the login information.

7. Select **OK**.

Editing authentication settings

To enable this setting, you must run the application as an administrator.

1. Go to **Edit** > **Options**.
2. Select **Authentication** > **Enable local password**.
3. Enter and confirm the password for a local user.
4. Select **OK**.

   You can still save a password that does not meet the minimum requirements.

Editing default device polling settings

This setting lets you set default polling settings for new devices.

Changing the default values does not affect the settings for previously added devices

1 Go to **Edit** > **Options**.

2 Select **Default device polling settings**.

3 Specify the time intervals for the following settings:

- Status polling
- Counter polling
- Toner level polling

4 Select **OK**.

Editing SNMP trap settings

The SNMP protocol provides and transfers management information within the network environment. If an error occurs, the device automatically generates a trap, and then sends an error message to predetermined trap recipients.

The trap server is the SNMP trap packet receiver which runs in the application. To receive trap packets, start the trap server, and then configure the SNMP trap on the device

TCP port 162 must be available and not blocked by a firewall.

1 Go to **Edit** > **Options**.

2 Select **Trap**.

3 Do either of the following:

- If the trap server is not running, then select **Start**.

  If server connection fails, then check the application log file for an error message. Resolve the error, and then restart the trap server.

- If the trap server is running, then select **Stop**.

4 Enter a trap community name.

This allows the receipt of SNMP trap packets with the same community name as the trap community stored in the application.

5 If necessary, select **Automatically run trap server when the program starts**.

6 Select **OK**.

Editing default account polling settings

1 Go to **Edit** > **Options**.

2 Select **Default account polling settings**.

3 Select **Default account counter polling for new devices**, and then do the following:

a) For **Account counter polling interval**, set a recurring schedule for polling information.

b) Select a warning level.

4 Select **OK**.

Editing log management settings

1 Go to **Edit** > **Options**.

2 Select **Log management settings**.

3 Specify the log storage period.

4 If necessary, select **Export the log records before clearing them**, and then specify a folder location.

5 Select **OK**.

To view a list of saved log records, go to **File** > **Open and audit the log records**.

Editing proxy settings

1 Go to **Edit** > **Options**.

2 Select **Proxy Settings** > **On**.

3 For each protocol to be used, enter the proxy address and port number.

4 If the server requires authentication, then select **Require authentication**. Specify the login information.

5 If you do not want to use a proxy server for specific domains, then specify the domain names in Do not use proxy for following domains.

Separate domain names using semicolons.

6 Select **OK**.

Viewing audit log records

Audit logs are created and saved automatically each time you run the application or modify authentication options.

1. Go to **File** > **Open and audit the log records**.
2. Do any of the following:
   - To change the sorting order, select the column headers.
   - Search for a specific audit log.
   - To save the audit log records as a .csv file, select **Export**.
   - To update the list, select **Refresh**.
3. Select **Close**.

To configure audit log storage, go to **Edit** > **Options** > **Log management settings**.

3 View

The application offers the following views:

View	Description
My Views	You can create, change, or delete custom views.
Default Views	Includes the following read-only views: • Device • Accounting • Host You can customize the appearance of the lists, but changes are not saved after you leave the view.

In any device view, you can switch between view types by selecting **View as**.

My Views

Set up custom views and organize items in folders. In My Views, customize the devices, accounts, or hosts being displayed, as well as column order, number of columns, and other view settings. Save changes after modifying a view using Update view. Select the Manage views icon in My Views to open a menu for more options.

Adding custom views

Create and save a customized view of selected devices, accounts, or hosts. You can add custom views from any of the following view types:

Device

General, Capability, Counter, Firmware, Asset, Map

Accounting

Accounting Devices, Accounts

Host

Hosts, Host driver, Host Queue

1 Depending on your preferred view, do the following:

Option	Actions
Dynamic View A dynamic view is a copy of a default or custom view that you create in My Views. A dynamic view cannot be created when a manual view is selected in My Views.	**a.** From My Views or Default Views, select any view. **b.** Modify the view. You can change the order of columns, and show or hide columns. **c.** Select **Add dynamic view**.
Manual View A manual view is a custom view that includes devices, accounts, or hosts selected from an existing view. Advanced Search is not available for a manual view.	**a.** From any view, select one or more devices, accounts, or hosts. **b.** Select **Add manual view using selection**.

2 Specify the view name, and then press **Enter**.

For existing manual views, you can add another device, account, or host, by selecting and moving it from another view.

Adding a new folder

1 Go to **File** > **New folder**.

2 Specify a folder name, and then press **Enter**.

Renaming a folder or view

1 In My Views, right-click a folder or view, and then select **Rename**.

2 Specify the new name, and then press **Enter**.

Removing a device, account, or host

Remove a device, account, or host so that it does not appear in a custom view. This does not delete the item from the database.

1. From My Views, select a manual view.
2. Select one or more devices, accounts, or hosts to be removed from the view.
3. Select **Edit** > **Remove from view**.

> There is no confirmation dialog box after selecting Remove from view.

Updating and saving a view

When any view in My Views changes, an asterisk displays after its name in the title bar until it is saved.

Use Update view after you do any of the following:

- Changing the column width, column order, adding or removing columns.
- Using **View** > **View as** to change the view type.
- Sorting the information in list columns.

If you switch to another view without updating a view, then any changes are not saved.

1. After making changes in a view, go to **View**.
2. Select **Update view**.

Duplicating a view

1. In My Views, right-click a view to be copied, and then select **Duplicate**.
2. Specify the view name, and then press **Enter**.
3. Modify the new view as needed.

Deleting a view

1. In My Views, select the view to be deleted.
2. Select **Edit** > **Delete**.

> - There is no confirmation dialog box after selecting Delete.
> - A deleted view cannot be restored.
> - Default views cannot be deleted.

Default Views

The application provides standard views in Default Views that cannot be removed or edited.

In any view except Map View, you can temporarily add or remove columns. The modified views are not saved when you switch to a different view.

Device

General View

Displays general information, such as display name, host name, and model name.

Capability View

Displays support for various device capabilities, such as duplex, total memory, and job log.

Counter View

Displays the device counters for jobs, such as total printed pages, total scanned pages, and fax printed pages.

Firmware View

Displays device firmware information, such as system firmware, engine firmware, and scanner firmware.

Asset View

Displays asset information, including MAC address, serial number, and asset number.

Map View

Displays device icons on a background image that you can customize, for example, a floor plan of your office.

Accounting

Accounting Devices View

Displays general information and counters for devices that support accounting.

Accounts View

Displays account information for managed devices, such as counter totals for copy, fax, and scan.

Host

Host View

Displays general information about network host computers.

Host Driver View

Displays printer drivers installed on host computers.

Host queue view

Displays the device queues of host computers.

Customizing map views

With any map view in My Views or Default Views, you can add a background image, for example, a floor plan of your office. You can then arrange managed devices accordingly, and resize the map view.

1. In My Views or Default Views, select a map view.
2. Right-click the map background, and then select any of the following:

Option	Actions
Import map background Import an image, and then move each device icon to a preferred location. The map is shared by all map views in the current workspace.	Browse for the preferred image file (.bmp or .jpg), and then select **OK**.
Zoom in, Zoom out, Zoom to fit Adjust the size of the map. Changing the screen size of the application does not change the size of the map.	Do any of the following: • Select **Zoom in** or **Zoom out** to change the size of the image by a fixed interval. • Select **Zoom to fit** to place the entire image within the screen. • Specify a percentage value between 50% and 300%, and then press **Enter**.
Clear map background Delete the background image. All device icons retain their position.	There is no confirmation dialog box after you select this option.

Zoom in, Zoom out, Zoom to fit, and Clear map background are available only if the map view has a map background.

Exporting view, list, and device information

Export information about devices from various view options to .xml or .csv files.

1. From any view, go to **File** > **Export**, and then select from the following:
   - **View**
   - **List**
   - **Devices**

Options may vary depending on your view.

2 Complete the export details:

- File location
- File name
- File type

The .csv export uses UTF-8 encoding.

3 Select **Save**.

Each export option provides different information. Review the results for each type.

Updating views

Device and host information are automatically updated according to the polling schedules. At any time, you can manually update this information for one or more devices.

1 From any host or device view, select one or more hosts or devices.

2 Right-click your selection, and then select **Refresh**.

This option is not available in any account view.

To refresh all items in a host or device view, go to **View** > **Refresh all**.

Creating and exporting a folder report

After creating a folder in My Views and adding custom views from Accounting Devices View or Accounts View, you can create and export an accounts or accounting devices folder report.

Accounts folder report

This report can be created if the folder contains at least one Accounts view. Only the accounts selected in the Accounts Folder Report dialog box are included in the exported report.

Accounting Devices Folder Report

This report can be created if the folder contains at least one Accounting devices view. Only the devices selected in the Accounting Devices Folder Report dialog box are included in the exported report.

Once a folder report is created, it can be exported to a .csv or .xml file.

1 Right-click a folder in My Views, and then select **Folder report**.

2 Select **Accounts** or **Accounting Devices**, and then select one or more accounts or devices to be included in the report.

3 Select **Export**.

4 Complete the export details:

- File location
- File name
- File type

5 Select **Close**.

Searches

The following options are available for finding devices, accounts, or hosts with particular characteristics.

- Search finds data in the currently displayed view. Entries are not saved when you move one view to another.
- Advanced Search finds all devices, accounts, or hosts in the database for the values selected in the search dialog box.

Finding information with search

Search can find exact matches for full or partial terms in the following columns or in Map View:

Device search

Display name, IP Address, Host name, Model name

Account search

Account ID

Host search

Host name, Driver name, Queue name, IP Address, OS Information

Search includes the columns if they have been removed from view. The results are not saved when you move from one view to another, or perform an Advanced Search. Search does not include the expanded information area.

1 Enter an alphanumeric search term in the text box.

As you type, the search examines the data of all the devices, accounts, or hosts in the original view.

2 To clear the search term, select the icon next to the Search text box.

This removes any text in the text box, and restores the view to the original list of devices, accounts, or hosts before the search.

Finding information with advanced search

Use the Advanced Search feature to find all devices, accounts, or hosts in the database that match your selected criteria. The results are displayed until you change to another view or perform another search.

1. In Default Views, select a view.

   Advanced search is not available for Host driver view and Host queue view.

2. Go to **Edit** > **Advanced search**.

3. In the Advanced Search dialog box, select a search logic:

   Match all criteria

   This option searches for devices, accounts, or hosts that meet all the search terms specified in Criteria.

   Match any criteria

   This option searches for devices, accounts, or hosts that meet at least one of the search terms specified in Criteria.

