

Device Manager

User Guide

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.

© 2023 KYOCERA Document Solutions Inc.

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 1 Product overview

Documentation.....	1-1
Conventions.....	1-1
System requirements.....	1-2
Prerequisites.....	1-2
Supported operating systems.....	1-3
Supported browsers.....	1-3
Standard configuration hardware requirements.....	1-3
Installation checklist.....	1-4

Chapter 2 Login authentication

Chapter 3 Dashboard

Dashboard: Active Tasks.....	3-1
Dashboard: Polling Requests.....	3-1
Dashboard: Status of Devices.....	3-1
Dashboard: Scheduled Tasks.....	3-1
Dashboard: Device Reports.....	3-1
Dashboard: Notifications.....	3-2

Chapter 4 Devices / Device list

Search.....	4-1
Advanced search.....	4-1
Paging.....	4-2
Devices: Columns.....	4-3
Device Groups.....	4-3
Device Groups: Fixed vs. dynamic.....	4-4
Device Groups: Add a dynamic device group.....	4-4
Device Groups: Columns in dynamic groups.....	4-5
Device Groups: Add a fixed device group.....	4-6
Device Groups: Import fixed device groups.....	4-6
Device Groups: Add a folder.....	4-6
Device Groups: Delete a device group.....	4-7
Device Groups: Delete a device group folder.....	4-7
Device Groups: Download.....	4-7
Device Groups: Duplicate a device group.....	4-7
Device Groups: Edit a device group.....	4-8
Device Groups: Rename a device group folder.....	4-8

Add devices.....	4-8
Devices: Enable smart discovery.....	4-10
Devices: Add devices using saved discovery settings.....	4-10
Devices: Automatic discovery.....	4-10
Devices: Switching between Wi-Fi and wired connection.....	4-11
Devices: Restore deleted devices.....	4-12
Devices: Delete devices.....	4-12
Device Home on a single device.....	4-12
Refresh.....	4-13
Create tasks.....	4-13
Event triggers.....	4-13
Panel Note.....	4-14
Upgrading device firmware.....	4-16
Device Settings: Multiple devices.....	4-17
Device Settings: Single device.....	4-20
Configurations.....	4-21
Multi-Set Template Editor.....	4-30
Restart a single device.....	4-33
Restart multiple devices.....	4-33
Device tags.....	4-34
Editing tags for a single device.....	4-34
Editing tags for multiple devices.....	4-35
Device properties.....	4-35
Communication Settings.....	4-36
Device Properties: General.....	4-39
Device Properties: Counters.....	4-39
Device Properties: Alerts.....	4-39
Device Properties: Logs.....	4-39
Device Properties: Management.....	4-40
Applications list.....	4-40
Certificate list.....	4-42
Certificates: Multi-Set Configurations.....	4-44
Optional Functions: Activate.....	4-46
Address book.....	4-47
Address Book: Add contacts on a single device.....	4-47
Address Book: Add groups on a single device.....	4-49
Address Book: Add One Touch Keys on a single device.....	4-49
Address Book: Delete contacts, groups, or One Touch Keys on a single device.....	4-50
Address Book: Duplicate contacts or groups on a single device.....	4-50
Address Book: Edit contacts on a single device.....	4-51
Address Book: Edit groups on a single device.....	4-51
Address Book: Edit One Touch Keys on a single device.....	4-52
Address Book: Export contacts on a single device.....	4-53
Address Book: Export groups on a single device.....	4-53
Address Book: Export One Touch Keys on a single device.....	4-53
Address Book: Import contacts, groups, or One Touch Keys on a single device.....	4-53
Address Book: Refresh contacts, groups, and One Touch Keys.....	4-54
Address Book: Settings in Multi-Set Configurations.....	4-54
Device Users.....	4-55
Device Users: Add users.....	4-56
Device Users: Delete users.....	4-56
Device Users: Edit users.....	4-56
Device Users: Export a user list.....	4-57
Device Users: Import a user list.....	4-57
Device Users: Simple Login Keys.....	4-58
Device Users: Network groups.....	4-59
Device Users: Settings in Multi-Set configurations.....	4-60

Document Box.....	4-61
Document Box: Add a document box.....	4-61
Document Box: Delete a document box.....	4-63
Document Box: Edit a document box.....	4-63
Document Box: Export a document box.....	4-63
Document Box: Import a document box.....	4-64
Document Box: Settings in Multi-Set Configurations.....	4-64
Device Users: Authentication.....	4-65
Authentication: General.....	4-66
Authentication: Network User Properties.....	4-67
Authentication: Password Policy.....	4-67
Authentication: User Account Lockout.....	4-68
Map View.....	4-68
Creating a Map.....	4-68
Managing Map View.....	4-69

Chapter 5 Tasks

Tasks: Detail screens.....	5-1
Active task detail screen.....	5-1
Scheduled task detail screen.....	5-1
Completed task detail screen.....	5-1
Tasks: Creating a scheduled task.....	5-1
Tasks: Scheduling Options.....	5-2
Tasks: Select multiple devices for tasks.....	5-2
Using check boxes.....	5-2
Using device groups.....	5-3
Common features on the tasks tabs.....	5-3
Active tasks.....	5-4
Scheduled tasks.....	5-4
Completed tasks.....	5-5
Tasks: Retry completed tasks.....	5-6
Pre-defined tasks.....	5-6

Chapter 6 Reports

Reports: Configure and run reports.....	6-1
Reports: Add scheduled report.....	6-1
Reports: Delete scheduled report.....	6-2
Reports: Edit scheduled report.....	6-2
Reports: Enable or Disable report.....	6-3

Chapter 7 System

Smart Polling.....	7-1
SMTP.....	7-2
Testing SMTP Settings.....	7-2
Security.....	7-2
Selecting a protocol type.....	7-2
Password policy.....	7-3
Login/Logout.....	7-4
Configuring SCEP server settings.....	7-5
Issued Device Certificates.....	7-6
System Settings.....	7-8
System Users.....	7-8

License agreement.....	7-9
Database connection: SQL.....	7-9
Database connection: Firebird.....	7-10
Importing Net Admin data.....	7-10
Proxy settings.....	7-14
Logs.....	7-14
SNMP Trap Server.....	7-15
Setting SNMP Traps for a single device.....	7-15
Setting SNMP Traps for Multiple Devices.....	7-16
Using the SNMP Trap Server.....	7-17
Database backup and restore.....	7-17

Chapter 8 Notifications

Notifications: View notifications.....	8-1
Notifications: Manage device notifications.....	8-2
Notifications: Create user notifications.....	8-2
Notifications: Receive task notifications.....	8-3
Notifications: System.....	8-3

Chapter 9 Miscellaneous

Administrator password change.....	9-1
General behaviors that apply to multiple actions.....	9-1
Troubleshooting.....	9-1
USB devices.....	9-1
Connecting a USB device.....	9-1
Import USB devices from Net Admin backup.....	9-2
Discovering USB-connected devices.....	9-2

1 Product overview

Device Manager is a server-based application that lets you monitor and manage printing devices. With this application, you can:

- Configure device settings
- Install applications on one or more devices
- Receive automated alert messages
- Check toner levels
- Upgrade firmware
- Generate device reports
- Arrange devices in groups



Features and options may vary depending on your device.

Documentation

Installation and Upgrade Guide

Provides instructions on how to install Device Manager, and configure this application to an internal or external database.

This guide is for IT professionals, and non-IT personnel with knowledge of database installation and configuration.



- This guide includes instructions on installing and configuring Microsoft SQL Server Enterprise and Express editions. Follow these instructions if you prefer to use Device Manager with an external database.
 - This guide is not intended to replace the official documentation for Microsoft SQL. For more information, refer to the documentation in the Microsoft website.
-

User Guide

Provides instructions on how to use the features and settings of the application.

This guide is for IT administrators and service technicians.

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

- Text or commands that a user enters are displayed as text in a different font or in a text box as shown in these examples:

1. On the command line, enter `net stop program`
2. Create a batch file that includes these commands:

```
net stop program
gbak -rep -user PROGRAMLOG.FBK
```

- Icons are used to draw your attention to certain pieces of information. Examples:



This indicates information that is useful to know.



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

System requirements

Prerequisites

- Microsoft .NET Core 6.0.9
- Microsoft ASP.NET Core 6.0.9



- .NET Core and ASP.NET Core installation prerequisite: Microsoft Visual C++ Redistributable for Visual Studio 2015.
- .NET Core and ASP.NET Core are included in the installer package. For .NET Core and ASP.NET Core to work properly, your system must have all the latest Windows updates.

- Depending on your system setup and preference, you can configure Device Manager with an internal or external database.



You can only configure Device Manager with one database.

Internal database: Embedded Firebird

This database is embedded with the application, and will be installed in the same computer as the application.

External database: Microsoft SQL Server

This database is installed and set up before installing the application. There is only one database administrator that will access the database locally.

The following versions are supported:

- SQL Server 2019
- SQL Server 2017
- SQL Server 2016

- SQL Server 2014

Determine the SQL Server edition to install, based on your needs:

- Enterprise
- Standard
- Express



- This free edition has lower memory capacity compared to the Enterprise or Standard editions, with a maximum database size of 10 GB.
- For more information on the different Microsoft SQL Server editions, go to the Microsoft website.

Supported operating systems

- Windows 11
- Windows 10
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Supported browsers

- Google Chrome 52 or later
- Microsoft Edge for Windows
- Firefox 53 or later
- Safari


Standard configuration hardware requirements

Recommended hardware	Number of supported devices	Database
<ul style="list-style-type: none">• 4 GB RAM• 2 cores (physical)• 1.5 GHz CPU	Up to 100 devices	Internal
<ul style="list-style-type: none">• 6 GB RAM• 4 cores (physical)• 3.6 GHz CPU	Up to 300 devices	Internal or external

Recommended hardware	Number of supported devices	Database
<ul style="list-style-type: none">• 32 GB RAM• 8 cores• 2.2 GHz CPU• 1,000 Mbps gigabit Ethernet adapter	Up to 10,000 devices	External

Installation checklist

Depending on your database preference, refer to the following chapters in the *Installation and Upgrade Guide*:

Database type	Chapters
Embedded Firebird (internal database)	<i>Device Manager installation and setup</i>  Since the embedded Firebird database will be used, you do not need to install and set up Microsoft SQL Server and SQL Server Management Studio.
Microsoft SQL (external database)	<ol style="list-style-type: none">1. <i>SQL database installation and setup</i>2. <i>Device Manager installation and setup</i>

2 Login authentication

Device Manager supports the following user authentication methods:

Device Manager local authentication method

If Device Manager is installed on the same computer that is used to access it, the user is automatically logged in using the default administrator account. To enable local login, do the following:

1. In Device Manager, go to **System > Security > Login/Logout**.
2. Enable **Local login required**, then select **Apply**.



For local login, log out is disabled.

Administrators can also add accounts in Device Manager to allow users to log in to the application without a domain name. For Device Manager account creation, refer to *System Users*. For each account, administrators can set the following roles:

Admin

Modify all operations and system settings.

User

View and modify some settings for tasks such as adding devices, upgrading firmware, and creating multi-set configurations.

Read-only

View some information such as device status, reports, and notifications.

Windows Active Directory authentication method

Device Manager administrators can configure the settings to automatically or manually log in the user with their Lightweight Directory Access Protocol (LDAP) credentials. The application uses the Active Directory service to collect credentials for accounts that are managed by the domain.



-
- Make sure that **Integrated Windows Authentication** is enabled for your browser.
 - For automatic authentication, log out is disabled.
 - For manual authentication, users must input their credentials in a down-level logon name format.
-

To enable this authentication method, do the following:

1. In the Device Manager installation folder, open **ProfileMain.json** using a supported file editor.
2. Set `disableWindowsAuthentication` to `false`.

3. In the `adLdap` section, specify the IP address of the Active Directory server and corresponding account credentials. You may configure multiple Active Directory servers. For example:

```
"adLdap": [ {  
  "server": "123.123.123.1",  
  "username": "administrator",  
  "password": "admin123"  
}, {  
  "server": "123.123.123.2",  
  "username": "domainName\\administrator",  
  "password": "admin456" } ],
```



To connect the Active Directory using a specific domain account, use two backslashes (\\) to separate the domain name and user name.

4. In the `adGroups` section, specify the group roles of the Active Directory users. These users must belong to a specific group in the Active Directory. For each role, only one group is allowed. For example:

```
"adGroups": {  
  "adminRole": "LDAP-IT-Admin",  
  "userRole": "LDAP-IT-User",  
  "readOnlyrole": "LDAP-IT-Read-only"  
}
```

5. Save the file, then restart Device Manager.

3 Dashboard

With Dashboard, you have one place to look at overall system health and functions, and the ability to jump to detail screens.

The Dashboard offers these overview sections:

Dashboard: Active Tasks

This widget displays the number of active tasks and the average percentage of execution progress, with a link to go to the Active Tasks page.

Dashboard: Polling Requests

This widget displays the estimated number of polling requests with polling status label and a link to the Smart Polling page. Status indicators are:

- Empty: No maximum calculated yet
- Good (green): Current polling below 50% of maximum
- Moderate (orange): Current polling over 50% of maximum
- Excessive (red): Current polling at or over maximum

Dashboard: Status of Devices

This widget displays the number of devices with Ready status and a link to the Device list page.