4. In Criteria, select features or properties to find in the search.

   Property

   Select one property per property list. There are six property lists available. Properties may vary depending on your device.

   Condition

   Available conditions depend on the selected property.

   Value

   Type or select a value in the box.

5. Select **OK**.

The application searches through all devices, accounts, or hosts and displays those that match the selected criteria. In Map View, the search result devices appear in their saved position in the office map.

4 Device

Manage devices on your network.

For more information about device features, see the device *Operation Guide*. For more information about driver features, see the *Printer Driver User Guide*.

Displaying device properties

View settings and status information about the selected device.

1 From any device view, right-click a device, and then select **Properties**.

The following settings appear:

Depending on your device, some options may vary and may require device login.

Basic device settings

This area shows the display name, model, status, IP address, host name, location, and description of the device. The Panel message box shows the information currently displayed on the device operation panel. You can edit the display name, location, and description of the device.

Device alert

This area describes alerts that are currently occurring, and any troubleshooting measures that can be taken.

Media input

This area shows the trays and cassettes that are currently installed, their capacity, and roughly how much paper they currently contain.

Capabilities

This area shows some of the key specifications of the currently selected device.

Counters

This area shows a variety of counters for different types of paper or media and output.

Firmware versions

This area lists the versions of firmware for various parts of the system.

System firmware (details)

This area shows the versions of controller firmware installed on your selected device.

Memory

This area shows the capacity and usage of each supported storage device.

Asset

This area shows the MAC address of the network adapter in the device, the Serial number of the device itself, and the Asset number which may be assigned by your organization.

Wi-Fi

This area shows the details of wireless network connection, if a wireless network card is installed on your selected wireless-enabled device.

Trusted Platform Module (TPM)

This area shows the device status, manufacturer name, manufacturer version, and specification version.

Card reader

This area shows the firmware and application versions, if a card reader is installed on your device.

Maintenance Kit

This area shows the usage levels of any maintenance kit that is supported by your device.

Allowlisting

This area shows the allowlisting status of your device.

2 Select **Refresh** to update any settings that might have been changed on the device while this dialog box was open.

Displaying device home page

View the home page of a device with an embedded web server. The device home page contains information about the current status and settings of the device.

The layout and information in the home page may vary depending on your device.

From any device view, select a device, and then go to **Device** > **Device home page**.

Device properties reports

Manage reports that provide detailed information about devices in the current device view in My Views. You can send the reports to multiple recipients, and can be scheduled for a specified time and day.

The report contains the same device information that is shown in the selected view. Each view can only have one device properties report, and a total of five reports can be created for all device views.

The device properties report has a user-specified name, and can be sent to the email addresses specified in a list. You can schedule the reports to be sent daily, weekly, or monthly. You can also add a user-specified message in the email subject line.

You can create .xml or .csv reports.

- This feature is not available in map view.
- This feature requires mail settings to be set in Options.

Creating a device properties report

- You can only create device properties report in My Views.
- This feature requires mail settings to be set in Options.

1. From My Views, select a device view, and then go to **Device** > **Add device properties report**.
2. Change the default settings as needed.
3. Select **OK**.

Viewing and changing device properties report settings

1. From My Views, select a device view, and then go to **Device** > **Show device properties reports**.
2. Select a report, and then select **Properties**.
3. In Edit Device Properties Report, modify the settings as needed.
4. Select **OK**.

Managing certificates

Import and delete device and root certificates to one or more devices, and assign device certificates to protocols.

The following certificates can be installed:

Device certificate

A file that identifies the device.

Root certificate

A file the device uses for secure communication. Some applications can also use a root certificate as a server certificate.

Managing certificates on one device

When managing certificates on one device, you can view the details of the certificates added on the device.

Importing a certificate on one device

You can only import on an inactive certificate.

1. From any device view, select a device, and then go to **Device** > **Certificates**.
   You may be required to provide login information.
2. Select **Import certificate**.
3. Do either of the following:

Option	Actions
Import a device certificate	**a.** In the Certificate menu, select **Device certificate**. **b.** If necessary, in the Installation area menu, select a certificate number. To use the default active certificate, select **Auto (Default)**. **c.** In Certificate file, select **Browse** to specify the certificate to import. **d.** In the Password field, enter a password for the certificate. **e.** Select **OK**.
Import a root certificate	**a.** In the Certificate menu, select **Root certificate**. **b.** If necessary, in the Installation area menu, select a certificate number. To use the default active certificate, select **Auto (Default)**. **c.** In Certificate file, select **Browse** to specify for the certificate to import. **d.** Select **OK**.

4. Select **OK**.
   The device network restarts automatically after processing is finished. The processing page shows you the status of certificate processing. Processing may take several minutes.

After processing completes, the Certificates screen refreshes. If an error occurs, then select **Export** to view a detailed result log.

Assigning a device certificate to protocols on one device

You can only assign an active device certificate to protocols.

1. From any device view, select a device, and then go to **Device** > **Certificates**.
   You may be required to provide login information.
2. Right-click an active device certificate, and then select **Assign device certificate to protocols**.
3. In the Protocols list, select one or more protocols, and then select **OK**.

   Clear previously selected protocols to remove them.

4. Select **OK**.
   The device network restarts automatically after processing is finished. The processing page shows you the status of certificate processing. Processing may take several minutes.

After processing completes, the Certificates screen refreshes. If an error occurs, then select **Export** to view a detailed result log.

Deleting a certificate on one device

You can only delete active certificates.

1. From any device view, select a device, and then go to **Device** > **Certificates**.
   You may be required to provide login information.
2. Right-click an active certificate, select **Delete certificate**, and then select **Next**.
3. Select **Yes** > **OK**.
   The device network restarts automatically after processing is finished. The processing page shows you the status of certificate processing. Processing may take several minutes.

After processing completes, the Certificates screen refreshes, and then the selected certificate is set to **Inactive**. If an error occurs, then select **Export** to view a detailed result log.

Viewing certificate details

You can only view the details of active certificates.

1. Select a device, and then go to **Device** > **Certificates**.
   You may be required to provide login information.
2. Right-click an active certificate, and then select **View certificate**.
3. Select **OK**.

Retrieving certificates for one device through SCEP

You can import secondary device certificates for a device from a defined Certificate Authority (CA) through Simple Certificate Enrollment Protocol (SCEP). For more information on SCEP settings, contact your system administrator.

This feature is available only for inactive Device Certificates 2, 3, 4, and 5 in some devices.

1. From any device view, select a device, and then go to **Device** > **Certificates**.
   You may be required to provide login information.
2. Right-click an inactive secondary device certificate, and then select **Retrieve certificate via SCEP**.
3. Review or modify the SCEP server settings, and then enter the required CSR settings.
4. Select **Enroll**.
   After the importing finishes, review the status of the certificate.

To view or modify any of the available SCEP settings for individual devices, in Certificates, right-click the secondary device certificate, and then select **Auto import settings**.

- Auto import settings may vary depending on the status of the device certificate.
- This option is available only for individual device certificates that have been retrieved through SCEP.

Managing certificates on multiple devices

You cannot view certificates when managing multiple devices. To view certificates on a device, you need to manage the devices individually.

Importing a certificate on multiple devices

1. From any device view, select multiple devices, and then go to **Device** > **Advanced** > **Manage certificates**.
   You may be required to provide login information.
2. Select **Import certificate** > **Next**.
3. Do either of the following:

Option	Actions
Import device certificate	a. Select **Device certificate** > **Next**. b. Specify the .csv file containing the configuration, and then the .zip file containing the certificate files. If necessary, select **Assign device certificates to protocols** to assign the certificates to available device protocols. c. Select **Next**. d. If Assign device certificates to protocols is selected, then add one or more protocols, and then select **Next**.
Import root certificate	a. Select **Root certificate** > **Next**. b. Specify the certificate to import. c. Select **Next**.

4 Review your settings, and then select **Finish**.

5 Select **OK**.
The device network restarts automatically after processing is finished. The processing page shows you the status of certificate processing. Processing may take several minutes.

After processing completes, select **Export** to view a detailed result log.

Assigning a device certificate to protocols on multiple devices

1 From any device view, select multiple devices, and then go to **Device** > **Advanced** > **Manage certificates**.
You may be required to provide login information.

2 Select **Assign device certificate to protocols** > **Next**.

3 Do either of the following:

Option	Actions
Specify subject of the certificate	a. Type the subject of the certificate as a distinguished name (DN). b. Select **Next**.

Option	Actions
Select certificate file	**a.** Specify the certificate file. **b.** If the selected certificate file requires a password, then enter the certificate password, and then select **Next**.

4 In Choose protocols, select a protocol, and then add it to Selected protocols.
If necessary, repeat this step to add more protocols.

5 Select **Next**.

6 Review your settings, and then select **Finish**.

7 Select **OK**.
The device network restarts automatically after processing is finished. The processing page shows you the status of certificate processing. Processing may take several minutes.

After processing completes, select **Export** to view a detailed result log

Deleting a certificate on multiple devices

1 From any device view, select multiple devices, and then go to **Device** > **Advanced** > **Manage certificates**.
You may be required to provide login information.

2 Select **Delete certificate** > **Next**.

3 Select either **Device certificate** or **Root certificate**, and then select **Next**.

4 Do either of the following:

Option	Actions
Specify subject of the certificate	**a.** Type the subject of the certificate as a distinguished name (DN). **b.** Select **Next**.
Select certificate file	• For device certificates **a.** Specify the certificate file. **b.** If the selected certificate file requires a password, then enter the certificate password, and then select **Next**. • For root certificates **a.** Specify the certificate file. **b.** Select **Next**.

5 Review your settings, and then select **Finish**.

6 Select **OK**.
The device network restarts automatically after processing is finished. The processing page shows you the status of certificate processing. Processing may take several minutes.

After processing completes, select **Export** to view a detailed result log.

Retrieving certificates for multiple devices through SCEP

You can import secondary device certificates for two or more devices from a defined Certificate Authority (CA) through Simple Certificate Enrollment Protocol (SCEP). For more information on SCEP settings, contact your system administrator.

This feature is available only for inactive Device Certificates 2, 3, 4, and 5 in some devices.

1 From any device view, select multiple devices, and then go to **Device** > **Advanced** > **Manage certificates**.
You may be required to provide login information.

2 Select **Retrieve certificate via SCEP** > **Next**.

3 Select a secondary device certificate that is inactive for all devices.

4 Review or modify the SCEP server settings, and then enter the required CSR settings.

5 Select **Enroll**, then do any of the following:

- To review or modify the settings, select **Back**.
- To continue, select **Finish**.
- To exit the operation without saving the settings, select **Cancel**.

6 After importing finishes, review the results for each device.
To save the results to a file, select **Export**. To continue, select **Close**.

To view or modify any of the available SCEP settings for individual devices, in Certificates, right-click the secondary device certificate, and then select **Auto import settings**.

- Auto import settings may vary depending on the status of the device certificate.
- This option is available only for individual device certificates that have been retrieved through SCEP.

Address book

Manage the Address Book which contains a list of individuals and their contact information that is stored on the device. Each entry for an individual is called a contact, and contacts can be organized into groups. This contact and group information is stored on the device, and is used for faxing and scanning operations.

Adding a contact

1. From any device view, select a device, and then go to **Device** > **Address book**. You may be required to provide login information.
2. Select **Add contact**.
3. From Contact Settings, select a number for the contact.

   To use the next available number, select **Auto**.

4. In the Name text box, type a name for the contact.
5. Modify additional settings for the new contact.

   Options may vary depending on your device.

   Cover page
   Cover page information of the contact.

   Email
   Enter email address for the contact.

   FTP
   Enter information and settings for FTP shared folders.

   SMB
   Enter information and settings for SMB shared folders

   FAX
   Enter fax information and settings for the contact.

   Internet FAX
   Enter internet fax information and settings for the contact.

6. Select **OK**.

To edit, select a contact, and then select **Properties**. Modify the settings as needed, and then select **OK**.

To delete, select a contact, and then select **Delete** > **Yes**.

Adding a group

Organize contacts into groups. This feature is useful when the device sends out notifications of certain types of events.

1. From any device view, select a device, and then go to **Device** > **Address book**. You may be required to provide login information.

2 Select **Add group**.

3 In Group Settings, enter a name for the group.

4 Select a number for the group.

To use the next available number, select **Auto**.

5 Select **OK**.

To edit, select a group, and then select **Properties**. Modify the settings as needed, and then select **OK**.

To delete, select a group, and then select **Delete** > **Yes**.

Adding a contact to a group

Each step requires communication with the device, which may be slow depending on network condition.

1 From any device view, select a device, and then go to **Device** > **Address book**.
You may be required to provide login information.

2 Select a group, and then select **Properties**.

3 In Group Settings, select **Add members**.
The contact list is downloaded from the device, and then displays it in the dialog box.

4 In Add Group Members, select one or more contacts, and then select **Add**.

5 Select **OK** in all dialog boxes.

To remove contacts from a group, select one or more contacts, and then select **Remove members**.

One touch keys

You can access Address Book entries for contacts or groups by pressing one key on the device operation panel.

- The number of One Touch keys that can be created varies depending on your device.
- This feature is available only on some devices.

Adding a one touch key

1 From any device view, select a device, and then go to **Device** > **Address book**.

You may be required to provide login information.

2 Select **Show One Touch keys**.

3 In One Touch Key, select **Add One Touch key**.

4 In Add One Touch Key, specify a key name, and then select a number from 1 to 1000.

- If the key name is not specified, then the contact name is used.
- To automatically select the next available number, select **Auto**.
- The maximum number varies depending on your device.

5 Select **Add destination**, and then in One Touch Key Destination, select a contact or group.

6 Select **OK** in all dialog boxes.

To delete, select a One Touch key entry, and then select **Delete One Touch key**.

Viewing and editing one touch key properties

1 From any device view, select a device, and then go to **Device** > **Address book**.
You may be required to provide login information.

2 Select **Show One Touch keys**.

3 In One Touch Key, select a key entry, and then select **One Touch key properties**.

4 In One Touch Key Properties, select **Edit destination**, and then modify the settings as needed.

5 Select **OK** in all dialog boxes.

Searching one touch keys

You can search One Touch keys when searching for key entries or when editing a key destination.

1 From any device view, select a device, and then go to **Device** > **Address book**.
You may be required to provide login information.

2 Select **Show One Touch keys**.

3 In Searchable fields, select one of the following options:

- **Number**
- **Address number**
- **Address type**
- **Name**
- **Destination**

Depending on the contact type, this can be an email address or folder location. This option is available only when editing One Touch Key destinations.

4 In Search text box, type the text you want to find.

To clear the search results and display the list again, on the toolbar, select **Clear search**.

Copying contacts and groups

1 From any device view, select a device, and then go to **Device** > **Address book**. You may be required to provide login information.

2 Select a contact or group, and then select **Copy**.

3 Select **Paste**.

4 If necessary, modify the new contact or group settings.

5 Select **Close**.

Exporting an address book list

Export contacts, groups and One Touch lists to a .csv or .xml file. You can import the exported list to the Multi-Set feature.

1 From any device view, select a device, and then go to **Device** > **Address book**. You may be required to provide login information.

2 Select **Export**.

3 Enter a file name, and then save the file.

Searching the address book

1 From any device view, select a device, and then go to **Device** > **Address book**. You may be required to provide login information.

2 In the Searchable fields menu, select one of the following options:

Options may vary depending on your device.

Number

The unique number assigned to the contact.

Name

The name of the contact.

Email

The email address of the contact.

FTP

The host name of the FTP folder.

SMB

The host name of the SMB folder.

FAX number

The fax number of the contact.

Internet FAX address

The internet fax address of the contact.

3 In Search text box, type the text you want to find.

To clear the search results and display the list again, on the toolbar, select **Clear search**.

Managing S/MIME certificates

S/MIME certificates allow you to encrypt your emails.

The S/MIME certificate option is available only for individual address book contacts with email addresses.

1 To access the S/MIME certificate option, make sure to unblock S/MIME by doing the following:

a) From any device view, select a device, then go to **Device** > **Advanced** > **Device network settings**.

b) Go to **Protocol settings**, then make sure that **SMTP (Email TX)** is unblocked. If necessary, modify the setting, then select **Apply**.

c) Make sure that **S/MIME** is unblocked. If necessary, modify the setting, then select **Apply**.

d) Select **OK**.

2 From any device view, select a device, then go to **Device** > **Address Book**.

You may be required to provide login information.

3 Right-click a contact with an email address, and then select **S/MIME certificate**.

4 Select a certificate from the list, then select any of the following options:

- To update the list, select **Refresh**.

- Some options may be available depending on the certificate status.

Import certificate

Specify the certificate installation target and browse for the appropriate S/MIME certificate.

Delete certificate

Remove the selected certificate from the list.

View certificate

View the contents of the selected certificate.

Device users

Manage the login information for users on the device.

- If user authentication is set, then only users who have administrative rights are able to use the functions of the device.
- To access the user list of a device, the correct login information must be set in the Communication Settings for the device. If an administrator password is set for the device, then only an administrator can change the user list.

Adding device users

1. From any device view, select a device, and then go to **Device** > **Users**.
   You may be required to provide login information.
2. Select **Add user**.
3. In Add user, enter the login information.
4. Choose **Select** to set an account ID.
5. If necessary, select **Allow administrator access** to give the user administrative access on the device.

   Clear the check box to give the user default user access.
6. Select **Advanced**, and then specify a language and default screen.

   The Application option in Default screen is available only if more than one application is installed in your device.
7. Depending on your selected default screen, configure the following:

Default screen for Send/FAX

Select the default operation panel screen that is displayed when you select **Device System Settings** > **Send Settings** on the device.

Default address book

Select the local address book or an external address book for the user.

Default screen for Favorites/Application

Select the default operation panel screen that displays when you select **Device System Settings** > **Program/Favorites (or Application)** on the device.

Default application

Select the application that displays when a user first logs on to the physical device.

8 In ID card information, specify the unique ID card for the user.

This option is available only if a card authentication kit is installed on your device.

9 In Authorization, set permissions for each available feature.

10 Select **OK**.

To edit user information, select a user, and then select **Properties**. Modify the settings as needed, and then select **OK**.

To delete, select a user, and then select **Delete user** > **Yes**.

Exporting a device user list

You can export to a .csv or .xml file.

1 From any device view, select a device, and then go to **Device** > **Users**.
You may be required to provide login information.

2 Select **Export Users**.

3 Select **Yes** to export all users, or select **No** to export selected users.

4 Enter a file name, and then save the file.

Searching the device user list

1 From any device view, select a device, and then go to **Device** > **Users**.
You may be required to provide login information.

2 In the Searchable fields menu, select the type you want to find.

3 In the Search text box, enter the text to find.

To clear the search results and display the entire list again, select **Clear search**.

Setting a simple login key

This feature is available only in some devices.

1 From any device view, select a device, and then go to **Device** > **Users**.
You may be required to provide login information.

2 Select **Show Simple Login keys**.

3 In Simple Login Keys, select **Add Simple Login key**.

4 Select an icon, and then enter a name.

5 In the Key text box, select a specific number from 1 to 20, or select **Next available number** to set the number automatically.

6 Select either of the following authentication modes:

Use local authentication

Use available device user login information. Choose **Select from user list**, select a user, and then select **OK**.

Use network authentication

Use network user login information. Enter network login user name and password.

7 If necessary, in Password login, select **On** to require password login, or select **Off** to disable the password requirement.

8 Select **Add**.

To edit, select a simple login key, and then select **Simple Login key properties**. Modify the settings as needed, and then select **OK**.

To delete, select a simple login key, and then select **Delete Simple Login key** > **Yes**.

Searching the simple login key list

1 From any device view, select a device, and then go to **Device** > **Users**.
You may be required to provide login information.

2 Select **Show Simple Login keys**.

3 In the Searchable fields menu, select the type you want to find.

4 In the Search text box, enter the text to find.

To clear the search results and display the entire list again, select **Clear search**.

Jobs

Manage jobs that are currently in the queue for the device, and job logs that contain information about recent jobs that were processed.

Viewing job details

1 From any device view, select a device, and then go to **Device** > **Jobs**.
You may be required to provide login information.

2 Select **View as**, and select one of the following job status or log:

- **Print job status**
- **Send job status**
- **Store job status**
- **Scheduled job status**
- **Print job log**
- **Send job log**
- **Store job log**

3 In the job list, select a job, and then select **Properties**.

4 Review the job information.

Information may vary depending on the type of job selected.

5 Select **Close**.

To cancel one or more jobs, in the list, select one or more jobs, and then select **Cancel job**.

Exporting the job log

1 From any device view, select a device, and then go to **Device** > **Jobs**.
You may be required to provide login information.

2 Select **Export**, and then select a job log.

3 Specify the file name, and the location where to save the file.

4 In the Maximum entries menu, enter the number of lines to save in the log.

5 Select **OK**.

Searching a job list

1. From any device view, select a device, and then go to **Device** > **Jobs**.
   You may be required to provide login information.
2. In the Searchable fields menu, select the type you want to find.
3. In the Search text box, enter the text to find.