Dashboard: Scheduled Tasks

Shows the number of scheduled tasks and a link to the Scheduled Tasks page.

Dashboard: Device Reports

The largest widget shows four charts, and allows you to select groups to use as source for the charts. The default uses the All devices group, but all custom groups from the Device list page are available from the drop-down list at the top right corner of Device Reports. Within the Device Reports widget, you also have choices for each chart to show the top 5–10 devices. Available charts are:

Highest Cumulative Errors

Displays a pie chart with the total cumulative errors per device using all error type alerts for the last month. Select any section of the chart to jump to Device properties for that device (except the cumulative Other section, which jumps to the last selected group on Device list).

Highest Device Counters

Displays top highest models by the average of device counters over multiple devices using the total printed pages counter.

Fewest Remaining Days

Shows devices with the lowest average of toner remaining days.

Lowest % of Toner

Devices with lowest average toner % level compared with other devices.

Dashboard: Notifications

Displays the five most recent notifications showing: Notification type, date and time of notification, how long ago it was issued, and a link to the Notifications page (the link itself shows the total of all notifications in the system).

4 Devices / Device list

The Devices tab is the default screen for Device Manager. All devices that have been discovered by Device Manager appear in the Device list. You can customize your view of device data by managing columns, pagination, searching for keywords within device data, and configuring groups of devices for custom access.

The main toolbar on the Devices tab contains the following buttons:

- **Device groups:** Add, view, and manage devices in custom fixed or dynamic groups; the default group is All devices
- **Search**
 - Perform a quick search by typing all or part of a search term into the box
 - Advanced search options let you create specialize queries into device data within Device Manager
- **Add devices**
 - Add devices now
 - Save discovery settings
 - View deleted devices
- **Delete devices**
- **Device home**
- **Refresh**
- **Create task**
 - Restart devices
 - Firmware upgrade
 - Device settings
 - Configurations
- **More...**
 - Communication settings
 - Device tags

You can select **Back to top** to jump back to the top of the screen.

Search

A Search box with filtering options, such as Model name, Host name, and Asset number, is available in some screens in the application.

Advanced search

The Advanced Search option is available only in the Devices tab. You can use Advanced Search in the All devices group or any selection from the groups list.

The specified criteria can be used when creating a dynamic group.

- 1 In Devices, select the filters icon to the left of the search box, and then select **Advanced Search**.
- 2 In Criteria, select an option to match all or any of the added properties.
- 3 Select a property.
The list includes all the properties available in Device Manager. To move to a specific property, start typing the property name to limit the list.



Options available for condition and value may vary depending on the selected property.

- 4 Select a condition, and then enter a value. To make your search more specific, include the following operators in your value:

Operator	Description
*	Use to match zero or more characters.
?	Use to match a single character.
!	Use for NOT operator. For example, an asset number entry that contains a value of *34 && !*3534 will only include printers with asset number that ends in 34, and exclude printers with asset number that ends in 3534.
	Use for OR operator. For example, an asset number entry that contains a value of *34 *35 will only include printers with asset number that ends in 34 or 35.
&&	Use for AND operator. For example, an asset number entry that contains a value of 43* && *34 will only include printers with asset number that starts with 43 and ends in 34.

- 5 If necessary, select + to add another property.
- 6 Select **OK**.

The Device list screen displays devices that match your criteria.

Paging

This feature lets you control the number of devices to show on a page, and is available in the rightmost side of all screens. When you change device groups, changes to the number of devices per page revert to the default value.

Devices: Columns

The column selection button (+) is at the far right of the column headers row on the Device list screen.

Using column selections, you can customize the data presented on the Device list and in device groups by setting configurations for Dynamic groups.

The column selections are grouped into properties groups as follows:

- Common columns
- General
- Service
- Capability
- Counter
- Firmware
- Asset
- SCEP enrollment

Select a column group that has a subset of columns preconfigured and you can use the column group check box to select or remove ALL columns in that group. The basic Device list display uses Common columns and General as defaults.

To change, select the column select button and then check or clear the column group name check box to add or remove all columns in that group from your display.

If you want to add or remove individual columns to customize the Device list display temporarily, use the individual column check boxes.

To close the column selection list, select the column group icon again.

Once you've set the columns to use for the Device list, you can rearrange them by dragging them into a new position (select the column name on the list and drag left or right). You can also resize the columns; hover over the dividing lines until the cursor changes, then select and drag the column width.



Changes made to column selections hold until you change the Device Group that you are viewing. They remain in place if you switch pages, or change the paging option (to show more or fewer devices on the screen). You can switch to another tab (Tasks or Notifications, for example) and return to Devices with the column changes maintained, as well.

Similarly, changes made by dragging and dropping columns to reposition them revert to default positions when you change Device Groups.

All column changes revert to defaults when you log off and back on to Device Manager.

Device Groups

Rather than sorting or selecting columns to display each time you want to see just certain devices or device property, use Device Groups to organize devices on meaningful criteria; like location, buildings, floors, specific device properties, etc.

Fixed groups will contain a static set of devices and use the selected columns from the source group. Dynamic groups let you set up detailed search criteria for adding devices and choosing columns to be displayed for that group.

You can create as many folders and sub-folders as you need under Device Groups. Folders can help you further organize your device information. Select the Move icon to rearrange the display order of folders and groups.

Device Groups: Fixed vs. dynamic

With a Fixed group, the devices displayed do not change except for the deletion of one or more devices.

For Dynamic groups, on the other hand, the system adds newly discovered devices that match your group criteria. Dynamic groups behave the same way with Deleted devices – the device is moved to Deleted devices and stays there, undiscoverable, until and unless it is edited to Include Device. Other conditions that affect whether or not device display in Dynamic groups include Device Property updates from polling (like a change in Device Status if that is specified in the criteria of a Dynamic group.)

A simple example of when to use a Dynamic rather than a Fixed custom group:

You want to have a listing that shows all devices with "TASKalfa" as part of the model name. You can sort All devices to find them, you can use quick search to filter for them on the All devices screen, but you don't want to have to set up a search or sort whenever you want to see just those devices. You can select all devices with "TASKalfa" in the model name in the All devices group and create a Fixed group, but the only condition under which that list would change would be if one or more devices were deleted (or included).

However, you want to know when Add Devices discovers a new TASKalfa device. That won't work with a Fixed group; you would have to delete it, select all TASKalfa devices and create a new Fixed group to capture any newly discovered devices.

A custom Dynamic group can be configured to search for devices with "TASKalfa" in the Model Name. When the system discovers new TASKalfa devices, it updates the custom Dynamic group automatically.

Device Groups: Add a dynamic device group

- 1** Go to **Devices > Groups**.
- 2** Select the **Add group** icon, and then select **Dynamic**.
- 3** Specify the group name and location.
- 4** Configure selection criteria.
 - a) In Criteria, select an option to match all or any of the added properties.
 - b) Select a property.

The list includes all the properties available in Device Manager. To move to a specific property, start typing the property name to limit the list.



Options available for condition and value may vary depending on the selected property.

- c) Select a condition, and then enter a value. To make your search more specific, include the following operators in your value:

Operator	Description
*	Use to match zero or more characters.
?	Use to match a single character.
!	Use for NOT operator. For example, an asset number entry that contains a value of *34 && !*3534 will only include printers with asset number that ends in 34, and exclude printers with asset number that ends in 3534.
	Use for OR operator. For example, an asset number entry that contains a value of *34 *35 will only include printers with asset number that ends in 34 or 35.
&&	Use for AND operator. For example, an asset number entry that contains a value of 43* && *34 will only include printers with asset number that starts with 43 and ends in 34.

- d) If necessary, select + to add another property.



You can also set the dynamic view criteria automatically using advanced search.

- 5 In Customize Columns, organize the display of the information.
- 6 Select **Submit**.

Device Groups: Columns in dynamic groups

When creating or editing a Dynamic group, you have complete control over column selection and order. Selecting columns or groups of columns works the same way as it does in the Device list. Use the Organize columns drop-down (+) list to select or deselect column groups (default is for Common columns plus General, as with the Device list page). You can select individual columns with check boxes as well. Once you've made your selections, you can arrange them using the list of columns under the drop-down list.

That list shows all the columns that you've already selected in their default sequence. There are up and down arrows on the right side of the box. Select any column name and use the up and down arrows to reposition it in the list. To remove a selected column, select **X** by the selected name.

Device Groups: Add a fixed device group

A fixed group is a custom group that includes printers selected from an existing group. For example, you can use this feature to select specific printers, and then add them into a custom fixed group. You can also organize the fixed group by adding it into a folder.

- 1 Go to **Devices > Groups**.
- 2 Select the **Add Group** icon, and then select **Fixed**.
- 3 Add or remove printers.
- 4 Specify a group name, and then select **Submit**.

Device Groups: Import fixed device groups

- 1 Go to **Devices > Groups**.
- 2 Select the **Add group** icon, and then select **Import fixed groups**.
- 3 Specify the appropriate .csv file to upload, and then select **Upload File**.



- If the uploaded file contains headers, then select **Skip first row as header** to exclude the header row from being imported.
- If a valid .csv file is uploaded, then a preview of device groups to be imported is displayed.

- 4 In Device information, select one of the following information included in the .csv file:
 - **IP address**
 - **Host name**
 - **Serial number**
- 5 Select **Import**.

Device Groups: Add a folder

Devices > Groups

Folders are containers of groups that help you to organize groups into hierarchies.

- 1 Select the Add Folder icon.
- 2 Specify a name and select a location from the drop-down list.
- 3 Select **Add**.

Device Groups: Delete a device group

Devices > Groups

- 1 Select the **Delete** icon (trash can) by the group to delete.
- 2 Select **Yes** on the next screen.

Device Groups: Delete a device group folder

Devices > Groups

- 1 Select the Delete icon (trash can) by the name of a folder to delete.
- 2 Select **Yes** on the next screen.
Groups stored in that folder are also deleted.

Device Groups: Download

Devices > Groups

You can download a list of devices for a selected group. The .csv formatted file includes device and toner information.

- 1 Select a group from the Groups List panel.
- 2 Select devices in the list or select none to download the entire list.
- 3 Select **Export Group** at the bottom of the panel.
- 4 Depending on the device selection, you can choose to export selected or all group devices.
- 5 Select **Yes**.

Device Groups: Duplicate a device group

Devices > Groups

You can create a copy of a fixed or dynamic group. This is useful if you want to create a new group that is only slightly different from an existing group.

- 1 Select a group from the Groups List panel.
- 2 Select **Clone group**.
The new group, named Copy (#) of [original name] is added to the same folder.
- 3 Select **Edit**. Edit the new group, rename, and change criteria, as needed after cloning.

If you clone a Fixed group, you can only change the name and folder location.

Device Groups: Edit a device group

- 1 Go to **Devices > Groups**.
- 2 From Group List, select a fixed or dynamic group, and then select the **Edit** icon.
- 3 Do either of the following:
 - For fixed groups, add or remove printers, modify the group name, and then select **Submit**.



Printers already added in the group are selected automatically.

- For dynamic groups, modify the settings, and then select **Submit**.



Deleting a printer from any group moves it into Deleted devices, removes it from all groups, and makes the printer undiscoverable.



To move a group to a folder, select a group, select the **Move** icon, select a destination, and then select **Yes**. You can select the up and down arrows to change the group order.

Device Groups: Rename a device group folder

- 1 Select a folder.
- 2 Select **Edit**.
- 3 Edit the folder name in the edit box, and press **Enter** to save.



To exit edit mode without change, you must still place your cursor in the name field and press **Enter**.

Add devices

With this feature you can scan networks for printers. When new printers are found, the application updates its database with information about the printers. You can add single or multiple printers manually, or schedule it to run automatically on a set date or based on configured triggers.

All found printers are added to Device Manager. If you want to exclude one or more printers, then delete them from the Device list.

- 1 In Devices, select **Add devices > Add devices now**.



To reuse available discovery settings, select **Saved discovery settings**.

2 In Discovery method, select one or more of the following:

By local network

Search for printers within your network. Select **IPv4** or **IPv6**.

By IP address or host name

Search printers using their IP address or host name. Enter the IP address or host name of the printer. Select **+** to add another printer, or **-** to remove the printer.

By IP address range

Search for printers using the specified IP address range. Enter the starting and ending IP addresses. Select **+** to add another IP address range, or **-** to remove the IP address range.

By importing a list

Search for printers listed in the imported .txt or .csv file. Select **DROP FILES TO UPLOAD**, browse to the .txt or .csv file, then select **Upload file**.



- The imported file can contain a list of IP addresses, hostnames, or a combination of both.
- The file must contain a header line with **IP address** or **Host name** column headers. A device list exported from Net Viewer or Net Admin will have the correct format.
- When importing a list, a preview of the list is shown after browsing and opening the file. If the file is invalid, then no preview is shown.
- If the file contains both IP address and host name, then Device Manager uses whichever appears first.

3 If necessary, do the following:

- Select **Skip optional NICs** to skip discovery of optional network interface cards (NIC) installed in the printer.
- Modify communication settings.

4 In Device Login, select **Local authentication** or **Device settings**, then if necessary, change the user name and password.