   To clear search results and display the entire list again, select **Clear search**.

Stored jobs

View, print, or delete Temporary and Permanent print jobs stored in the device hard disk.

To view stored jobs, from any device view, select a device, and then go to **Device** > **Stored Jobs**.

To refresh the list, select **Refresh**.

This feature is available only for some devices with a hard disk installed.

Printing stored jobs

1. From any device view, select a device, and then go to **Device** > **Stored Jobs**.
   You may be required to provide login information.
2. From the list, select a job, and then select **Print** > **Print selected jobs** > **Yes**.

Printing a stored job list

1. From any device view, select a device, and then go to **Device** > **Stored Jobs**.
   You may be required to provide login information.
2. Select **Print**, and then select either of the following:
   - **Print temporary job list**
   - **Print permanent job list**

Deleting stored jobs

1. From any device view, select a device, and then go to **Device** > **Stored Jobs**.
   You may be required to provide login information.
2. Select **Delete**, and then select one of the following options:
   - **Delete selected jobs**

- **Delete temporary jobs**
- **Delete permanent jobs**
- **Delete all jobs**

3 Select **Yes**.

Searching stored jobs

1 From any device view, select a device, and then go to **Device** > **Stored Jobs**.
You may be required to provide login information.

2 In the Searchable fields menu, select the type you want to find.

3 In the Search text box, enter the text to find.

To clear the search results and display the entire list again, select **Clear search**.

Document box

Manage the Document Box on the device. This is used by individuals and groups to manage files that are stored on the device.

- If authentication is set, then accessing the document box requires the correct login information in the Communication Settings for the device.
- If authentication is not set, then the login dialog box may appear depending on your device.

Adding a document box

1 From any device view, select a device, and then go to **Device** > **Document box**.
You may be required to provide login information.

2 Select **Add box**.

The number of document boxes that you can create may vary depending on your device.

3 From the Add Box dialog box, enter the name for the new box.

The default box type is Custom box. Some devices also support a fax box or Subaddress box for receiving faxes.

4 Enter a password to create a password-protected document box.

5 Configure the following settings:

Settings and information displayed may vary depending on your device.

Name

Enter the name for the box.

Type

View the type of document box.

Number

Select an available box number.

Owner

Select a new owner from the list. This option is available only if Owner setting is enabled.

Owner setting

Select the following owner type:

- **Off**
- **Local user**
- **Network user**

Domain

Select from the list of available domains.

Usage

View the current usage of the box.

Restrict usage (MB)

Restrict usage of the device from 1 to 30,000 MB.

Automatically delete files delay (days)

Set the number of days to save a file in the device memory, from 1 to 31 days.

Shared

Select to enable multiple users to use the box.

Password change

Enter a new password for the box.

Overwrite setting

If selected, then a new document replaces the existing document with the same name.

Sub address

View sub address of the box.

This setting is available only for subaddress boxes.

Delete after printed

Select to permanently remove the document from the box after printing it.

6 Select **OK**.

To edit, select a document box, and then select **Box properties**. Modify the settings as needed, and then select **OK**.

To delete, select a document box, and then select **Delete box**.

Exporting a document box list

You can use the exported file to import settings through the Multi-Set feature.

1 From any device view, select a device, and then go to **Device** > **Document box**.

You may be required to provide login information.

2 Select a box from the list.

3 Select **Export**, and then select a file format for the exported file.

Multi-Set and KX Driver export formats are not available for FAX or Subaddress boxes.

4 Select **Yes** to export all boxes, or **No** to export selected boxes.

Custom boxes with passwords are not exported when you select either Multi-Set export format.

5 Name and save the file.

Viewing document properties

1 From any device view, select a device, and then go to **Device** > **Document box**.

You may be required to provide login information.

2 Under Custom box, select a document box.

3 Select the document, and then select **Document properties**.

4 Select **OK**.

Viewing a document

1. From any device view, select a device, and then go to **Device** > **Document box**.
   You may be required to provide login information.
2. Select a document box, and then select **View**.
3. Select one or more of the following:

   Options may vary depending on your device.

   Thumbnail
   Display a thumbnail image of the document.

   Preview pane
   Display a preview of the document contents.

Downloading a document

1. From any device view, select a device, and then go to **Device** > **Document box**.
   You may be required to provide login information.
2. In Custom box, select a document box.
3. Select a document, and then select **Download document**.
4. In the file to field, specify the location where to save the file.
5. Enter a file name, and then select a file type.
6. Select **Save**.

Searching a document box

1. From any device view, select a device, and then go to **Device** > **Document box**.
   You may be required to provide login information.
2. In the Searchable fields menu, select what type to find.
3. In the Search text box, enter the text to find.

   To clear the search results and display the entire list again, select **Clear search**.

Moving documents to another box

1. From any device view, select a device, and then go to **Device** > **Document box**.

   You may be required to provide login information.
2. In Custom box, select the document box containing the file to move.
3. Select one or more files, and then move the documents to the destination document box.
4. Select **Yes**.

Virtual mailbox

Manage the mailboxes created on the hard disk of the device.

This feature is available only in some devices with a hard disk installed.

Adding a virtual mailbox

1. From any device view, select a device, and then go to **Device** > **Virtual mailboxes**.
2. Select **New mailbox**.
3. Enter an ID, name, and password for the mailbox.

   Use a unique name for the mailbox.
4. Select **OK**.

To edit, select a mailbox, and then select **Mailbox properties**. Modify the settings, and then select **OK**.

To delete, select a mailbox, and then select **Delete mailbox** > **Yes**.

If a password is set, then enter the correct password.

Searching virtual mailboxes

1. From any device view, select a device, and then go to **Device** > **Virtual mailboxes**.
2. In the Searchable fields menu, select what type to find.
3. In the Search text box, enter the text to find.

To clear the search results and display the entire list again, select **Clear search**.

Exporting a virtual mailbox list

1. From any device view, select a device, and then go to **Device** > **Virtual mailboxes**.
2. Select a virtual mailbox, and then on the toolbar, select **Export list**.
3. Complete the export details.

You can import the exported file to a printer driver.

Setting advanced virtual mailbox options

1. From any device view, select a device, and then go to **Device** > **Virtual mailboxes**.
2. Select a mailbox, and then select **Advanced**.
3. If a password has been set, enter the correct password, and then select **OK**.
4. Modify the following settings as needed:

   Maximum VMB size

   Set the size of the mailbox from 0 to 9999 MB. Set the value to **0** to prevent usage of the mailbox.

   Change master password

   Set a numerical value from 1 to 65535. This password is used to override or change the current mailbox password. To remove the password, clear the New password and Confirm new password text boxes.

   Delete all virtual mailboxes

   Erase all virtual mailbox data from the hard disk. Select **Delete all** > **Yes**.
5. Select **OK** > **Close**.

Device applications

Manage applications on one or more devices remotely. Available features may vary depending on your device.

Before you install, activate, deactivate, or uninstall an application, do the following:

- Enable TLS and IPP over TLS on the device.
- For some devices, enable enhanced WSD over TLS.

- Enter the correct login information in the Communication Settings for the device.

Applications are created by dealers or third-party companies to enhance printing, copying or accounting features.

Managing applications on one device

Manage applications remotely on one device using the Manage Applications wizard.

Installing applications on one device

1. From any device view, select a device, and then go to **Device** > **Applications**. You may be required to provide login information.
2. From the toolbar, select **Install New**.
3. Browse to find a valid application package file (.pkg), then select **Open** > **Yes**.

Activating installed applications on one device

1. From any device view, select a device, and then go to **Device** > **Applications**. You may be required to provide login information.
2. Select the application, and then select **Activate**.
3. In License Key Settings, select either of the following:

   Activate without a license key

   Select this option if the application does not require a license key.

   Use the following license key

   Enter a valid 20-digit license key.
4. Select **OK** > **Close**.

Deactivating installed applications on one device

1. From any device view, select a device, and then go to **Device** > **Applications**. You may be required to provide login information.
2. Select the application, and then from the toolbar, select **Deactivate**.
3. Select **Yes** > **Close**.

Uninstalling applications on one device

1. From any device view, select a device, and then go to **Device** > **Applications**. You may be required to provide login information.

2 Select the application, and then from the toolbar, select **Uninstall**.

3 Select **Yes** > **Close**.

Managing applications on multiple device

Manage applications remotely on multiple devices using the Manage Applications wizard.

Installing applications on multiple devices

Install applications remotely on one or more devices using the Manage Applications wizard. Once an application is installed, the application can be activated immediately.

1 From any device view, select multiple devices, and then go to **Device** > **Advanced** > **Manage applications**.

You may be required to provide login information.

2 Select **Install application**. If you have licenses available, then select **Activate application after installation**.

3 Select **Next**.

4 Specify a valid application package file (.pkg), and then select **Open** > **Next**.

5 If Activate application after installation is selected and a license is required, then select any of the following:

Option	Actions
Activate without a license key	Go to the next step.
Use the following license key	Select a device, and then type the 20-digit license key.

Option	Actions
Import license keys	**a.** Browse to find a valid license key file (.csv) for your device, and then select **Open**. If you do not have a .csv file provided by the dealer, then create a .csv license key file that includes columns for device serial number and license key. If the contents of the .csv file are incorrect, then select **Yes**. **b.** In the License Keys Mapping dialog box, select mapping values for each property. If the first line of the .csv file contains headers, then select **File has headers**.

If necessary, select **Export license keys** to save the license key to a .csv file.

6 If the application is not activated during installation, then the Apply license keys page does not appear. Select **Next**.

7 Select **OK**.

8 Review your settings, and then select **Finish** to install the application.

When installation is finished, select **Save log** to save an installation log file (.csv).

Activating installed applications on multiple devices

1 From any device view, select multiple devices, and then go to **Device** > **Advanced** > **Manage applications**.

You may be required to provide login information.

2 Select **Activate application**, and then select **Next**.

3 Select how to choose the application:

Option	Actions
Specify application package	**a.** Select **Next**, and then browse to find a valid installation package file (.pkg). **b.** Select **Next**, and then go to step 8.
Specify application installed on the device	Select **Next**.

4 Select a device, and then select **Next**.

You may be required to provide login information.

5 Select the application to be activated, and then select **Next**.

6 Select a method to choose license keys:

Option	Actions
Activate without a license key	Go to the next step.
Use the following license key	Select a device, and then type the 20-digit license key.
Import license keys	**a.** Browse to find a valid license key file (.csv) for your device, and then select **Open**. If you do not have a .csv file provided by the dealer, then create a .csv license key file that includes columns for device serial number and license key. If the contents of the .csv file are incorrect, then select **Yes**. **b.** In the License Keys Mapping dialog box, select mapping values for each property. If the first line of the .csv file contains headers, then select **File has headers**. The first line of the file is ignored and only the data is used.

If necessary, select **Export license keys** to save the license key to a .csv file.

7 Select **Next**.

8 Review your settings, and then select **Finish** to activate the application.

When activation is finished, select **Save log** to save an activation log file (.csv).

Deactivating installed applications on multiple devices

1 From any device view, select multiple devices, and then go to **Device** > **Advanced** > **Manage applications**.

You may be required to provide login information.

2 Select **Deactivate application**, and then select **Next**.

3 Select either of the following:

Option	Actions
Specify application package	**a.** Select **Next**, and then browse to find a valid installation package file (.pkg). **b.** Select **Next**, and then go to step 6.
Specify application installed on the device	Select **Next**.

4 Select a device, and then select **Next**.

You may be required to provide login information.

5 Select the application you want to deactivate, and then select **Next**.

6 Review your settings, and then select **Finish**.

Uninstalling applications on multiple devices

1 From any device view, select multiple devices, and then go to **Device** > **Advanced** > **Manage applications**.

You may be required to provide login information.

2 Select **Uninstall application**, and then select **Next**.

3 Select how to choose the application:

Option	Actions
Specify application package	**a.** Select **Next**, and then browse to find a valid installation package file (.pkg). **b.** Select **Next**, and then go to step 6.
Specify application installed on the device	Select **Next**.

4 Select a device, and then select **Next**.

You may be required to provide login information.

5 Select the application to be uninstalled, and then select **Next**.

6 Review your settings, and then select **Finish** to uninstall the application.

Searching applications

1 From any device view, select a device, and then go to **Device** > **Applications**.

You may be required to provide login information.

2 In the Searchable fields menu, select **Name** or **Version**.

3 In the Search text box, enter the text to find.

To clear the search results and display the entire list again, from the toolbar, select **Clear search**.

Setting device notification

Manage notifications for changes in the status of the device. Notifications can be triggered by one or more events. For example, a paper jam can be set to trigger a notification.

Before you can send email notifications, make sure that:

- TCP port 25 is available and not blocked by a firewall or virus scanner.
- Email settings are configured in **Edit** > **Options** > **Mail settings**.

1 Select one or more devices, and then go to **Device** > **Notification settings**.

2 Select one or more notification actions.

Display pop-up window

Displays a pop-up window every time a notification is triggered.

Show Windows event log

Opens the Windows event log to display the notification that was triggered.

Send email to the following addresses

Send the notification to specified email addresses. In the text box, enter the email addresses separated by a comma.

3 Specify one or more events that trigger a notification.

Options may vary depending on your device.

4 Select **OK**.

Configuring device communication settings

If authentication is enabled on the device, then you must set the login information correctly in Communication Settings to access device features, such as Address Book, Users, or Document Box.

1 From any Device view or Accounting devices view, right-click a managed device, and then select **Communication Settings**.

2 Depending on your device, modify any of the available settings.

Setting	Actions
Network interface settings Displays settings for each network interface card attached to the device.	Select the primary network card to edit any of the available settings: **TCP/IP port** Type the port number set on a device. Some operations send a command or command file via logical device port. Set the port number on the print device home page. **Communication timeout (seconds)** The number of seconds the application tries to establish a connection with the device. **SNMP communication retries** The number of retries to establish communication with the device after a communication failure. **Command Center administrator password** The password used to access the device through its web interface. **Use SNMP v1/v2** Enter the Read community and Write community names for the device. The Read and Write community names are sent with all SNMP receive and send requests, and must match the community values on the device. **Use SNMP v3** Enter the login information set on the device, and then configure the Authentication and Privacy settings.

Setting	Actions
Secure protocol settings Transport Layer Security (TLS) is a cryptographic protocol that provides security for network communication.	Select from either of the following: • To use HTTPS, select **TLS**. • To use HTTP, clear **TLS**.
Login Sets the user login information if supported in the selected device.	Depending on your preferred view, enter the following login options: • User information switch • Login user name and password • Authenticate mode switch
Account polling settings Polls devices at specific time intervals to check for account counter information.	**a.** Select **Account counter polling**. **b.** Set a recurring schedule for polling information.
Device polling settings Polls devices at specific time intervals to check for error conditions, operational status, and low toner levels. For a device selected from an Accounting view, only the Status polling setting is available.	Set the following polling modes at specific time intervals: **Status polling** Gathers information about the current operational state of the device, such as error conditions, panel messages, and operating mode. **Counter polling** Gathers information about the values held by various counters in the device, such as the number of color pages printed, number of black and white pages, and number of faxes received. **Toner level polling** Gathers information about the current level of toner in the device.

3 Select **OK**.

Advanced menu

To access the Advanced menu, go to **Device** > **Advanced**. The following settings are available:

Settings and options may vary depending on your device.

Set multiple devices

Sends configuration parameters to multiple devices at the same time.

Restart devices

Restarts devices or device networks remotely.

Manage applications

Install, uninstall, activate or deactivate applications on devices.

Manage optional functions

Activate installed optional functions on one or more devices.

Manage certificates

Import, assign, and delete valid (not expired) certificate files that contain encrypted information for device authentication and communication.

Upgrade firmware

Install the most current firmware on devices.

Device default settings

Set default settings of the selected device, such as duplex, print quality, and fax settings. Only one device may be selected at a time.

Device system settings

Set system settings of the selected device, such as operation panel language, timer settings, and panel lock. Only one device may be selected at a time.

Device network settings

Set network settings of the selected device, such as IP address, email settings, and protocol settings. Only one device may be selected at a time.

Install driver

Install printer drivers on devices.

Upgrade driver

Upgrade printer drivers to a later version.

Uninstall driver

Uninstall printer drivers.

Authentication settings

Set authentication settings of the selected device, such as user login and LDAP settings, and permitting jobs with unknown IDs. Only one device may be selected at a time.

Network groups

Create, enable, and disable groups used for group authorization.

TCP/IP Send Data

Send data directly to the interface of one or more selected devices.

Remote services

Use this setting to configure the connection mode and proxy settings to allow KYOCERA Fleet Services to communicate with the device and perform remote maintenance.

Register devices

This feature is enabled only if the device is not yet registered to KYOCERA Fleet Services.

Device multi-set

Use Device Multi-Set to send configuration parameters to one or more devices simultaneously.

Creating device settings in quick mode

1. Select one or more devices, and then go to **Device** > **Advanced** > **Set multiple devices**.
2. In Multi-Set Mode, select **Quick mode** > **Next**.
3. In Device group, select one or more groups to which settings will be applied and then select **Next**.
4. In Source Device, select a device from the list, and then select **Next**.

   If local authentication is enabled, then an administrator must specify login information in the Login section of the communication settings for the device. All settings and passwords for the source and destination devices must be correct in Communication Settings for a successful Multi-Set completion.

5. Review your settings.
   - To accept, select **Finish**.
   - To make changes, select **Back**.

   If the device must be restarted to save the settings, then a message appears. Select **OK** to close.

Creating device settings in custom mode

With custom mode, you can customize and copy settings to one or more device groups. Select the settings to copy and the method to use.

1. From any device view, select one or more devices, and then go to **Device** > **Advanced** > **Set multiple devices**.
2. Select **Custom mode**, and then select **Next**.

3 Select one or more groups, and then select **Next**.

4 Select one or more settings to copy to the destination devices, and then select **Next**.

Options may vary depending on your device.

Device System Settings

Basic device settings including operation panel language, timers, and security options.

Device Network Settings

Basic settings for TCP/IP, security, and network configurations.

Device Default Settings

Settings that define default behavior for device functions, such as print, copy, and fax jobs, including paper size, print and scan quality, and default media types.

Device Authentication Settings

Settings that define local or network authorization for accessing a device.

Device User List

Information about user accounts for each device.

Device Address Book

Contact information such as email, FTP, and fax.

Device Document Box

Custom and fax boxes.

Device Network Groups

Creation of groups used for group authorization, and enabling or disabling of groups.

Device Virtual Mailbox

Virtual mailboxes, including ID, name, and maximum size are included.

Remote Services Settings

Connection mode and proxy settings for remote maintenance.

5 Select from the following options, and then select **Next**.

For some settings, select **Overwrite Settings on target device.** When selected, the settings template is copied over the current destination device settings.

Option	Actions
Create from device Copy device settings from a source device.	On the Source device page, select one device from the list, and then select **Next**. If authentication is required, enter the login information.
Create from file Copy device settings from a file.	**a.** Select **Browse** to locate the preferred file. Supported format may vary depending on your device. **b.** Select **Open**, and then select **Next**. **c.** If Device User List, Device Address Book, or Device Document Box and a .csv file is selected, then do the following: **1.** Select mapping values for each property. Any items that are not selected are skipped. **2.** If the first line of the .csv file contains headers, then select **File has headers**. The first line of the file is ignored and only the data is used. **d.** Select **Next**.
Create new Create a new device settings template. In Device group, if more than one device is selected, then this option is not available.	If multiple options are selected, then do the following: **a.** Select a setting group from the list, and then select **Edit Settings**. **b.** Select **OK** > **Close**.

6 Review your selections.

If **Edit settings** is enabled, then you can select this option to make changes to the settings. Select **Save to file** if you want to save your settings to a file. If you

select more than one setting, then this file is saved as a .zip file. Select **Back** to make any changes.

Multi-Set Template (.zip) files consist of XML files generated by this application only.

7 Select **Finish**.

A message displays if the device must be restarted to save the settings. Select **OK** to close.

- If the process completes successfully, then the properties or settings are copied from the source device to the destination device. Select **Close**.
- If the process does not complete successfully, then select **Details** to see a list of the errors. To save the error list to a .csv file, select **Export**.

Restarting a device or device network interface

This feature lets you restart one or more devices or network interface of the device remotely.

1 Select one or more devices, and then go to **Device** > **Advanced** > **Restart devices**.

2 Select the type of restart, and then select **Next**.

Device restart

Restarts the selected printing devices.

Network restart

Restarts the network interface for the selected printing devices.

3 Review your selections, and then select **Finish**.

If authentication is required, enter login information.

Select **Export** to save the result to a .csv file.

Manage optional functions

Use Manage optional functions to activate optional functions on one or more devices. These functions are included in the device firmware. The administrator has the 20-digit license key needed for activation, or use a temporary trial version of a feature.