5 Do one of the following:

- Select **Run** to start discovery using the current settings.
- Select **Save Settings** to save the current settings for later use. Enter a setting name, then select **OK**.
- Select **Reset** to cancel any changes made to the settings.
- Select **Cancel** to cancel the activity and close the dialog box.

A progress window of the discovery process is shown with the time remaining estimate. Closing this window does not affect the discovery process. Discovery progress is also shown in the Task tab.

Devices: Enable smart discovery

Smart discovery runs in the background, once a day, at a time determined in the Device Manager Maintenance component.

Smart discovery reduces the need for full-range discovery in networks that have devices that fail frequently. It uses the following baselines:

- Find a range of IP addresses where printers have been discovered. Select a subset in the middle of these ranges to focus.
- If there are printers outside of the ranges with the Not connected status, then discover the printers individually.
- Discover the following groups:
 - Each range of IPs where there may be missing printers.
 - The group of printers outside those ranges with the Not connected status.

To enable, do the following:

- 1** Select **System > System Settings > Function Settings**.
- 2** Select **Enable smart discovery**.
- 3** Select **Save**.

Devices: Add devices using saved discovery settings

Devices > Add devices

When you select Saved discovery settings, you have a choice of previously configured discovery options.

- 1** Select **Add devices > Saved discovery settings** in the Device list.
- 2** Select the check box for a saved setting. Select **Add** to create new settings to save. Select **Edit** to make changes to previously saved settings. Select **Delete** to delete settings
- 3** Select **Run** to start discovery using the saved settings.

The Discovering Devices progress screen shows a progress bar (% complete) with a Time remaining estimation.

There are three buttons on this screen:

- **Save Settings...**: Saves the current settings
- **Close**: Closes the progress display without canceling the task
- **Cancel**: Cancels the activity and closes the dialog box

Devices: Automatic discovery

Devices > Add devices > Saved discovery settings

Configure automatic device discovery to run on a schedule. Follow these steps to configure and use Automatic discovery:

- 1** Select **Add devices > Add devices now** in the Device list.
- 2** Set discovery parameters as needed. When you have an acceptable set of conditions, select **Save Settings**.
- 3** Create a settings name, and select **OK**.
- 4** On the Saved discovery settings screen, select the check box of the settings you just saved and select **Edit**.
- 5** Scroll down to the Automatic Discovery area.
- 6** Enable Automatic Discovery by setting the **On/Off** switch to **On**.
- 7** Select the check box by **On recurring schedule**.
- 8** Select the schedule from one of the following options:

Daily

Time of day

Weekly

Day of the week and time of day

Monthly

Select a number day of the month or the last day of the month and the time of day

- 9** Select **Save**.

To run a scheduled discovery immediately, select the Saved discovery and select **Run**.

Devices: Switching between Wi-Fi and wired connection

If a device switches connection type between wired and Wi-Fi, then Device Manager will no longer connect to the device, as the original detection method has changed. To restore the connection, use the following procedure:

- 1** Select **Devices > List**.
- 2** Select the check box for the desired device and select **Delete devices**.
- 3** Select **Add devices > View deleted devices**.
- 4** Select the device and select **Include Device**.
- 5** Select **Add devices > Add devices now** and select **Run**.

Devices: Restore deleted devices

Device list > Add Devices > View deleted devices

When you restore deleted devices in the Deleted Devices list, you must discover and add them again in Device Manager.

- 1 Select **Add devices > View deleted devices**.
- 2 Select the check boxes for one or more devices in the Deleted Devices list.
- 3 Select **Include Device**.
- 4 Select **Close**.
- 5 Select **Add devices > Add devices now**.
- 6 Run the discovery.

Select **Download Log** to download a list of deleted devices in a zipped .csv file. The file shows the following information: Model name, Serial number, IP address, Host name, and Description.

Devices: Delete devices

When you delete a device from a device list, Device Manager places it in a Deleted devices group. Remove devices to make them non-discoverable for security purposes. The Add devices task cannot find deleted devices, and Device Manager cannot modify deleted devices.

- 1 From any device group (default or custom), select one or more devices using the check boxes.
- 2 Select **Delete devices**.
- 3 Select **Yes** to confirm.



You can delete devices from any group. The effect is global, affecting all groups. If you delete a device from a custom group (fixed or dynamic), it is removed from all other groups. If you then restore that device, it reappears in all groups that previously showed it. You can restore deleted devices only from the Deleted Devices list, accessed from the Add devices menu.

Device Home on a single device

Devices > Device home

Device Properties > Device home

Devices that contain web servers can display a web page containing information about the device's status and settings. The layout and information shown on this page differs by device model. Select a device or start from the Device Properties page, and

select **Device home** to open the web page for that device. (This action only works for single devices, not for groups or multiple device selections.)

Refresh

With one or more devices selected in the Device list, select **Refresh** to update information.

Create tasks

You can create tasks for one device, multiple devices (using the check boxes), or entire groups (select a group and do not check any individual devices) in the Device list. Configure a task to run immediately, at a scheduled date and time, or triggered by selected Device Manager events. Select tasks from the Create task drop-down list:

- Restart devices
- Firmware upgrade
- Device settings
- Configurations (configure multiple operations to run as a single task)

See sections about each task for detailed information about configuration.

Event triggers

Device Manager uses the following events as triggers for running tasks:

Alert detected	Select from the following alert types: <ul style="list-style-type: none">• Paper jam• Cover is open• Toner is low• Toner is empty• Low paper• No paper• Waste toner is almost full• Waste toner is full• Call for service• Maintenance kit change• Offline• Not connected• Needs attention
Counter reached	Set counter thresholds for: Total pages, Total black & white pages, Total full color pages, Total single color pages, Total single color pages, Total printed pages, Total scanned pages, or Total copier pages

Firmware version becomes	Select trigger based on Firmware type and Firmware version: <ul style="list-style-type: none"> • System firmware • Scanner firmware • Fax Port 1 firmware • Fax Port 2 firmware • Panel firmware • Browser firmware • Engine firmware
Toner level reached	Select Black toner level, Magenta toner level, Cyan toner level, Yellow toner and set a level number (0-100)

After selecting the event to use as a trigger, select the trigger conditions. Choices are:

- On every occurrence
- After number of occurrences: select a number of X events that occur in a day (applies only to alerts)
- After event remains unresolved for: select a number of hours or days (applies only to alerts)

Panel Note

A Panel Note contains a title and a body that can be sent for display on the device front panel and the Message Board in the device's embedded web server.

You can create a Panel Note in Device Properties, a Multi-Set Configuration, and in Create task. In Device Properties, Panel Notes do not have the scheduling feature found in the other options. In Multi-Set Configuration settings, you can replicate Panel Notes from other devices.

The previous 10 posted panel notes can be edited and reused. You can enable and disable panel notes and the Message Board on the device's embedded web server. To turn off the Message Board, clear the **Enable Disable** check box, select **Submit**, select **Submit** again, and select **Close**.

You can prioritize panel notes in the Panel Note list. Prioritization determines what message in the list is sent and displayed first. Each Message type for Panel Note has an associated color code and an icon which is displayed in the Message Board list.

Creating a Panel Note for a Single Device

- 1 In the Device list, select a device under **Model name**.
- 2 Select **Panel Note**.
- 3 Select **Add**.
- 4 Enter a Title.

- 5 Enter a note in the Body text.
- 6 Select the **Show priority** check box to show the note in an exclusive window on device panel first.
- 7 Select a **Message type** in the drop-down: **Normal**, **Alert**, **Prohibition**. The selected Message type determines the icon accompanying the message on the web server.
- 8 Select a **Device to show** location in the drop-down: **Hide**, **Panel**, **Web server**, **Panel and web server**. The Web server refers to the Message board that must be enabled in the Command Center RX UI. Panel refers to the device's operation panel.
- 9 Select a **Place to show** location on device's operation panel: **Home**, **Log in**, **Home and Log in**. Home refers to the home screen of the device's operation panel. Log in refers to the login screen of user login administration.
- 10 Select **OK**.
- 11 Select **Submit**.

Creating a Panel Note as a task

- 1 Select two or more devices.
- 2 Select **Create task > Panel note**.
- 3 Select **Next**.
- 4 Select **Add**.
- 5 Enter a **Title**.
- 6 Enter a note in the Body text.
- 7 Select the **Show priority** check box to show the note in an exclusive window on device panel first.
- 8 Select a **Message type** in the drop-down: **Normal**, **Alert**, **Prohibition**. The selected Message type determines the icon and color accompanying the message on the web server.
- 9 Select a **Device to show** location in the drop-down: **Hide**, **Panel**, **Web server**, **Panel and web server**. Web server refers to the Message board that must be enabled in the Command Center UI. Panel refers to the operation panel of the device.
- 10 Select a **Place to show** location on device's operation panel: **Home**, **Log in**, **Home and Log in**. Home refers to the home screen of the device's operation panel. Log in refers to the login screen of user login administration.
- 11 Select **Next**.

- 12** Select a schedule and select **Next**.
- 13** Modify the **Name** and add a **Description**.
- 14** Select the **Receive notifications** check box.
- 15** On the Confirm Details page, select **Apply**.

Upgrading device 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.




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** In **Devices > Device list**, select one or more printers.
- 2** Go to **Create task > Firmware upgrade**.
- 3** Review or modify the selections, and then select **Next**.



If multiple printers are selected, then make sure that the printers belong to the same model group.

- 4** Select either of the following:

Option	Actions
Upload from local file system	<p>Select and upload a valid firmware package.</p> <p> <u>Uploaded firmware packages are saved in the file server for later use.</u></p>
Select from the file server	<p>Browse and select from the available firmware packages that have been previously uploaded to the file server.</p>

- 5 Select **Next**.
- 6 If necessary, resolve any conflicts, then select **Next**.
- 7 Specify other upgrade options:



Options may vary depending on your devices or selection.

- Schedule
- Trigger
- Retries
- Task details
- Notifications

- 8 Select **Next**, and then review the warning.
- 9 Acknowledge the warning, and then select **Apply**.

Leave the progress window open to see the status of devices being upgraded.

- Any Device: Processing times may vary.
- IB-2x: No indication of the upgrade appears on the device operation panel. Check the firmware version in Firmware view, or check the upgrade status in Tasks.

Upgrade Error Indicators

- Any Device: The upgrade results are recorded in the log file as Failed.
- System: The device failed the power-on self-test.
- FAX: This function is not working.
- IB-2x: No link light appears. Option or Network does not appear in the Interface menu on the device operation panel

Upgrade Error Recovery

- System: You must replace the DIMM in the device. If the old DIMM is not physically damaged, you can erase and reload it using a DIMM writer.
- FAX: You must replace the FAX board.
- IB-2x: A special recovery mode for the IB-2x called Boot Loader mode is available. You can use a jumper setting to set IB-2x to Boot Loader mode: SW1 on IB-20/21 and IB-21E, or J2-1 on IB-22. Once in Boot Loader mode, you can use a Windows utility named IBVERUP to load a new firmware file.

Device Settings: Multiple devices

- 1 Select check boxes for individual devices in the Device list or select a Group in the Groups list.
- 2 Select **Create task**.
- 3 Select **Device settings**.

- 4 Confirm the selected devices, and select **Next**.
- 5 Select a method, and select **Next**.
Methods:
 - New
 - From source device
 - From source file
- 6 On the Settings screen, add all of your device settings. Select **Next**.
- 7 On the Schedule screen, configure schedule options. Select **Next**.
- 8 Enter a task name and description.
- 9 Select the check box for **Receive notifications** (cleared by default) to be notified when the task finishes, and select **Next**.
- 10 On the Confirm details screen, review the settings. Select **Back** to make further changes to the settings or **Apply** to accept.
- 11 On the Tasks tab, check the Active tab to view a task that is still running. Check the Scheduled tab to view a scheduled task or review results in the Completed tab.

Device Settings: Tasks

With Device settings, you can send configuration parameters to one or multiple devices simultaneously, use a device as a template for resetting selected parameters on multiple devices, and save settings in a file to use for future resets. Major settings areas (each having additional settings) are System, Default, and Network.

Device Settings: Scenarios

There are several ways to update settings for one or more devices in Device Manager.

Device settings scenarios:

-
- With a single device selected, create new settings.
 - With multiple devices selected, create new settings.
 - After creating settings, save them to a zipped ("source") file.
-
- With a single device selected, select a source device (on intermediate "Source" screen) and use its settings
 - With multiple devices selected, select a source device (on intermediate "Source" screen) and use its settings.
 - After creating settings, save them to a zipped ("source") file.
-
- With a single device selected, select a previously saved source file
 - With multiple devices selected, select a previously saved source file
-

Note that if you only need to use Device Settings for a single device, you can access a simplified wizard by selecting the Device Properties icon for that device and then selecting **Device Settings** from the Device Properties screen.

Create New

The Create New method starts from a set of all default values, all cleared. Make changes to preferred settings by selecting the boxes and entering new settings to apply to the target devices.

- 1 On the Settings screen, configure the selected settings. You can scroll through All settings, or filter your choices using System, Default, or Network.
- 2 Save your selections to a file, if wanted.
- 3 Select **Next**.

Create from source device

This method loads settings from the source device and provides the opportunity to make changes to the target devices.

- 1 Select a device from the list to use as the source for settings changes and select **Next**.