Activating an optional function on multiple devices

1 Select multiple devices, and then go to **Device** > **Advanced** > **Manage optional functions**.

2 Select a function name, and then select **Next**.

3 Select **Official** or **Trial**, and then select **Next**.

If Trial is selected, then go to step 6.

4 Select devices to add a license key. Devices can use the same or different license keys.

Option	Actions
Add a license key	**a.** Enter a 20-digit license key. **b.** Select **OK**. **c.** Select **Export license keys** to save the license key to a .csv file.
Import license keys	**a.** Browse for a valid license key file (.csv) provided by your dealer. You can create a license key file that includes columns for device serial number and license key. **b.** If the contents of the .csv file are incorrect, then select **Yes**. **1.** In the License Keys Mapping dialog box, select mapping values for each property. **2.** If the first line of the .csv file contains headers, select **File has headers**. The first line of the file is ignored and only the data is used.

Select **Export license keys** to save the license key to a .csv file.

5 Select **Next**.

6 Review your settings, and then select **Start**.

Licensing progress and results are displayed. When activation is finished, select **Save log** to save an activation log file (.csv).

Activating an optional function on one device

1 Select a device, and then go to **Device** > **Advanced** > **Manage optional functions**.

If authentication is required, enter login information.

2 Select from the following activation option:

Option	Actions
Activate license	**a.** Select a function, and then select **Activate license**. **b.** Enter a 20-digit license key, and then select **OK**. **c.** Select **Yes**. If necessary, select **Export** to save the activation result to a .csv file.
Activate trial Some functions are not supported by trial activation.	**a.** Select one or more functions, and then select **Activate trial**. **b.** Select **Yes**. If necessary, select **Export** to save the activation result to a .csv file.

3 Select **Close**.

Upgrading the firmware

Deploy a newer version of firmware to one or more devices from a master file provided by an administrator or a dealer.

- If the master file version is older than the device firmware version, then the firmware level is downgraded.
- Make sure that TCP ports 800 to 899 are not blocked by a firewall or virus scanner.
- Make sure that the devices are turned on during the process.
- Make sure that the Start of Job String is blank for the logical printer used. Go to the device home page to review the settings.
- If local authentication is on, then you must specify login information in **Device** > **Communication settings** > **Login**. For some devices, logging in with a user name and password is not supported. All settings and passwords for the destination devices must be correct in Communication settings.

If a device is turned off or loses power at a critical point during the upgrade, then the device may become inoperable and require servicing to replace damaged components. Review this process with your administrator or support group, and establish contingency plans.

1. From any device view, select one or up to five managed devices.
2. Go to **Device** > **Advanced** > **Upgrade firmware**.
   If the selected devices have different firmware, then Upgrade firmware is not available.
3. Read the warning information. If you understand and accept the warning, then select the check box, and then select **Next**.
4. Browse for a valid firmware file, and then select **Next**.
5. Review the details.
   - If the firmware file cannot be validated, then select **Back** to browse for another firmware file.
   - Select **Upgrade**.

   Make sure that there are no issues with the devices or details.
6. Review the results.
   - If you are upgrading multiple devices, then you can select **Cancel** to abort the process for devices that are still in the queue.

     Selecting Cancel does not affect the device that is being processed.
   - You can export the log as a .csv file by selecting **Save log**.
   - Select **Close**.

Configuring authentication settings

Manage device-specific login preferences for local device users or network users.

Settings and options may vary depending on your device.

1. From any device view, right-click a managed device, and then go to **Advanced** > **Authentication settings**.

   - You must be connected to a managed device to configure authentication settings.
   - You can configure up to three devices at once by repeating this step for each device.
2. Depending on your device, modify any of the available settings:

Setting	Actions
Enable user login	Select either of the following options: • **Use local authentication** • **Use network authentication** You can configure additional network authentication settings, such as setting one or more Domain names, selecting a Server type, and specifying a Host name.
Permit jobs with unknown IDs	When selected, any user can access the device. When not selected, the device is restricted to users that are configured in User Login. To review or modify User Login for a device, do the following: **a.** In Control Panel, select **Devices and Printers**. **b.** Right-click your device, and then select **Printer properties**. **c.** Go to **Device Settings** > **Administrator Settings** > **User Login**.
Local authorization	Prohibit job use by specific users on a device that supports this feature.
Simple Login	Require users to select their account on the device panel, and provide login details, if necessary.
PIN Login	Require users to provide a PIN on the device. This setting is available only if Use network authentication is selected, and the Server type is Ext.
ID card login settings	You can configure Keyboard login and Password login preferences. This setting is available only if the ID card authentication kit is configured with the device.

Setting	Actions
Network user properties	**a.** Enable or disable **Obtain network user properties**. **b.** In LDAP settings, specify the following: • **Server name** • **Port number** • **Search timeout** • **Encryption** • **Authentication type** **c.** In Acquisition of user information, specify the following items used by the device when searching for user information from the LDAP server: • **Name 1**, **Name 2** • **Email address**

3 Select **OK**.

Network groups

Manage network groups added on your device.

Adding a network group

1 From any device view, select a device, and then go to **Device** > **Advanced** > **Network groups**.

- If authentication is set, then accessing the settings requires the correct login information in the Communication Settings for the device.
- If authentication is not set, then the login dialog box may appear depending on your device.

2 Select **Add group**.

3 In Group ID, enter a unique group ID.

4 In Group name, enter a name for the group.

5 Set the Access level to either **User** or **Admin**.

6 From the Job authorization settings section, set the group access to available device features.

Settings not supported by the device are disabled.

Permit

Enable access to the selected device feature.

Prohibit

Disable access to the selected device feature.

Permit all

Enable access to all device features.

Duplex restriction, Combine restriction, and EcoPrint restriction settings are set to **Off**.

Prohibit all

Disable access to all device features.

Duplex restriction, Combine restriction, and EcoPrint restriction settings are set to their highest restriction option.

7 Select **OK**.

To edit, select a group, and then select **Properties**. Modify the job authorization settings as needed, and then select **OK**.

You cannot edit the group ID and name.

To delete, select a group, and then select **Delete group** > **Yes**.

You cannot delete the group Other. This group is used by the application.

Setting group authorization

Enabling group authorization sets users to operate within permissions set for the group. This feature activates or deactivates group authorization for all network groups.

1 From any device view, select a device, and then go to **Device** > **Advanced** > **Network groups**.

- If authentication is set, then accessing the settings requires the correct login information in the Communication Settings for the device.
- If authentication is not set, then the login dialog box may appear depending on your device.

2 From the toolbar, select **Authorize groups**.

3 Select **On** to activate group authorization, or select **Off** to deactivate group authorization.

4 Select **OK**.

Searching the group list

1 From any device view, select a device, and then go to **Device** > **Advanced** > **Network groups**.

2 In the Searchable fields menu, select the type you want to search.

3 In the Search text box, enter the text to find.

To clear the search results and display the entire list again, from the toolbar, select **Clear search**.

Sending TCP/IP data

This feature sends data files, text, or device commands directly to the interface of one or more devices.

This is an advanced feature. Incorrect use can cause the device to be inoperable.

1 From any Device view, select a device, and then go to **Device** > **Advanced** > **TCP/IP Send data**.

- If authentication is set, then accessing the settings requires the correct login information in the Communication Settings for the device.
- If authentication is not set, then the login dialog box may appear depending on your device.

2 Select one of the following transmission methods:

Default TCP port

Use the default TCP port set on the device.

Specified TCP port

Specify a TCP port to use for the device. From the Port menu, enter the port number.

The port number must match one of the logical devices defined on the print device home page.

IPPS

Use IPPS to transmit data. From the Path text box, enter a valid path.

3 Select one or more of the following data types:

- If Text and File are selected, then the application sends text data first, and then file data.
- The application sends `{#FILE#}` commands and text in the order they appear in the Text box. Binary data can appear in text as bytes in hexadecimal form with the 0x string prefix.
- Some options may not be available depending on your device.

Type	Action
Text	**a.** Select **Text**. **b.** In the Text field, enter the text to send. • You can send PRESCRIBE commands. • To access any of the last 10 sent text strings, select **History**.
File	**a.** Select **File**. **b.** Browse for the file to send. You can send macros or printable files, such as .pdf or .prn files.

4 Select **Send**.

Enabling remote services

You can enable remote services to connect your device to KYOCERA Fleet Services.

This feature is available only on some devices.

1 From any device view, select a device, and then go to **Device** > **Advanced** > **Remote services**.

You may be required to provide login information.

2 In Remote services, select **On**.

3 In Connection mode, select either **Manage** or **Monitor**.

4 If Manage is selected, then configure the following settings:

Options may vary depending on your device.

Expiration time

Enable and set expiration time of remote services.

Remote operation

Enable and set allowed users to use remote services.

5 Review or modify any of the following settings:

Options may vary depending on your device.

AI diagnostic service

Enable automatic status monitoring and maintenance notification of your printer.

Server certificate verification

Configure the following server verification properties:

- Use default settings
- Certificate auto verification
- Revocation check type
- Hash

Proxy Settings

Configure additional settings when using a proxy server.

6 Select **OK**.

Registering devices

Register a device to KYOCERA Fleet Services for remote maintenance.

This feature is available only on some devices.

1 From any device view, select a device, and then go to **Device** > **Advanced** > **Register device**.

2 Enter requested information.

3 Select **OK**.

5 Account

Manage the accounts on your devices, and the devices associated with specific accounts.

Managing devices

When you manage a device, you can create and view accounts, use notification and reporting features, and view or reset counters.

1. From any accounting devices view, right-click a device, and then select either of the following options:
   - **Manage device**

     You may be required to provide login information.
   - **Don't manage device**

     If a device is not managed, then features and options available in this application are limited.
2. To switch between viewing or hiding devices that are not managed, go to **Account** > **Hide/Show unmanaged devices**.

Adding account devices

1. From any accounts view, select an account, and then go to **Account** > **Add devices to account**.
2. Select one or more devices to be added to the account.

   Only managed devices can be added.
3. Select **OK**.

Creating a new account

1. From any accounting devices view, select a managed device, and then go to **Account** > **New account**.

   You can only create new accounts for devices that are managed.
2. Specify the account ID and name.

3 Select **OK**.

Viewing accounts and devices

1 From any accounting view, do either of the following:

- From an accounting devices view, select a managed device.
- From an accounts view, select an account.