You can search the list on Model name, Serial number, IP address, or Description.

Wait while Device Manager establishes a connection to the device and loads the settings.
- 2 On the Device Settings screen, configure selected settings. You can scroll through All settings, or filter your choices using System, Default, or Network.
- 3 Save your selections to a file, if wanted.

Create from source file

- 1 On the Source screen, browse to select a settings file and select **Next**.
- 2 Review the selected settings on the Device Settings screen.

You may change or add additional selections here, as well. You can scroll through All settings, or filter your choices using System, Default, or Network.
- 3 If you make any changes to the settings from the original source file, you can save your selections.

Device settings preview

To check that selected settings are applicable to the devices selected, use the Preview function.

- 1 Select **Preview** on the Device Settings screen.

- 2 Select a device model from the drop-down list.
- 3 Review the selected settings and notes to confirm that each is supported on the selected device



If no selected settings are supported, the Preview screen will be blank for the selected device.



If you do not see a setting reflected for a particular device in the Preview, or the Preview shows that the model does not support the selected property or setting, you may consider removing that device from the list of devices for this action. Device Manager will skip unsupported settings when Device Settings runs.

- 4 Make any needed settings changes and select **Next** to continue.

Save Device Settings to a file

- 1 On the Method screen, choose **New** or **From source device**.
- 2 Configure the settings.
- 3 Select **Save to file**.

The downloaded zip file includes the selected device settings in .xml format. If you changed settings in only one of the sections, the Save to file selection downloads a single .xml file, like "DeviceSystemSettings.xml."

Device Settings: Single device

Device Properties > Device settings

When you select Device Settings in the Device Properties tab, Device Manager reads and displays the device's settings.

- 1 In Device Properties, select **Device settings**.
Wait while Device Manager establishes a connection to the device and loads the settings.
- 2 Change settings as needed. You can save your changes to a file for future use.
- 3 Select **Next**.
- 4 Review your choices on the Confirm details screen and select **Apply**. You can also go **Back**, or **Cancel**.

Configurations

Allows you to set up multiple device actions to run on one or more devices. You can schedule the Configuration to run on a predefined date and time, or configure event triggers to start a multi-configuration session.

To access Configurations, select one or more devices, and then select **Create task > Configurations**.

You can select different sources for your configuration file:

Replicate from device

Copy another device configuration file.

Upload from file

Use a saved configuration file from your computer.

Create new

Create a new configuration file. After creating and running the configuration file on selected devices, you can save and use it for another device or device group. The following configurations are saved:

- Device settings
- Restart devices
- Address book
- Document box
- Users and groups

From Multi-Set Configurations, you can select one or more of the following operations for selected devices:



Some operations are available only on some devices.



- Device settings, application actions, and firmware upgrade can cause damage to incompatible devices.
- Restarting the device at the wrong time can interrupt printing operations.
- Address book can be overwritten or deleted.
- Keep in mind that while you may see 10 devices listed in a dynamic or default group when you set up a Configuration task, the schedule or event-triggered action of the task may occur when additional devices have been added or removed from the group.

Device settings

Configure settings, such as send settings, scan basic, email SMTP, and more.

Remote service settings

Configure settings when connecting to the device remotely.

Certificate management

Delete, import, or assign certificates. You can also enroll and unenroll certificates for automatic renewal with Simple Certificate Enrollment Protocol (SCEP).

Restart devices

Restart the device, or the device network interface. Restarting the device network interface will not restart the device, only the network interface card for the device is restarted.

Application

Install, activate, deactivate, or upgrade applications.



The General Data Protection Regulation (GDPR) sets rules for the handling of personal identification information on all citizens in the European Union (EU).

If you are in a geolocation where the GDPR applies, you are shown the Data Processing Terms and Conditions screen during installation of an application. Select **OK**, to activate the license for the application.

Address book

Configure and manage address book contacts.

Firmware upgrade

Upgrade the firmware to another version.

Document box

Configure and manage document boxes.

Optional functions

Enable optional functions available for the device.

Panel note

Configure and manage notes available on the device control panel.

KFS registration

Configure connection settings and login information for connecting to KFS.

Users and groups

Configure and manage users and groups for the device.

Send data

Configure settings for sending device information.

Configurations: Create new configurations

- 1 From the device list, select devices or groups, and then select **Create Task > Configurations**.
- 2 Review devices selections, and then select **Next**.
Clear check boxes to remove devices.
- 3 Select **Create new > Next**.
- 4 Select one or more operations to use in the configuration. For more information, see *Configurations*.
- 5 From the left pane, navigate to your selected operations, configure additional settings, and then select **Next**.



- For more information on each operation, see the corresponding topics in this *User's Guide*.
- If any of the operations require user intervention, then a red exclamation point is displayed.
- You cannot proceed until each operation has a green check mark.

- 6 Configure the schedule or trigger to run your configuration, do one of the following:
 - To run the configuration immediately, select **Now**.
 - To run the configuration on a predefined date and time, select **Later**.
 - To run the configuration when a specific event occurs in the device, select **On event occurrence**.



If you want to run the configuration again at a given interval when the operation encounters an issue, then enable **Retry**.

- 7 Select **Next**.
- 8 Enter the task name and description, and then select **Next**.
To receive an email notification, select **Receive notifications**.
- 9 Review configuration details, and then select **Apply** to run the configuration depending on the trigger or schedule.
To save the configuration for reuse, select **Save to file**.





If you saved the configuration, then the configuration will exist even if the process is canceled.

To view your configuration task, select **Tasks**, and then select either **Active** or **Scheduled**.

Configurations: Replicate configurations

- 1 From the device list, select devices or groups, and then select **Create Task > Configurations**.
- 2 Review devices selections, and then select **Next**.
Clear check boxes to remove devices.
- 3 Select **Replicate from device**, select either **Custom** or **Express**, and then select **Next**.
- 4 From the list, select the device from which the configuration is copied, and then select **Next**.
- 5 Do either of the following:

Condition	Actions
Custom is selected	<ol style="list-style-type: none"> a. Select one or more operations to use in the configuration. For more information, see <i>Configurations</i>. b. From the left pane, navigate to your selected operations, configure additional settings, and then select Next. <div style="margin-top: 10px;">  <ul style="list-style-type: none"> For more information on each operation, see the corresponding topics in this <i>User's Guide</i>. If any of the operation requires user intervention, then a red exclamation point is displayed. You cannot proceed until each operation has a green check mark. </div>
Express is selected	<p>Device manager reads the configuration of the selected device, and automatically set the configuration file for your device.</p> <div style="margin-top: 10px;">  <p>You cannot change the settings copied from the selected device.</p> </div>



The restart type is automatically set to **Device**, because the Restart device operation is not a setting on the device.

- 6 Modify the schedule or triggers as needed, and then select **Next**.
To run the configuration again at a given interval when an error occurs, enable **Retry**.

- 7 Modify the task name and description as needed, and then select **Next**.
To receive an email notification, select **Receive notifications**.
- 8 Review configuration details, and then select **Apply** to run the configuration depending on the trigger or schedule.
To save the configuration for reuse, select **Save to file**.



If you save the configuration, then the configuration will exist even if the process is canceled.

To view your configuration task, select **Tasks**, and then select either **Active** or **Scheduled**.



Configurations: Upload configurations

- 1 From the device list, select devices or groups, and then select **Create Task > Configurations**.
- 2 Review devices selections, and then select **Next**.
Clear check boxes to remove devices.
- 3 Select **Upload from file**, and then select either **Custom** or **Express**.
- 4 Specify the location of the saved multi-set configuration .zip or .xml file, and then select **Upload file > Next**.



- You can use multi-set configuration files created by Network Print Monitor or MSTe.
- Device Manager reads the saved configuration options and operations from the file, and then imports information that was saved with the settings, such as task name, description, trigger, and more.

- 5 Do either of the following:

Condition	Actions
Custom is selected	<p>a. Select one or more operations to use in the configuration. For more information, see <i>Configurations</i>.</p> <p>b. From the left pane, navigate to your selected operations, configure additional settings, and then select Next.</p> <hr/> <p> • For more information on each operation, see the corresponding topics in this <i>User's Guide</i>.</p> <p>• If any of the operation requires user intervention, then a red exclamation point is displayed.</p> <p>• You cannot proceed until each operation has a green check mark.</p> <hr/>
Express is selected	<p>If the following operations are in the uploaded configuration file, then the available operation is added to your configuration.</p> <ul style="list-style-type: none"> • Device settings • Restart devices • Address book • Document box • Users and groups <hr/> <p> You cannot change the settings in the uploaded configuration file.</p> <hr/>

- 6** Modify the schedule or triggers as needed, and then select **Next**.
To run the configuration again at a given interval when an error occurs, enable **Retry**.

- 7** Modify the task name and description as needed, and then select **Next**.
To receive an email notification, select **Receive notifications**.

- 8** Review configuration details, and then select **Apply** to run the configuration depending on the trigger or schedule.
If necessary, to save the configuration for reuse, select **Save to file**.



If you save the configuration, then the configuration will still exist even if the process is canceled.

To view your configuration task, select **Tasks**, and then select either **Active** or **Scheduled**.

Configurations: KFS Registration

The application lets you choose a Multi-Set Configuration for KFS Registration in selected devices. Before you register devices in KFS, you need the registration URL for KFS and the access code of the KFS group to which devices are registered. If you add your KFS user credentials, devices are registered as managed in KFS. In contrast, devices registered without user credentials have a management status of pending, which enables KFS users to monitor device logs and counters. A Managed status means the KFS user can change maintenance mode and device settings, send files, retrieve snapshots, and update firmware.

If a proxy is used, you must set the Hostname, Port, Username, and Password in the Multi-Set configuration.

Enrolling certificates in SCEP

- 1 From the device list, select devices or groups, then select **Create Task > Configurations**.
- 2 Review or modify your selections, then select **Next**.
- 3 Select **Create new > Next**.
- 4 Select **Certificate Management**, use the arrows to navigate to **SCEP enrollment**, then select **Next**.
- 5 Review or modify the available options:

Set SCEP Settings

These settings have the same configuration fields in Certificate Server Configuration. You can also import a previously issued Certificate Authority (CA) zip package.



- Make sure to set the preferred CA server type and enter the correct CA server URL.
- You can also configure SCEP server in **System > Security > Configure SCEP**.

Device certificate slot

Select the preferred device certificate slot.



- To assign a certificate a protocol, select **Assign device certificate protocols**. In Assign protocols, select one or more protocols.
- A device cannot have one protocol assigned to two slots.

Certificate signing request

You can configure the attributes of the request that will be sent to enroll the certificate.

Enter challenge password

Enter the challenge password (CP) used during certificate enrollment on the CA server.

- If CA server supports using the same CP for enrollment of each certificate, select **Enter the single password for all certificates**.
- Select **Enter the challenge password for the selected devices** and enter multiple unique CPs equal to the number of devices selected, then select **Add**.

6 Select **Next**.

If necessary, complete other selected configuration items.

7 Modify the schedule or triggers as needed, then select **Next**.

To run the configuration again at a given interval when an error occurs, select **Retry**.

8 Modify the task name and description as needed, then select **Next**.

To receive an email notification, select **Receive notifications**.

9 Review configuration details, then select **Apply**.

To save the configuration, select **Save to file**.



The configuration will be saved even if the process is canceled.

Unenrolling certificates in SCEP



This feature is not available if none of the selected devices or groups do not have any devices enrolled in SCEP.

1 From the device list, select devices or groups, and then select **Create Task > Configurations**.**2** Review or modify your selections, then select **Next**.**3** Select **Create new > Next**.**4** Select **Certificate Management**, then use the arrows to navigate to **SCEP unenrollment**, then select **Next**.**5** Select any of the available options:**Unenroll all certificates**

Remove certificates enrolled in selected devices from monitoring and automatic-renewal.

Clean certificates

Remove expired certificates related to selected devices from monitoring and automatic-renewal.

You can see the following information related to the selected devices:

- Currently active certificates
- Expired certificates
- Total certificates

6 Select **Next**.



If necessary, complete other selected configuration items.

7 Modify the schedule or triggers as needed, then select **Next**.

To run the configuration again at a given interval when an error occurs, select **Retry**.

8 Modify the task name and description as needed, then select **Next**.

To receive an email notification, select **Receive notifications**.

9 Review configuration details, then select **Apply**.

To save the configuration, select **Save to file**.



The configuration will be saved even if the process is canceled.

Send Data

The Send Data feature allows you to send file and text commands to devices. Accessed through Multi-Set Configurations, the feature allows sending data and PJI commands via text, file, or both. When using PJI commands, you must prepend the messages with the 0x1b hex string to specify the command start.



Send Data only works through Configurations. In the Select Configuration Source screen, you cannot use Replicate from device or Upload from file.