2 Depending on your selection, go to:

Option	Description
Account > View devices for this account	Display information about devices associated with a specific account. • Add or remove devices • Export Account Devices reports
Account > View accounts on this device	Display information about accounts associated with a managed device. • Create new accounts • Add or delete existing accounts • Manage Device Accounting settings • Export Device Accounts reports

Displaying account properties

View account-specific information about counters and set usage restrictions.

1 From any accounting devices view, double-click a managed device.

You must manage a device to view the accounts associated with it.

2 Double-click an account, and then review the properties.

Properties may vary depending on your device.

General

Account ID and name.

Counters by function

Number of pages printed, copied, or received through fax.

Counters by media

Number of pages used according to media size or type.

Counters by duplex/combine

Number of pages for single-sided, double-sided, and combined printing, such as 2-in-1 and 4-in-1.

Counters for scanned pages

Number of pages scanned for copy, fax, or other functions.

Counters for FAX transmission

Number of pages transmitted, and the total transmission time.

Timestamp

Date and time when the counters were last updated.

Usage restriction by function

Set the limit for the number of pages allowed for printing, copying, scanning, or faxing.

Off

Usage is not restricted.

Counter limit

Set the maximum usage limit and reset the value if the maximum is reached.

Reject usage

Usage is restricted.

Reset counters

Reset all device counters to zero.

Select **Refresh device counters** to keep the account information updated. To manually refresh device counters, go to **Account** > **Refresh counters**.

3 Select **OK** to save any changes, or select **Cancel**.

Exporting current account details

From any accounting view, you can export account details for all managed devices to a .csv or .xml file.

The .csv export uses UTF-8 encoding.

1 From My Views or Default Views, select any accounting view.

2 Go to **File** > **Export** > **Accounts**, and then select an option:

Option	Description
Account IDs	Export a list of accounts in all managed devices that can be imported to the printer driver. Account IDs can only be exported to a .csv file.
Counters	Export the detailed counter information for all managed devices and accounts.
Information	Export an accounting information summary for all managed devices, including some counter information.

3 Complete the export details:

- File location
- File name
- File type

4 Select **Save**.

Exporting specific device or account details

From any accounting view, you can export specific device or account details to a .csv or .xml file.

The .csv export uses UTF-8 encoding.

1 From My Views or Default Views, select any accounting view:

- From an accounting devices view, select a managed device, and then go to **Account** > **View accounts on this device**.
- From an accounts view, select an account, and then go to **Account** > **View devices for this account**.

2 Select one or more entries, and then select **Export**.

3 Select from the following options:

Option	Description
Account IDs	Export the account ID list that can be imported to the printer driver. Account IDs can only be exported to a .csv file.

Option	Description
Counters	Export the detailed device counter information.
Information	Export the device accounting information summary, including select counter information.
Properties	Export properties information of all accounts. This option is available only in Device Accounts.

If you selected View accounts on this device, then a message appears after you select a Device Accounts export option.

- Select **Yes** to export the details of all entries.
- Select **No** to export only the details of your selection.

4 Complete the export details:

- File location
- File name
- File type

5 Select **Save**.

Adding counter reports

An account view can have one counter report containing device counter information for one or more accounts. Counter reports can be sent as a .csv or .xml attachment in a periodic email to one or more recipients.

To add counter reports, you must configure Mail settings in **Edit** > **Options**.

1 From My Views, select any account view, and then go to **Account** > **Add counter report**.

2 Configure the settings.

To reset the counters on a device to zero when a counter report is successfully sent, select **Automatic counter reset**.

3 Select **OK**.

You can only add up to five counter reports.

To display a list of existing current reports, go to **Account** > **Show counter reports**.

- To view or change report settings, select a report entry, and then select **Properties**.

- To remove one or more reports, select one or more entries, and then select **Delete**.

To manually reset counters, select one or more managed devices or accounts from any accounting view, right-click the section, and then select **Reset counters**.

Setting account counter status notification

When a device counter for any account exceeds a warning level or counter limit, you can choose to be notified by configuring Notification settings.

The Notification settings option is available only for managed devices.

1. From any accounting devices view, right-click a managed device, and then select **Notification settings**.
2. Select one or more notification methods:
   - **Display pop-up window**
   - **Show Windows event log**

     To view the Windows event log, in Windows Event Viewer, go to **Event Viewer (Local)** > **Windows Logs** > **Application**, and then search for the application event.
   - **Send email to the following addresses**

     - TCP port 25 must be available and not blocked by a firewall or virus scanner.
     - You must configure Mail settings in **Edit** > **Options**.
     - You can only add up to three email addresses.
3. Select one or more events to trigger a notification:
   - **Notify when counter exceeds warning level**
   - **Notify when counter exceeds counter limit**
4. Select **OK**.

Configuring device accounting settings

Control and monitor a managed device using Device Accounting Settings.

1. From any accounting devices view, right-click a managed device, and then select **Device accounting settings**.

   You may be required to provide login information.
2. Review the settings:

   Settings may vary depending on your device.

General

View network and account information.

Job accounting

Enable or disable job accounting for various device functions.

Media type

Set the paper size and type for each counter.

Error handling

Print a report, show a warning, or cancel a job for illegal account errors or exceeded counter limits.

Additional

Allow or decline job processing without a device account, and choose to separate or combine counters for printing and copying.

3 Select **OK**.

Accounting multi-set

Deploy account lists and device accounting settings to multiple devices simultaneously.

1 From any accounting devices view, select one or more managed devices.

You must be connected to the managed device.

2 Right-click your selection, and then select **Set multiple accounting devices**.

3 Select a device group to apply multi-set.

- Only the devices that support multi-set are displayed.
- The devices are organized by model group.

4 Select the type of settings to be applied to the device group, and then select **Next**:

Device Accounting Settings

Includes settings for job accounting, media type, error handling, permitting job processing without an account ID, and copy counter.

Account List

Includes print, copy, scan, and fax counter information associated with device accounts.

5 Select a multi-set option, and then select **Next**:

- For Account List, you can select **Overwrite settings on target device**. When selected, specify if existing counters are reset or not.
- For Device Accounting, multi-set automatically overwrites all settings.

Option	Actions
Create from device	Select a source device, and then select **Next**.
Create from file	Browse for a multi-set template (.xml or .csv), and then select **Open** > **Next**. If necessary, resolve any file selection issues, and then repeat this step. For Account List, if you select a .csv template, then you may need to map the file columns to the respective account properties. Items that are not mapped are skipped. Select **File has headers** to ignore the first row in the file.

Create new	• For Device Accounting, configure the available items in Device Accounting Settings, and then select **OK**.
	• For Account List, select an option:
	  • To add new accounts, select **New account**, and then specify the account information.
	  • To add existing accounts, select **Add account**, and then select one or more entries from the list. You can review and change the properties for each added account.

6 Confirm your settings.

You can either edit or save the settings to a file.

7 Select **Finish**.

- You may be required to restart the device to save the settings.
- If necessary, resolve any issues, and then repeat the process.
- Select **Export** to save the results as a .csv file.
- Select **Close**.

6 Host

Manage printer drivers and print queues. Use host views to install, upgrade, or uninstall printer drivers on host computers, and configure login settings.

Host discovery

This feature lets you find network host computers. If new hosts are found, the application updates its database with information about the host. This process can be performed manually for single or multiple hosts, or it can be scheduled to run automatically according to a schedule. It is also possible to exclude hosts from being discovered.

Activate host services

For the application to discover hosts, Windows Management Instrumentation (WMI) and Remote Procedure Call (RPC) services must be active on the host computers and on the computer where the application is installed.

Installing certificates for signed drivers

Digital signatures are required for hardware-related drivers. Before installing a signed driver, Windows requires a trusted certificate. For Microsoft-signed drivers, the certificate is already installed. For manufacturer-signed drivers, you must install the certificate on the host computer.

1. From the driver package, open the appropriate security catalog (.cat) file, depending on your operating system.
2. Select **View Signature** > **View Certificate** > **Install Certificate**.
3. Select a store location, and then select **Next**.
4. Select **Place all certificates in the following store**, and then select **Browse**.
5. In Select Certificate Store, select **Trusted Publishers**, and then select **OK**.
6. Select **Next** > **Finish**.

Activating WMI

For the application to discover hosts, Windows Management Instrumentation (WMI) services must be active on the host computers and on the computer where the application is installed.

1. On each computer, go to **Start** > **Control Panel** > **System and Security** > **Administrative Tools** > **Computer Management**.

2 In Computer Management, select **Services and Applications**.

3 Right-click **WMI Control**, and then select **Properties**.

4 In Security, select **Security**.

5 In Group or user names, select **Administrators**.

6 In Permissions for Administrators, allow **Remote Enable**.

Activating RPC

For the application to discover hosts, Remote Procedure Call (RPC) services must be active on the host computers and on the computer where the application is installed.

1 On each computer, go to **Start** > **Control Panel** > **System and Security** > **Administrative Tools** > **Computer Management**.

2 In Computer Management, select **Services and Applications** > **Services** > **Remote Procedure Call (RPC)**.

Make sure that the service is running. If necessary, right-click **Remote Procedure Call (RPC)**, and then select **Start**.

Adding hosts

1 Go to **Host** > **Discovery** > **Add hosts**.

You may be required to provide domain administrator login information.

2 Select an option, and then select **Next**:

Option	Actions
Search current domain Scans all hosts in your domain.	Go to the next step.
Browse Active Directory Scans all hosts in a selected directory in your domain.	Select an active directory group in your domain.

Option	Actions
Specify IP address range Scans all hosts within the designated IP address range in your domain.	Enter a starting and ending IPv4 or IPv6 address, and then select **Add** to include the entry in the Selected network segments list. To remove an IP address range from the Selected network segments list, select the range, and then select **Remove**.
Specify IP address Scans the host using a specific address in your domain.	Select from the following methods: • Enter an IPv4 or IPv6 address or host name, and then select **Add** to include the entry in the Selected targets list. • Select **Import** to use an IP address list. To remove an IP address or host name from the Selected targets list, select the IP address or host name, and then select **Remove**.

3 Set a recurring schedule for discovery, or select **Next** to start immediately.

4 Confirm the details, and then select **Finish**.

Newly added hosts appear in the Host view.

To remove, right-click a host, and then select **Delete**.

Driver and queue information is also removed.

Scheduling automatic host discovery

Set up a regular schedule for performing the discovery process. If hosts are frequently added to or removed from the network, then performing discovery on a regular basis keeps the host database updated.

1 Go to **Host** > **Discovery** > **Automatic discovery**.

2 In Scheduled Discovery, do any of the following:

- To create a new discovery mode, select **Add**. Set up a recurring schedule, and then select **Finish**.
- To remove a discovery schedule, select **Delete**.
- To edit an existing discovery mode, select **Properties**. Set up a recurring schedule, and then select **Apply changes**.