To use the Send Data feature, follow these steps:

- 1 With one or more devices selected, select **Create task**, and then **Configurations**.
- 2 Select **Next**.
- 3 Select **Create new**, and then **Next**.
- 4 Select **Send Data** (you may select other operations at the same time), and then select **Next**.
- 5 For Transmission Method, select from three methods: Default TCP port, Specified TCP port, or IPPS (and specify the path).
- 6 For Send Text, enter PJI commands with the command start hex string. Sample:

```
0x1b%-12345X@PJI JOB NAME="asd.aa"
```

```
@PJI SET JOBNAM="asd.aa"
```

```
@PJL SET HOLD=KUSERBOX @PJL SET KUSERBOXID="0001"  
@PJL SET KUSERBOXPASSWORD="  
{#FILE#}  
0x1b%-12345X@PJL EOJ NAME="asd.aa"
```

- 7** Alternatively, use the **Send File** tab to upload a text file of commands. You can drag and drop or browse to locate the file, and then select **Upload File**.
- 8** On the Preview tab, review the Transmission Method, the Source (which will show either the file name or the text you entered) and the selected devices with status indicators (whether the device supports the operation).
- 9** Select a schedule and select **Next**.
- 10** Modify the **Name** and add a **Description** as desired.
- 11** Select the **Receive notifications** check box.
- 12** Review options on the Task screen, and select **Next**.
- 13** On the Confirmation screen, select **Apply**.

Multi-Set Template Editor

With Multi-Set Template Editor, you can create or change the template files. The template files specify settings for particular groups of devices that are managed by Device Manager. The Multi-Set function in Device Manager applies the templates to devices on a network.

Template files in .xml or .zip format are specific to groups of device models, and to groups of settings shared by those models.

.xml format contains one Multi-Set setting.

.zip format can contain multiple Multi-Set settings.

.xml template files created in Device Manager can also be used.

Several template files can be displayed at one time. You can select a file and select **Edit** to view and change the settings.

Installing Multi-Set Template Editor

The Multi-Set Template Editor installer can be downloaded from Device Manager.

- 1** Select **Create task > Open the Multi-Set Template Editor > Download**.
- 2** Once the zip file downloads, extract to a folder on your computer.
- 3** Open the extracted folder and open Setup.exe to install MSTe.

The next time you select **Create task > Open the Multi-Set Template Editor** in Device Manager, the editor will open.

Creating and saving new settings

You can create a new settings file from a blank template. The template appears in **Multi-Set Template Editor** as **Newly Created***.

- 1 Select **Create task > Open the Multi-Set Template Editor > Run**.
- 2 In Multi-Set Template Editor, select **File > New**.
- 3 In the Select target device for Multi-Set drop-down, select the target device group for the template.
- 4 Select **.xml template file** or **.zip template file** as the file type.
For .xml, select a settings option.
For .zip, select more than one settings option.
- 5 Select **OK**.
- 6 Select **Newly Created***.
- 7 Select **File > Save as**.
- 8 Enter a name for the settings file, then select **Save**. You can view the details and download the results of the Multi-Set Template Editor. Select **Details** to view results or select **Export** to save the results to a .csv file.
- 9 Select **Close**.

Editing a Multi-Set Template

You can edit an existing template with updated settings.

- 1 Select **Create task > Open the Multi-Set Template Editor**.
- 2 In Multi-Set Template Editor, select **File > Open**.
- 3 Select an .xml template file or a .zip template file and select **Open**.
- 4 Select an .xml file or .zip file and, select **Edit**.
- 5 Update settings in the open dialog box, and then select **OK**, **Apply**, or **Cancel**.
- 6 Select **File > Save as** to save updated settings to the template file.
- 7 Select **Save**.
- 8 Select **Close**.

You can view the details and download the results of the Multi-Set Template Editor. Select **Details** to view results or select **Export** to save the results to a .csv file.

Adding an existing template file

You can add an existing .xml template file to a .zip template file.

- 1** Select **Create task > Open the Multi-Set Template Editor**.
- 2** In Multi-Set Template Editor, open an existing .zip template file.
- 3** In the Select target device for Multi-Set drop-down, specify the target device for the template. You cannot select Device Group, only a specific device. Select **OK**.
- 4** Select **Add Existing**.
- 5** Browse to select a template file (.xml) that is not in the .zip file.
- 6** Review your selections and select **Open**.
The setting option appears in the Settings list, where it can be edited.
- 7** Select **File > Save as**.
You can create new settings in a .zip template file by selecting **Create New**.
You can remove a setting option from the .zip template file by selecting it and selecting **Delete**.
- 8** Select **Save**.
- 9** Select **Close**.

Multi-Set template options

Each template supports a set of custom device settings. For some settings, the template can restart the device after the Multi-Set process is finished. Settings vary by device.

Device System Settings

View and edit select device system settings.

Device Network Settings

View and edit select network settings for TCP/IP, security, and network protocols.

Device Default Settings

View and edit select device default settings for print, copy, scan, and fax jobs.

Device Authentication Settings

View and edit select authentication and authorization settings.

Device User List

View and edit select user list settings.

Device Address Book

View and edit select address book settings.

Device Document Box

View and edit select document box settings for users' custom and fax boxes.

Device Network Groups

View and edit select network group settings.

Remote Services Settings

View and edit connection mode and proxy settings for remote maintenance.

Remote Service Settings

In Multi-Set Configurations, Remote Service Settings are replicated from a device or uploaded from a Multi-Set Configuration file and applied to other devices. The configuration files, in .xml or .zip, can be generated by the MSTE (Multi-Set Template Editor). Remote Service Settings include a number of configurations that cannot be changed when they are imported from a file. In addition to Remote Service Settings, you can create Proxy settings in the configuration file, if necessary.

After importing the settings from a file or replicating them from another device, you must select a schedule. The schedule may be based on a trigger. You can also name the task, show a description, and receive notifications after the task complete.

Restart a single device

Device Properties > General > Restart devices

- 1** In the Device list, select a device under **Model name**.
- 2** Select **Restart devices**.
- 3** Select a radio button to select **Device** or **Network** restart.
 - Device restart: Restarts the selected devices
 - Network restart: Restarts just the network interface for the selected device
- 4** Select **Next**.
- 5** Review the details and select **Restart**.

Restart multiple devices

Device List > Create Task > Restart devices

You can restart one or more printing devices or device networks remotely.

- 1** In the Device list, select multiple devices or a group.
- 2** Select **Create task > Restart devices**.

- 3 Review your selections.
 - If you selected multiple devices, you can make changes by selecting the check boxes for devices to restart.
 - If you started from a group, the number of devices in the group is displayed. You cannot make changes.
- 4 Select **Next**.
- 5 Select **Device** or **Network** restart.
 - Device: Restarts the selected devices
 - Network: Restarts only the network interface for the selected device
- 6 Select **Next**.
- 7 Accept the default to run the restart now, configure the restart to run at a specified date and time, or configure event triggers for automated restarts.

If you choose to run now:
- 8 Select **Next** on the Schedule screen.

If you want to set the Restart for a later date/time or configure event triggers:
- 9 Set up the schedule, using date/time or by configuring event triggers, and select **Next**.
- 10 Enter a task name and description.
- 11 Select the **Receive notifications** check box to receive an email after the task finishes.
- 12 Select **Next**.
- 13 Review task details, and select **Restart**.

Select **Download Results** to save the task information in a .csv file to your local system. Select **Close** to close the Progress screen.

You can also go to the Active Tasks tab to view progress, or the Scheduled Tasks tab to view, modify, enable, or disable scheduled tasks.

Device tags

Create tags to assign a short description or information for your printers.

Editing tags for a single device

- 1 Open the edit dialog box, do either of following:
 - From Device list, select a printer, and then select **More > Device tags**.
 - From Devices, open device properties, and then in Tags, select the **Edit** icon.

- 2 In the text box, specify the tag name.



- To add more tags, select +.
- To remove tags, select -.

- 3 Select **Save**.

Editing tags for multiple devices

- 1 From Device list, select multiple printers or a device group, and then select **More > Device tags**.
- 2 Select either to append or overwrite existing tags of selected printers or device group.



Existing tags of selected printers or device group are not displayed.

- 3 In the text box, specify the tag name.



- To add more tags, select +.
- To remove tags, select -.

- 4 Select **Save**.

Device properties

When you select any device on the Device list, the detailed information about that device and options for managing the device are displayed. Tabs shown such as Address Book or Document Box, may vary depending on your device.

From Device Properties, you can view additional information about the device:

General

Displays detailed information about the device.

Counters

Displays the counters for each function the device supports.

Alerts

Displays the alert messages for each issue the device encounters.

Logs

Displays a graphical view of the toner usage and counters.

The following options are also available:

Restart devices

Restarts the device.

Firmware upgrade

Upgrade the firmware of the device.

Device settings

Set additional device settings.

Device home

Go to device home page.

To view the properties of the previous or next device in the device list, select the up and down arrows beside the device model name.

Communication Settings



For KYOCERA printers, make sure that both SNMP and Enhanced WSD protocols are enabled for secure and optimized performance. If either protocol is disabled, then some functions may not work correctly.

Changing communication settings for a single device

- 1** In Devices, select the printer in Device list.
- 2** In Device Properties, under Communication settings, select the edit icon.
- 3** Configure the following settings:

Network interface

Select one of the available network interface cards installed on the printer.



- To add multiple network interfaces for the printer, discover the printer using the different installed network interface cards.
 - To always use the selected network interface for printers with multiple discovered interfaces, select **Always use this interface**.
-

TCP/IP port

Enter a port number from 1024 to 65535.

Secure protocol (SSL)

Select to enable secure connection to your device.

Communication timeout (seconds)

Set the time from 5 to 120 seconds your TCP/IP operation retries before it stops.

SNMP connection retries

Set how many attempts your SNMP operation retries before it stops.

SNMP type

Set the SNMP connection type. Select either **SNMPv1/v2** or **SNMPv3**, then configure additional settings for each type.

Command Center password

Enter the password for accessing the web page of the device.

Authentication type

Select either **Local authentication** or **Device settings**.

Authentication information

Enter the user name and password used for the selected authentication type.

- 4** Select **Save**.

Communication Settings: Change for multiple devices

- 1** Select one or more devices, and then select **More > Communication settings**.
- 2** Make changes as needed to the following settings:

TCP/IP port

Enter a port number from 1024 to 65535.

Secure protocol (SSL)

Select to enable secure connection to your device.

Communication timeout (seconds)

Set the time from 5 to 120 seconds your TCP/IP operation retries before it stops.

SNMP connection retries

Set how many attempts your SNMP operation retries before it stops.

SNMP type

Set the SNMP connection type. Select either **SNMPv1/v2** or **SNMPv3**. Configure additional settings for each type.

Command Center password

Enter the password for accessing the web page of the device.

Authentication type

Select either **Local authentication** or **Device settings**.

Authentication information

Enter the user name and password used for the selected authentication type.

3 Select **Save**.

These changes immediately affect all selected devices or all devices in the group.



The settings shown when you open Communication settings are the default settings that Device Manager uses to communicate with devices. If you make changes for a group or selected devices, and open Communication settings, then the settings are reverted to the default settings.

SNMPv3 and Context name

KYOCERA devices do not require or support SNMPv3 Context names. If a Context name is entered in SNMPv3 communication settings, then a search for KYOCERA devices will fail.

Some non-KYOCERA devices require a Context name when SNMPv3 is enabled. If the Context name is not entered, the search for these devices will fail.

Using SNMPv3 with Ricoh and HP devices

Ricoh and HP devices require a context name when using SNMPv3. To add a context name, follow these steps.

1 Select **Add devices** > **Add devices now** in the Device list.

Select **Saved discovery settings** to reuse available discovery settings.

2 For Discovery method, select **By IP address or host name**.**3** Enter an IP address or host name for the device.**4** In Communication settings, enter values or accept the default settings.**5** For SNMP method, select **SNMPv3**.**6** Enter the **User name** and **Password**.**7** For SNMP authentication, select the method used by the device.**8** Select **SNMP Privacy**.**9** Enter the **Context name** for the device.

- For Ricoh: GWNcS
- For HP: Jetdirect

10 Select **Run**.

Device Properties: General

This screen is divided into functional areas to display information in the following categories:

- Asset number (select the Edit icon to add a number)
- Capabilities
- Communication settings (select the Edit icon to change settings)
- Description (select the Edit icon to add text)
- Firmware versions
- General (printing device image, model, serial number, host name, manufacturer, IP address, MAC address, status and connection date/time)
 - Hover over the Information icon (i) to see a pop up display of options installed on the device
 - Select the hyperlinked status message to jump to the Alerts tab
- Location (select the Edit icon to add text)
- Media Input
- Memory (total memory, RAM disk status, RAM disk capacity, SD card capacity, SD free space)
- Options
- Panel Message
- Polling Intervals
- Tags (select the Edit icon to add text)
- Toner Information (color, name, remaining days, level, and waste toner container)
- Wi-Fi

Device Properties: Counters

Presents count information in a table format for multiple functions and paper sizes for Black & White, Full Color, Single Color printing and a Total column.

Device Properties: Alerts

Presents a table of alert information: Date, Status, Alert Description, Troubleshooting, and Code (PJL code). The system will show all current alert messages per device and up to 15 historical alerts. Status listed will be either Active or Resolved. The Troubleshooting column shows a tip for resolving the alert.

Device Properties: Logs

Shows two charts: Toner Log and Counter Log. If there have been no changes to data in the log on a given day, Device Manager shows only one plot point for that day.

Device Properties: Management

Management has three sub-sections: Applications List, Certificate List, and Optional Functions. If a device does not support a particular feature set, the corresponding management sub-tab will be hidden.

Applications list

Device Properties > Management > Applications List

Displays a list of applications with the following information:

Settings Name	Description
Name	Application name
Version	Application version
License	<ul style="list-style-type: none"> Not used: Application not activated Trial: Application using a trial license Official: Application has been activated
License date	When (date/time) the license was activated
Remaining counts	Number of launches remaining in trial for the app
Trial expiration date	Trial expiration date
Type	<ul style="list-style-type: none"> Resident User initiated
State	<ul style="list-style-type: none"> Ready Running Error

The top row of the Applications List screen has buttons for Install, Upgrade, Activate, Deactivate, and Refresh. There is also a Search box to the right.

Applications: Activate on a single device

- 1 In Devices, select a printer, and then select **Management > Applications List**.
- 2 Select an application with the Not used status in the License column, and then select **Activate**.



You can activate only one application at a time.

- 3 From Activate Application, select **Trial** or **Official**.



- If the application does not have a trial license, then Trial is disabled.

- If Trial is selected, then a license key is not required.

- 4 If Official is selected, then enter a valid license key or product ID. Do either of the following:
 - Specify the appropriate .csv license file, and select **Upload File**.
 - In Product ID/License key, enter the product ID or license key.
- 5 Select **Next > Activate**.

You may close the progress box without affecting the running process, or keep it open to see completion and any error message.

Applications: Deactivate on a single device

Device Properties > Management > Applications list

- 1 Select one or more applications.
- 2 Select **Deactivate**.
- 3 If you want to deactivate and uninstall the application, select the **Uninstall applications** check box. In some cases, **Uninstall applications** may be checked by default when working with older models that do not support deactivation.
- 4 Select **Next**.
- 5 Confirm details and select **Deactivate** to continue.

Applications: Install on a single device

Device Properties > Management > Application list

- 1 Select **Install**.
- 2 Drag and drop or browse to an application package (.pkg) and select **Upload File**.
- 3 Review application name and version, change if not what you expected.
- 4 Select the **Activate application** check box if you want it to activate upon installation.
- 5 Select **Next**.
- 6 Confirm details and select **Next** to continue with installation.

View progress on the next screen, which you can close without affecting the installation.

Applications: Upgrade on a single device

Device Properties > Management > Applications list

- 1 Select an installed application and select **Upgrade**.
- 2 Drag and drop a file, or browse to an upgrade package (.pkg) and select **Upload File**.
You will receive a warning if the file is the same or an earlier version than the one already installed.
- 3 Select **Next**.
- 4 Confirm details and select **Upgrade** to continue with the upgrade.

Certificate list

Device Properties > Management > Certificate List

Displays a listing page of Certificates employed on the device.

Column Name	Description
Certificate number	Device certificate number
Status	<ul style="list-style-type: none">• Active• Inactive
Subject	Identifies entities associated with the public key stored in the subject public key field
Protocols	Protocols that can be used with this certificate (Not used for Root certificates)
Expiration	Certificate's expiration date and time

The top row of the Certificate List screen has buttons for Import, Delete, View, Assign, and Refresh.

The View button displays certificate information for both Device and Root certificates. Select an Active certificate check box and then select **View**. Select **OK** to close.



The Import button will be disabled when the maximum number of certificates are already installed on the device.

Certificates: Actions on the certificate list screen

Device Properties > Management > Certificate List

Actions you can take on certificates depend on the certificate type and status. The following table outlines the actions and conditions:

Certificate Type	Status	Action	Permissions
Device Certificate	Active	Import certificate	Allowed
		Delete certificate	You cannot delete Device certificate 1. All other active device certificates can be deleted.
		View certificate	Allowed
		Assign certificate	Allowed
	Inactive	Import certificate	Allowed
		Delete certificate	Not allowed
		View certificate	Not allowed
		Assign certificate	Not allowed
Root Certificate	Active	Import certificate	Allowed
		Delete certificate	Allowed
		View certificate	Allowed
		Assign certificate	Not allowed
	Inactive	Import certificate	Allowed
		Delete certificate	Not allowed
		View certificate	Not allowed
		Assign certificate	Not allowed

Certificates: Assign a certificate to protocols for a single device

Device Properties > Management > Certificate list

- 1 Select an **Active Device** certificate, and select **Assign**.
The installation location is pre-selected for the chosen certificate.
- 2 In Protocols, select protocols to which you want the certificate to apply.
- 3 Select **Next**.
- 4 Review the details, select **Assign** to complete.

You can close the Progress window without stopping the import. You can also download the import results to a .csv file.

Certificates: Delete from a single device

Device Properties > Management > Certificate list

- 1 Select one or more certificates and then select **Delete**.
- 2 Use the check boxes on the first Delete Certificates screen to make changes, and then select **Next**.
- 3 Review choices on the confirmation screen, select **Delete**.

You can close the Progress window without stopping the process. You can also download the results to a .csv file.

Certificates: Import to a single device

Device Properties > Management > Certificate list

- 1 Select **Import**.
- 2 Select the Certificate type (Device or Root).
- 3 Select the Installation area (Auto or an already configured certificate number).
- 4 Drag and drop or browse to a certificate file, and then select **Upload file**.



For importing Device certificates on a single device, you need both a .pfx certificate file and associated password.

- 5 Enter the password for a Device certificate.
- 6 Select **Next**.
- 7 Review the details, select **Import**.

You can close the Progress window without stopping the process. You can also download the results to a .csv file.

Certificates: View a certificate

Device Properties > Management > Certificate list

- 1 Select an active Device or Root certificate by selecting the check box.
- 2 Select **View**.

Certificates: Multi-Set Configurations

There are a few minor differences in how you work with certificates when using Multi-Set Configurations.

Assign

- 1 Select **Certificate Management** among the Operations buttons.

- 2 Select **Assign** at the bottom of the button. Select **Next**.
- 3 Select one or more protocols in the **Select assigned protocols for device certificate** drop-down list.
- 4 Using the radio buttons, select **Specify subject of the certificate** or **Select a certificate file**:
- 5 Select **Next**.
- 6 Select a schedule and select **Next**.
- 7 Modify the **Name**, add a **Description**, select the **Receive notifications** check box, if desired.
- 8 On the Confirm Details page, select **Apply**.

Delete

- 1 Select **Certificate Management** among the Operations buttons.
- 2 Select **Delete** at the bottom of the button. Select **Next**.
- 3 Select a certificate type in the drop-down list (device or root).
- 4 Using the radio buttons, select **Specify subject of the certificate** or **Select a certificate file**:
- 5 Select **Next**.
- 6 Select a schedule and select **Next**.
- 7 Modify the **Name**, add a **Description**, select the **Receive notifications** check box, if desired.
- 8 On the Confirm Details page, select **Apply**.

Import

- 1 Select **Certificate Management** from the Operations buttons.
- 2 Select **Import** at the bottom of the button. Select **Next**.
- 3 Select a certificate type in the drop-down list (device or root).
- 4 Select the installation area (Auto or a configured device certificate number.)
- 5 Drag and drop or browse for the certificate files.
 - .csv configuration and .zip package files for Device certificate
 - .cer for Root certificate

You can choose to assign device certificate protocols.

- a. Select the **Assign device certificate protocols** check box.
- b. In the Assign protocols tab, select one or more protocols from the drop-down list.

6 Select **Next**.

For certificate import in Multi-Set Configurations, note that the file type is different from what is required when importing for a single device. For Multi-Set, you must use a .zip and .csv file set.

The .csv configuration file should contain the following information:

- Device serial number
 - If the device serial number is duplicated, the row for second and subsequent numbers are ignored
 - If the device serial number does not match with selected target devices, the row is ignored
- File name of certificate file in the .zip package
- Certificate password

The selected .csv configuration should contain at least one serial number that matches any of the selected devices. The .zip package should also contain at least one file described in the .csv configuration.

Optional Functions: Activate

These functions are included in the device firmware.

- 1 In Devices, select a printer, and then select **Management > Optional Functions**.
- 2 Select an optional function with the Not used status in the License column, and then select **Activate**.



You can activate only one function at a time.

- 3 If the function does not require a license key, then select **Yes** to activate.
- 4 If the application requires a license key or product ID, then do the following:
 - a) From Activate License, select **Trial** or **Official**.



- If the application does not have a trial license, then Trial is disabled.
- If Trial is selected, then a license key is not required.

- b) If Official is selected, then enter a valid license key or product ID. Do either of the following:
 - Specify the appropriate .csv license file, and select **Upload File**.
 - In Product ID/License key, enter the product ID or license key.

- c) Select **Next > Activate**.

You may close the progress box without affecting the running process, or keep it open to see completion and any error message.

Address book

The Address Book contains a list of individuals and their contact information that is stored on the device. Each entry for an individual is a Contact, and you can organize contacts into groups. This contact and group information is stored on the device, and is used for faxing and scanning operations.



If authentication is set, accessing the address book requires the correct Login username and Password in the Communication settings for the device.

Address book has three sub-tabs: Contacts, Groups, and One Touch Keys (model dependent) and each tab has a set of function buttons:

- Add
- Delete
- Edit
- Import
- Export
- Refresh
- Duplicate (on Contacts and Groups screens)

Changes made in any of these tabs result in a change to the UI. To complete a change, select **Submit Address Book**.

Column Name	Description
Contacts	Manage individual contacts on the Contacts tab. The listing screen shows contacts.
Groups	From the Groups tab, you can manage groups of users/contacts on the device.
One Touch Keys (model dependent)	You can assign a destination to contacts and groups from the Address Book with the One Touch Key feature. An assigned One Touch Key can be selected on the device's operation panel. The availability and number of One Touch Keys vary depending on your device.



Address Book: Add contacts on a single device

- 1 Select **Devices**, open the device properties, and then select **Address Book > Contacts**.
- 2 Select **Add**.

- 3** In Add Contact, specify the appropriate information for the following settings:



Some settings may be available only in some devices.

Setting	Actions
Name & Number	Specify the following information: Name Name of the contact. Number Unique number assigned to the contact. To use the next available number, select Auto .
Email	Enter the email address.
Basic Information	Specify additional contact information.
FTP	Specify the settings for the FTP shared folder.  You can only add one FTP shared folder. To add another FTP shared folder, add another contact.
SMB	Specify the settings for the SMB shared folder.  You can only add one SMB shared folder. To add another SMB shared folder, add another contact.
Fax	Set the fax settings for the contact.
Internet Fax	Set the internet fax settings for the contact.

- 4** Select **Save**, check if the contact is added, and then select the contact.

- 5** Select **Open Submit Panel > Submit > Submit**.

To save the task information in a .csv file, select **Download Results**.

Address Book: Add groups on a single device

Device Properties > Address Book > Groups

- 1 Select **Add** on the Groups tab.
- 2 Enter a name for the Group.
- 3 Select a number for the group from the drop-down list or allow Device Manager to auto-populate the number field.



Previously assigned numbers do not appear in the list.

- 4 Use the check boxes to select Contacts to add to the Group.
The drop-down list at the right on the column header can serve as a filter to show only users that have data in a selected field. Choices are:
 - SMB
 - FTP
 - Email
 - Fax
 - iFax
- 5 Select **Save**.
- 6 Select **Open Submit Panel**.
The Submit Panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.
- 7 Select **Submit** at the bottom of the panel.
- 8 Select **Submit**.

Select **Download Results** to save the task information in a .csv file to your local system. When you close the progress window, the screen refreshes to show the changes.

Address Book: Add One Touch Keys on a single device

Device Properties > Address Book > One Touch Keys

- 1 Select **Add**.
- 2 Enter a name for the One Touch Key.
- 3 Select a number for the key from the drop-down list.



Previously assigned numbers do not appear in the list.

- 4 Select a destination for the One Touch Key by selecting a radio button by a contact from the list.

The drop-down list at the right on the column header can serve as a filter to show only users that have data in a selected field. Choices are:

- SMB
- FTP
- Email
- Fax
- iFax
- Group

- 5 Select **Save**.

- 6 Select **Open Submit Panel**.

The submit panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.

- 7 Select **Submit** at the bottom of the panel.

- 8 Select **Submit** on the pop-up confirmation.

Select **Download Results** to save the task information in a .csv file to your local system.

Address Book: Delete contacts, groups, or One Touch Keys on a single device

- 1 Select **Devices**, open the device properties, and then select **Address Book**.
- 2 From the Contacts, Group, or One Touch Keys tab, select one or more entries, and then select **Delete**.
- 3 Select **Open Submit Panel**, and then review the entries to be deleted.
To remove an entry from the list, select **X**.
- 4 Select **Submit** > **Submit**.

Address Book: Duplicate contacts or groups on a single device

You can duplicate only one contact or group entry at a time.

- 1 Select **Devices**, open the device properties, and then select **Address Book**.
- 2 From the Contacts, or Groups tab, select an entry, and then select **Duplicate**.
- 3 Select **Open Submit Panel**, and then review the entry.
To remove the entry from the list, select **X**.

4 Select **Submit** > **Submit**.

To save the task information in a .csv file, select **Download Results**.

Address Book: Edit contacts on a single device

Device Properties > Address Book > Contacts

- 1** Select an existing contact by selecting the check box next to it. (You may only edit a single entry at a time.)
- 2** Select **Edit**.
- 3** Add or remove information about the contact. **Number** refers to the record ID, which is not editable.
- 4** Select **Save**.
- 5** Select **Open Submit Panel**.