3 Select **Close**.

Excluding a host from discovery

Exclude hosts from the discovery process to remove them from view for security purposes.

1. In Host View, select one or more hosts to exclude.
2. Right-click your selection, and then select **Delete**.

To add a deleted host, go to **Host** > **Discovery** > **Show excluded hosts**, select one or more entries, and then select **Include Host**.

Adding queues

1. From any host queue view, go to **Host** > **New queue**.
2. Select one or more hosts, and then select **Next**.
   You may be required to provide login information.
3. Select a device, and then select **Next**.
4. Select **Have disk**, and then browse for a valid .inf file for the device.

   Make sure to select the appropriate 32-bit or 64-bit .inf file, depending on the system type of your host.
5. Select **OK** > **Next**.
6. Review the device settings for each host.
   - In Selected printer model, select each item to edit the settings.
   - Select **Common settings** to configure host-independent settings.

   Factory Default

   If you select **Yes**, then browse for a .kxp file. After uploading the file, you can then select an option from the available profiles.

   If you select **No**, then the factory default profile will not be changed.

   Plug-ins

   Select one or more options.

   Comments

   Add custom notes to your common settings configuration.

   Open

   Browse for a configuration settings file (.kvp).

   Save

   Export the common settings to a configuration file.

- Select **Conflicts** to manage the behavior of the installation if certain conditions are met.

Condition	Options
Printer exists	**Keep settings** The current device settings remain the same and the printer is not installed. **Override** The current device settings will be replaced with new configuration.
Driver exists	**Does nothing** The current printer driver settings remain the same and a new driver is not installed. **Upgrade** The current printer driver is upgraded to a newer version.
Share name exists	**Add suffix** Extra characters are added to the existing share name **Fail** The device is not installed. **No share** The device is installed but Sharing is turned off.
Port is not available	**File, LPT1** Installation is attempted with the selected port. **Fail** The device is not installed.

- Select **Import** to add device settings from a .kvp file.
- Select **Export** to save the current device settings as a .kvp file.

7 Select **Next**, and then confirm your settings.

8 Select **Finish** to create the new queue.

9 Review the queue creation results.

- If necessary, resolve any issues, and then repeat the process.

- Select **Export** to save the results as a .txt file.
- Select **OK**.

To remove a queue, select it from the list, and then select **Delete queue**.

Editing a queue name

1. From any host queue view, right-click a queue, and then select **Rename**.
2. Enter a new queue name, and then select **Edit**.
3. Review the result.
   - If necessary, resolve any issues, and then repeat the process.
   - Select **Finish**.

Printer driver management

The printer driver application provides settings to customize output from your device. You can remotely install printer drivers onto a host computer. Once installed, drivers can be upgraded or uninstalled.

- You must be connected to a host computer to manage host printer drivers.
- To allow the print spooler to accept client connections, and to allow inbound remote administration exception, an administrator may need to set policies in Windows Local Group Policy Editor.

Allowing the print spooler to access client connections

1. In Windows Local Group Policy Editor, go to **Computer Configuration** > **Administrative Templates** > **Printers**.
2. Double-click **Allow Print Spooler to accept client connections**.
3. Select **Enabled** > **OK**.

Restart the print spooler for policy changes to take effect.

Allowing a remote administration exception

1. In Windows Local Group Policy Editor, go to **Computer Configuration** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Defender Firewall**.
   - If the computer is on the domain, then select **Domain Profile**.
   - If the computer is not on the domain, then select **Standard Profile**.

2 Double-click **Windows Defender Firewall: Allow inbound remote administration exception**.

3 Select **Enabled** > **OK**.

Installing printer drivers

1 Depending on your selected view, do the following:

View	Actions
Device view	**a.** Select one or more devices, and then go to **Device** > **Advanced** > **Install driver**. **b.** Select one or more host computers that you are connected to, and then select **Next**. You may be required to provide login information. **c.** For each device, select **Have disk**, and then browse for a valid .inf file. Make sure to select the appropriate 32-bit or 64-bit .inf file, depending on the system type of your host. **d.** Select **OK** > **Next**.

View	Actions
Host view	**a.** Select one or more host computers that you are connected to, and then go to **Host** > **Install driver**. **b.** Select an installation option, depending on the status of the devices: • If the devices appear in Devices view and are available on the network, then select **Install driver with device** > **Next**. **1.** Select one or more devices, and then select **Next**. **2.** For each device, select **Have disk**, and then browse for a valid .inf file. Make sure to select the appropriate 32-bit or 64-bit .inf file, depending on the system type of your host. **3.** Select **OK** > **Next**. • If the devices are not available on the network, then select **Install driver without device** > **Next**. **1.** For each device, select **Have disk**, and then browse for a valid .inf file. Make sure to select the appropriate 32-bit or 64-bit .inf file, depending on the system type of your host. **2.** Select one or more drivers. To find a specific driver, start typing the driver name in the Search box. **3.** Select **Next**.

2 Review the device settings for each host.

- In Selected printer model, select each item to edit the settings.
- Select **Common settings** to configure host-independent settings.

Factory Default

If you select **Yes**, then browse for a .kxp file. After uploading the file, you can then select an option from the available profiles.

If you select **No**, then the factory default profile will not be changed.

Plug-ins

Select one or more options.

Comments

Add custom notes to your common settings configuration.

Open

Browse for a configuration settings file (.kvp).

Save

Export the common settings to a configuration file.

- Select **Conflicts** to manage the behavior of the installation if certain conditions are met.

Condition	Options
Printer exists	**Keep settings** The current device settings remain the same and the printer queue is not installed. **Override** The current device settings will be replaced with new configuration.
Driver exists	**Does nothing** The current printer driver settings remain the same and a new driver is not installed. **Upgrade** The current printer driver is upgraded to a newer version.
Share name exists	**Add suffix** Extra characters are added to the existing share name **Fail** The device is not installed. **No share** The device is installed but Sharing is turned off.
Port is not available	**File, LPT1** Installation is attempted with the selected port. **Fail** The device is not installed.

- Select **Import** to add device settings from a .kvp file.

- Select **Export** to save the current device settings as a .kvp file.

3 Select **Next**, and then confirm your settings.

4 Select **Finish**.

5 Review the results.

- If necessary, resolve any issues, and then repeat the process.
- Select **Export** to save the results as a .txt file.
- Select **OK**.

Upgrading printer drivers

1 Depending on your selected view, do the following:

View	Actions
Device view	**a.** Select one or more devices, and then go to **Device** > **Advanced** > **Upgrade driver**. **b.** Select one or more host computers that you are connected to, and then select **Next**. You may be required to provide login information.
Host view	Select one or more host computers that you are connected to, and then go to **Host** > **Upgrade driver**.

2 For each host, select one or more printer drivers to be upgraded, and then select **Next**.

3 For each device, select **Have disk**, and then browse for a valid .inf file.

Make sure to select the appropriate 32-bit or 64-bit .inf file, depending on the system type of your host.

4 Select **OK** > **Next**.

5 Confirm your settings, and then select **Finish**.

6 Review the results.

- If necessary, resolve any issues, and then repeat the process.
- Select **Export** to save the results as a .txt file.
- Select **OK**.

Uninstalling printer drivers

1 Depending on your selected view, do the following:

View	Actions
Device view	a. Select one or more devices, and then go to **Device** > **Advanced** > **Uninstall driver**. b. Select one or more host computers that you are connected to, and then select **Next**. You may be required to provide login information.
Host view	Select one or more host computers that you are connected to, and then go to **Host** > **Uninstall driver**.

2 For each host, select one or more printer drivers to be uninstalled, and then select **Next**.

Selecting a printer driver also selects the associated queue.

3 Confirm your settings, and then select **Finish**.

4 Review the results.

- If necessary, resolve any issues, and then repeat the process.
- Select **Export** to save the results as a .txt file.
- Select **OK**.

Installing additional printer driver versions

With 32-bit or 64-bit printer drivers installed on a host computer, you can install an additional printer driver of the other version (64-bit or 32-bit, respectively).

This is useful in a client/server environment where the client system and printer driver are different in version.

1 From any host queue view, select one or more queues.

2 Right-click the selection, and then select **Install additional driver**.

3 For each device, select **Have disk**, and then browse for a valid .inf file.

Make sure to select the appropriate 32-bit or 64-bit .inf file.

4 Select **OK** > **Next**.

5 Confirm your settings, and then select **Finish**.

6 Review the results.

- If necessary, resolve any issues, and then repeat the process.
- Select **Export** to save the results as a .txt file.

- Select **OK**.

The added printer driver does not appear in any host view, but can be upgraded or uninstalled.

Viewing printer drivers or print queues

You must be connected to a host to be able to view Host Printer Drivers or Host Print Queues.

1. From Host view, right-click a host, and then select an option:
   - **Show printer drivers**
   - **Show print queues**

   You may be required to provide login information.
2. Select **Refresh** to update the list, or select **OK**.

Changing host login settings

1. From Host view, select a host and go to **Host** > **Host login settings**.
2. Select **Use this login to access the host**, and then specify the following:
   - **User name**
   - **Password**
   - **Domain**
3. Select **OK**.

Selecting domain administrator login settings

Set administrator login rights for retrieving host and queue information and for configuring a remote computer.

If domain administrator login rights have not been set, then a dialog box appears when adding hosts or managing printer drivers. For security purposes, the information is cleared when you exit the application.

1. From any host view, go to **Host** > **Domain administrator login settings**.
2. Select an option:
   - **Use the current Windows login settings**
   - **Specify a domain administrator user name and password**

     Specify the user name, password, and domain.
3. Select **OK**.

Exporting host information

1. From any host view, select one or more hosts, and then go to **File** > **Export** > **Hosts**.
2. Complete the export details:
   - File location
   - File name
   - File type
3. Select **Save**.

Configuring device settings

1. Go to any host view.
2. Depending on your host view, select one or more hosts, printer drivers, or queues, and then go to **Host** > **Printing settings**.

   You must be connected to a host computer to manage host printer drivers.

   If applicable, select one or more printer drivers in a host computer, and then select **Next**.
3. Review the device settings for each host.
   - In Selected printer model, select each item to edit the settings.
   - Select **Import** to add configuration settings from a .kvp file.
   - Select **Export** to save the current configuration settings as a .kvp file.
4. Select **Next**, and then confirm your settings.
5. Select **Finish** to apply the settings.
6. Review the results.
   - If necessary, resolve any issues, and then repeat the process.
   - Select **Export** to save the results as a .txt file.
   - Select **OK**.