The submit panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.
- 6** Select **Submit** at the bottom of the panel.
- 7** Select **Submit** on the pop-up confirmation.

Select **Download Results** to save the task information in a .csv file to your local system. When you close the progress window, the screen refreshes to show the changes.

Address Book: Edit groups on a single device

Device Properties > Address Book > Groups

You can change the group name and add or remove contacts in groups.

- 1** Select a group by selecting the check box on the group row. (You may only edit a single entry at a time.)
- 2** Select **Edit**.
- 3** Edit the name of the group, if wanted.
- 4** Add or remove users from the group by selecting or clearing boxes by names of contacts.

The drop-down list at the right on the column header can serve as a filter to show only users who have data in a selected field. Choices are:

- SMB
- FTP
- Email
- Fax

- iFax

5 Select **Save**.

6 Select **Open Submit Panel**.

The submit panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.

7 Select **Submit** at the bottom of the panel.

8 Select **Submit** on the pop-up confirmation.

When you close the progress window, the screen refreshes to show the changes.

Address Book: Edit One Touch Keys on a single device

Device Properties > Address Book > One Touch Keys

1 Select a One Touch Key by selecting the check box on the key row. (You may only edit a single entry at a time.)

2 Select **Edit**.

3 You can change the name of the key or the person/group with which it is associated. You cannot change the Number of the key.

4 Add or remove entries for the key by checking or clearing boxes in the list of contacts and groups.

The drop-down list under the Number field can serve as a filter to show only users that have data in a selected field. Choices are:

- SMB
- FTP
- Email
- Fax
- iFax
- Group

5 Select **Save**.

6 Select **Open Submit Panel**.

The submit panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.

7 Select **Submit** at the bottom of the panel.

8 Select **Submit** on the pop-up confirmation.

Select **Download Results** to save the task information in a .csv file to your local system. When you close the progress window, the screen refreshes to show the changes.

Address Book: Export contacts on a single device

Device Properties > Address Book > Contacts

The Export function creates a .csv with all data from the Address Book. It will execute without waiting for the Submit Address Book confirmation.

- 1 Using check boxes, select contacts to export.
- 2 Select **Export**.

Address Book: Export groups on a single device

Device Properties > Address Book > Groups

The Export function creates a .csv with all data from the Address Book. It will execute without waiting for the Submit Address Book confirmation.

- 1 Using check boxes, select groups to export.
- 2 Select **Export**.

Address Book: Export One Touch Keys on a single device



Device Properties > Address Book > One Touch Keys

The Export function creates a .csv with all data from the Address Book. It will execute without waiting for the Submit Address Book confirmation.

- 1 Using check boxes, select **One Touch Keys** to export.
- 2 Select **Export**.

Address Book: Import contacts, groups, or One Touch Keys on a single device

- 1 Select **Devices**, open the device properties, and then select **Address Book**.
- 2 From the Contacts, Groups, or One Touch Keys tab, select **Import**.
- 3 Do either of the following:

Option	Actions
Manual import	<ol style="list-style-type: none"> Select Manual import. Find the appropriate .csv file to upload, and then select Upload File. Modify the imported information as needed, and then select Save. <div>  Duplicate IDs are overwritten. Select Assign automatically to assign and create new IDs to new and duplicate entries, respectively. </div>
Auto import	<ol style="list-style-type: none"> Select Auto import. Find the appropriate .csv file to upload, and then select Upload File > Save. <div>  You cannot make changes to the imported information and duplicate entries are overwritten. </div>

- 4** Select **Open Submit Panel**, and then review the entries to import.
To remove an entry from the list, select **X**.

- 5** Select **Submit > Submit**.



To get the correct format for a .csv file to import, export a contact list first. You could delete all current contacts from the exported file and add new data to use for an import. Remember that the fields Number and Name are required.

Address Book: Refresh contacts, groups, and One Touch Keys

Device Properties > Address Book

Select **Refresh** to update all Address Book entries: Contacts, Groups, and One Touch Keys. Each Address Book tab has a refresh icon, but the refresh action affects all three entry types.



If you have made changes to Contacts, Groups, or One Touch Keys and have not submitted them, selecting **Refresh** will delete all uncommitted changes.

Address Book: Settings in Multi-Set Configurations

Devices > Create Task > Configurations

You can make all the same changes to device Address Books using Multi-Set Configurations that you can use for a single device, except Export.

With Multi-Set, each tab of the Address Book settings (Contacts, Groups, and One Touch Keys) appears on the left side of the screen, with a listing of all entries read from the device presented with check boxes. Task buttons appear at the top of each tab to Add, Edit, Delete, or Import.

The Enable switch gives you the option to disable configuration changes entirely for each tab. If you set it to Disable on all the tabs, the system displays a warning icon for the Address Book configuration or disables the Next button.

Changes in progress (add, delete, edit, and individual entries to be imported) appear in a Change History area to the right, where you can delete individual changes, if needed.

When making Address Book changes through Multi-Set Configurations, there is an extra tab for Preferences that only applies to Multi-Set. These Preferences settings let you choose how to apply changes to the Address Book. The Preferences choices are:

Full Overwrite

Overwrites the existing address books of devices selected for this Multi-Set operation. It ignores all current settings on the devices, and overwrites all data. A Full Overwrite cannot be undone.

Smart Merge (default/recommended)

Combines existing data on the target devices with source data for the Multi-Set operation (a source device or saved file). Smart Merge performs the merge based on the Number of the address book entry. Where there are duplicate Numbers, Smart Merge overwrites target device data with source data having a matching ID number.

Auto-generate

Keeps all source and target data, creating new Numbers (keeping the same Name) for duplicate entries from the source data (device or saved file) on the target devices.

With Enable set to **On**, no other selections and/or changes made, and the default of Smart Merge selected in Preferences, all source address book entries will be merged or added to the target devices entries.

Device Users

The user list contains the authorized device users and their login information. When user authentication is set, only users with administrator access can use various functions of the device. To access device user functions, go to the device list, select a device, and then select **Users**.

In Users, administrators can modify the following:

Users

Manage authorized device users.

Simple Login Keys

Simplify device login.

Network groups

Manage groups of network users.

Authentication

Select settings for user login, network user properties, password policy, and user account lockout.

You can manage the user list and remove an entry before submitting. If you switch tabs before selecting **Submit Address Book**, then a message appears to abandon uncommitted changes.



To access the user list of a device, the correct login information must be available in Communication Settings. If an administrator password is set for the device, then only an administrator can change the user list.

Device Users: Add users

Device Properties > Users > Users

You can use the list to manage user access to the device.

- 1** In Users, select **Add**.
- 2** Select available device user options under General, Advanced, and Authorization. Login user name and User name are required.
- 3** Select **Save**.
- 4** Perform other Device User operations (add, delete, and edit for Users, Simple Login Keys and Network Groups; plus import for Users, Groups authorization for Network Groups, and options on the Authentication tab).
- 5** Select **Open Submit Panel**.
The submit panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.
- 6** Select **Submit** at the bottom of the panel.
- 7** Select **Submit** on the pop-up confirmation.

When you close the progress window, the screen refreshes to show the changes.

Device Users: Delete users

Device Properties > Users > Users

To delete a device user, select user and select **Delete**. Follow the rest of the steps under Add.

Device Users: Edit users

Device Properties > Users > Users

To edit a device user, select the user and select **Edit**. Follow the rest of the steps under Add.

Device Users: Export a user list

Device Properties > Users > Users

You can save a list of users to a file on your computer or network. Once saved, you can import the file to another device. Device Manager does not export or import Passwords. You must enter them manually.

- 1 In the Users tab, select **Export**.
- 2 Select **Export all users** or **Export selected users only**.
- 3 Select **Continue**.
The selected users are saved in a .csv formatted file to the default download location on your system.

Device Users: Import a user list

Device Properties > Users > Users

You can import a list of device users that was exported from another device. Passwords are not exported or imported and must be entered manually.

- 1 In the Users tab, select **Import**.
- 2 In the Import Users dialog box, drag a valid user file (CSV) into the box, or select the box and browse to find a file.
- 3 Select **Upload File** to import the file, or select **REMOVE FILE** to delete it.
- 4 If the first line of the .csv file contains headers, select **Include file headers** to include them. Clear the check box if you want the first line of the file to be ignored and only the data used.
- 5 To map the columns to the properties, select available options under each property.
- 6 Select **Save**.
- 7 Select **Open Submit Panel**.
The submit panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.
- 8 Select **Submit** at the bottom of the panel.
- 9 Select **Submit** on the pop-up confirmation.

When you close the progress window, the screen refreshes to show the changes.

Device Users: Simple Login Keys

With Simple Login Keys, you can create a number shortcut to bypass the login requirement on a device.

To configure Simple Login settings for your device:

- 1** In the Device list, select a device under **Model name**.
- 2** Select **Users**.
- 3** Select **Simple Login Keys**.

Simple Login Keys: Add a key

Device Properties > Users > Simple Login Keys

- 1** Select **Add**.
- 2** In the Add Simple Login Key dialog box, enter a name.
- 3** For the Key, select the **Next available number** or a **Specific number** and type a number with a range of 1 to 20.
- 4** Select the icon and select one from the grid.
- 5** Select an **Authentication mode**.
 - For Use local authentication, choose **Select**, and then specify the login information.
 - For Use network authentication, specify the login information.
- 6** Select **Enable password login** to require a password at login. Clear the check box to disable the password requirement.
- 7** Select **Save**.
- 8** Select **Open Submit Panel**.

The submit panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.
- 9** Select **Submit** at the bottom of the panel.
- 10** Select **Submit** on the pop-up confirmation.

When you close the progress window, the screen refreshes to show the changes.

Simple Login Keys: Delete a key

To delete a key, select a key name and select **Delete**. Follow from step 7 under *Add*.

Simple Login Keys: Edit a key

To edit a key, select key name and select **Edit**. Follow from step 7 under *Add*.

Device Users: Network groups

With Network groups, you can create and manage groups of network users on the device. You can set printing permissions and restrictions for the group. This is useful when Use network authentication is selected in the Authentication tab.

- 1 Go to the Devices tab.
- 2 In the Device list, select a device under Model name to see the Device Properties.
- 3 Select **Users**.
- 4 Select **Network groups**.

Network Groups: Add a network group

Device Properties > Users > Network groups

You can add user groups to the group list on the device.

- 1 Select **Add**.
- 2 In the Add Group dialog box, enter a Group ID (numerals only) and a Group name.
- 3 Select the Access level.
- 4 Under **Authorization**, select the desired permissions and restrictions. Available options vary by model.
- 5 Select **Save**.
- 6 Perform other Device User operations (add, delete, and edit for Users, Simple Login Keys and Network Groups; plus import for Users, Groups authorization for Network Groups, and options on the Authentication tab).
- 7 Select **Open Submit Panel**.
The submit panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.
- 8 Select **Submit** at the bottom of the panel.
- 9 Select **Submit** on the pop-up confirmation.

When you close the progress window, the screen refreshes to show the changes.

Network Groups: Delete a network group

To delete a network group, select a group and select **Delete**. Follow the rest of the steps under *Add*.

Network Groups: Edit a network group

To edit a network group, select a group and select **Edit**. Follow the rest of the steps under *Add*.

Setting Group authorization

Device Properties > Users > Authentication

You can choose whether all users can operate within permissions set for the group.

- 1** Select **General**.
- 2** In the General section, select the **Group Authorization** check box.
- 3** Select **Save**.
- 4** Select **Open Submit Panel**.
The submit panel opens on the right side of the screen with the information about the change displayed with an **X** in a bubble. Cancel the change by selecting the **X** in the bubble.
- 5** Select **Submit** at the bottom of the panel.
- 6** Select **Submit** on the pop-up confirmation.

When you close the progress window, the screen refreshes to show the changes.

Device Users: Settings in Multi-Set configurations

Managing Device Users in a Multi-Set configuration follows the same basic steps as managing Device Users for a single device from the Device Properties screen. You can manage device Users, Network Groups, Simple Login Keys, and Authentication settings. You can add, edit, delete, and import device Users; add, edit, and delete Network Groups and Simple Login Keys; and change all Authentication settings.

The Enable switch gives you the option to disable configuration changes entirely for each tab. If you set it to Disable on all the tabs, the system will pop up a warning icon for the Users and Groups configuration or disable the Next button.

On the Preferences tab in Multi-Set, there are two options for handling existing data:

Full Overwrite

This option overwrites all data on the device. A Full Overwrite cannot be undone.

Smart Merge (recommended)

This option combines existing data on the target devices with source data for the Multi-Set operation (a source device or saved file.) Smart Merge performs the merge based on the Number of the entry. Where there are duplicate Numbers, Smart Merge overwrites target device data with source data having a matching ID number.



Both Full Overwrite and Smart Merge overwrite existing authentication settings.



With Enable set to On, no other selections and/or changes made, and the default of Smart Merge selected in Preferences, all source entries will be merged or added to the target devices entries.

Document Box

A Document Box is a type of virtual mailbox on a device, used by individuals and groups to manage files that are stored on the device.



If authentication is set, accessing the document box requires the correct User name and Password in the Communication settings for the device.

Depending on the device model, the following kinds of document boxes are available:

Custom Box

Stores print data for each individual user on the printer and allows the user to print single or multiple copies of the stored data later using the printer's operation panel.

Subaddress Box

Stores received originals on the machine for forwarding with a subaddress and password.

Fax Box

Stores received originals on the machine to which the fax system is installed.

Fax Polling Box

Stores originals to be used in polling transmissions.

Document boxes can be created, edited, deleted, imported, and exported. You cannot add or delete a Fax Polling Box. Password protected document boxes cannot be exported unless device authentication is set.

CCR_X link

In the Document Box view, select **Device home** to display the device home page in Command Center RX (Remote eXtension).

Open Submit Panel

When you add, edit, delete, or import document boxes, the task appears in the Submit Panel list. In this list, you can choose whether to finish or cancel the task.

Document Box: Add a document box

Device Properties > Document Box

You can create a new document box on a device. You cannot add a Fax Polling Box.

- 1 Select **Add**.
- 2 Configure the properties of the new document box:

Property	Description
Name	Enter the new box name.
Type	Box type depends on model: Custom box, Subaddress Box, Fax box.
Number	Use automatic numbering or select from list (box numbers may not be reused).
Owner	Select a new owner from the list.
Owner setting	Select the type of owner from the list (Off, Local user, or Network user).
Domain	Select a domain.
Usage	Shows the current usage in megabytes (in the edit screen).
Restrict usage (MB)	Set the value from 1 to 30000 MB.
Automatically delete (days)	Select the period to save the file in device memory, from 1 to 31 days.
Shared	Select to enable the box for multiple users.
Password	You can set or change your password for the box.
Overwrite settings	Select to permit a new document to replace an existing document with the same name.
Subaddress	Enter the subaddress. Available with subaddress boxes.
Delete after printed	Select this option to remove a document from the box permanently after it is printed.

- 3 Select **Add**.
- 4 Select **Open Submit Panel**.
The submit panel opens on the right side of the screen with the information displayed with an **X** in a bubble. Cancel the change by selecting the **X**.
- 5 Select **Submit** at the bottom of the panel.

- 6 Select **Submit** on the pop-up confirmation.

When you close the progress window, the screen refreshes to show the changes.

Document Box: Delete a document box

Device Properties > Document Box

- 1 Under Document Box Type, select a type.
- 2 Select a box to delete.
- 3 Select **Delete**.

Follow from Step 4 under *Add*.

Document Box: Edit a document box

Device Properties > Document Box

You can change document box settings.

- 1 Under Document Box Type, select a type.
- 2 Select a box to edit.
- 3 Select **Edit**.
- 4 Change settings as desired, see properties under *Add a document box*. You cannot change the box type.
- 5 Select **OK**.

Follow from Step 4 under *Add*.

Document Box: Export a document box

Device Properties > Document Box

You can export one or more document boxes to a file, and then import the file into another device. Password protected document boxes cannot be exported unless authentication is set on the device.

- 1 Under Document Box Type, select a type.
- 2 Select one or more document boxes.
- 3 Select **Export**.

Document Box: Import a document box

Device Properties > Document Box

You can import document boxes to a device. Device Manager merges the imported boxes with existing boxes.

- 1 Under Document Box Type, select a type.
- 2 Select **Import**.
- 3 In the Import Document Box dialog box, drag a valid .csv file into the box, or browse to find a file.
- 4 Select **Upload file** to import the file, or select **REMOVE FILE** to delete it.
- 5 To map the columns to the properties, select available options under File mapping.
- 6 Select **Import**.
- 7 Perform other Document Box operations (add, delete, edit, and import).
- 8 Select **Open Submit Panel**.
- 9 Select **Submit** at the bottom of the panel.
- 10 Select **Submit** on the pop-up confirmation.

When you close the progress window, the screen refreshes to show the changes.

Document Box: Settings in Multi-Set Configurations

Managing Document Boxes in a Multi-Set Configuration follows the same basic steps as managing them for a single device from the Device Properties screen. You can manage all box types. You can add, edit, delete, and import.

The Enable switch gives you the option to disable configuration changes entirely for each box type tab.



If you set it to Disable on all the tabs, the system will pop up a warning icon for Document Box configuration or disable the Next button.

When adding, editing or importing a document box in a Multi-Set configuration, Device Manager presents merge options as part of the configuration set up (Preferences tab). These Preferences settings let you choose how to apply changes. The Preferences choices are:

Full Overwrite

This option will overwrite the existing document boxes of devices selected for this Multi-Set operation. It ignores all current settings on the devices, and overwrites all data. A Full Overwrite cannot be undone.

Smart Merge (recommended)

This option merges imported boxes with those on the device. In case of a conflict, boxes on the device are overwritten by imported boxes. If the existing box cannot be overwritten (password protection, for example) a new number is generated for the imported box.

Auto-generate

This option keeps all sources and target data, and generates new numbers for imported boxes that conflict with existing ones.

With Enable set to On, no other selections and/or changes made, and the default of Smart Merge selected in Preferences, all source entries will be merged or added to the target devices entries.

Device Users: Authentication

Device Properties > Users > Authentication

With Authentication, an administrator can select settings for user login, network user properties, password policy, and user account lockout. Authentication settings information appears in the following sections.



Not all options on the Device Users Authentication panel are available on all devices.

To access Authentication, start with the Device Properties of a device:

- 1** In the Device list, select a device under **Model name**.
- 2** Select **Users**.
- 3** Select **Authentication**.
- 4** Make changes as needed in the Authentication properties areas: General, Network User Properties, Password Policy, and User Account Lockout, and select **Save**.



To make changes to those property areas, see the following procedures.

- 5** When all changes have been made, select **Open Submit Panel**.
The submit panel opens on the right side of the screen with the information about the change displayed with an **X** in a bubble. Cancel the change by selecting the **X** in the bubble.




For Authentication, there is only a single bubble to reflect all uncommitted changes.

- 6** Select **Submit** at the bottom of the panel.
- 7** Select **Submit** on the pop-up confirmation.

When you close the progress window, the screen refreshes to show the changes.

Authentication: General

- 1 In Devices, select a printer, and then select **Users > Authentication > General**.
- 2 Select one or more of the following options:
 - Enable user login**
Set user authentication as device setting.
 - Permit jobs with unknown IDs**
Disable user restrictions and accept print jobs without a user login and password.
 - Local authorization**
Prohibit job use by specific users on a printer that supports this feature.
 - Group authorization**
Allow all users to operate within permissions set for the group.
 - Simple login**
Enable simple login for a printer. This option is available only for some printers.
 - PIN login**
Enable PIN, ID card, or password login option on the printer panel. This option is available only for some printers.
- 3 If user login is selected, then select either of the following authentication mode:
 - Use local authentication**
The printer uses the Device User List to authenticate the user.
 - Use network authentication**
The printer uses the domain server to authenticate the user.
- 4 If network authentication is selected, then do the following:

 **To use more than one server for authentication, select [Use multiple authentication server](#).**

 - a) Select a domain.
For some printers, you can select multiple domains from the list. Select one to be the default domain.
 - b) If necessary, add or edit a domain. Select an empty slot or a domain from the list, and then select **Edit**.
 - c) From Edit domain Name, modify the settings as needed, and then select **OK**.

If multiple authentication server is enabled, then specify the primary and secondary servers.

d) Specify the server type, host name or IP address, and port number.

5 Select **Save**.

Authentication: Network User Properties

Device Properties > Users > Authentication

Under Network User Properties, an administrator can set network user properties as a device setting. Settings for user properties vary by model.



Not all options on the Device Users Authentication panel are available on all devices.

- 1** Select **Network User Properties**.
- 2** Select **Obtain network user properties**.
- 3** Select LDAP settings:
 - **Server name**
 - **Port number**
 - **Search timeout**
 - **Encryption**
 - **Authentication type**
- 4** In the Acquisition of user information, the settings are used for search and retrieval of login user information from the LDAP server. Enter one or two user names, to a maximum of 32 characters. Enter a valid email address, to a maximum of 32 characters.
- 5** Select **Save**.

Authentication: Password Policy

Device Properties > Users > Authentication

An administrator can set password policy for all device users.



Not all options on the Device Users Authentication panel are available on all devices.

- 1** Select the arrow to open **Password Policy**.
- 2** To enable password policy settings, select **Use password policy**.
- 3** To set a password expiration, select **Maximum password age**, and select the number of days, from 1 to 64.

- 4 You can set the **Maximum password length** from 1 to 64 characters.
- 5 Under Password complexity, select desired password restrictions.
- 6 Select **Save**.

Authentication: User Account Lockout

Device Properties > Users > Authentication

An administrator can set device user account lockout settings.



Not all options on the Device Users Authentication panel are available on all devices.

- 1 Select the arrow to open **User Account Lockout**.
- 2 Select **Enable lockout** check box.
- 3 Select the allowed number of retries, from 1 to 10.
- 4 Select the lockout duration, from 1 to 60 minutes.
- 5 Select whether to lock out all connections or remote login only.
- 6 Select **Save**.

Map View

Use the Device Manager Map View feature to create a map of the physical location of devices. Map view requires a fixed group. Dynamic groups are not supported for Map view.

The Device Manager Map View feature can import an image file of a map. You can use multiple maps with different groups of devices. The device icons can show any or all of the following information:

- An image of the device
- A link to the device
- The network address of the device
- Device status

Creating a Map

- 1 Select **Devices > Map** on the toolbar.
- 2 Select **Add map (+)** to add a map image.

- 3 In the Device group menu, select the device group for the map.



Devices must belong to a fixed group to be added to a map. The default group is All devices.

- 4 Enter a name for the map.
- 5 Select the device details that will be shown on the map.
- 6 Drop the image file on the DROP FILES TO UPLOAD field or select to browse to the file location and select **Upload File**.
- 7 Select **Apply**.
- 8 Select devices and drag them onto the map.

Managing Map View

You can make the following modifications to the map view.

Zoom controls

To change the size of the map view, select the zoom icons on the right edge of the map view. Use the Zoom to fit icon to center and resize the image to fit the screen.

Delete a map

Select the map name and select **Delete map** (the trash can icon).

Delete devices

To remove a device, select the device in the map, and then select **Delete devices > Yes**. Removing a device from a map only removes it from the map group. It does not delete it from Device Manager.

Change device or map details

To change the device details or image shown in the map, select **Map options** (the gear icon) and select the details.

Device home

To view the Device home page, select the device and select **Device home**.

5 Tasks

Tasks are composites of management operations and device information that provide the ability to remotely manage and collect information from devices in a network. Task views display actions or operations that are currently active, scheduled, or have been completed. Tasks are created in wizards from the Device list and Device Properties screens and show up in one of the Task views as soon as they are submitted. Individual tasks serve as operational templates. Run, modify, and re-run tasks on the same or different schedule with the same or different device selection.

Tasks: Detail screens

You can access the detailed view of a selected task by selecting the details icon (↔).

Active task detail screen

The Active tab detail screen shows the progress of each operation within the task. Device Manager calculates the operation's progress based on how many of the selected devices have completed or failed the specific operation. A pull-down menu by the task description reveals a list of all devices with individual progress bars, or you can drop-down the top Details list and select a device to view. This will show all tasks that are running on the device (in a Multi-Set Configuration).

Scheduled task detail screen

The Scheduled tab details shows basic task details, schedule parameters, conflicts with existing tasks, and included devices. The drop-down list at the top will give you a look at individual devices and actions configured in the task (if multiple selections). If a group is used for the tasks, only the total number of devices is displayed.

Completed task detail screen

The Completed tab details shows basic task details, start and end times, and included devices with status. The drop-down list at the top will give you a look at individual devices, actions configured in the task (if multiple selections), and a brief description in the event of task failure.

From the Completed detail screen, you can download a .csv file with task results for either individual or all devices.

Tasks: Creating a scheduled task

For most tasks run on single or multiple devices, Multi-Set Configurations or groups, you have the option to run the task immediately, schedule it to run at a specified date and time, or configure it to run when a selected event occurs. To configure the Schedule for tasks, follow these steps:

- 1** In the Multi-Set Configuration Schedule screen, select **Later** or configure it to run based on a date and time or **On event occurrence** which is based on both a trigger and event occurrence.
- 2** In Retry, select **Enable**, and then enter the preferred values.
- 3** Select **Next**, and then specify the task name.
- 4** Select **Next**, confirm the details, and then select **Apply**.

If a conflict is detected with the Devices discovered setting, choose **Select here to review tasks** to view the Conflict Details list and Task details.

Tasks: Scheduling Options

When scheduling a task to run, the scheduling choices are Later and On event occurrence. Later scheduling offers the following options:

Once

Select a future date and time for a single run of the task.

Daily

Set a time for the task to run every day.

Weekly

Set a time and select one or more days of the week for running the task. Remove individually selected days by selecting the **X** for each.

Monthly

Set a time and select the day of the month to run the task.

Tasks: Select multiple devices for tasks

There are several ways to select devices for use with tasks. For performing a task on a single device, go to the Device Properties screen for the device.

Device Manager supports listings for all discoverable devices on your network, but not all Device Manager tasks will work on all listed devices. If a group of devices is selected for a set of tasks and some tasks are not compatible with certain devices in the group, the incompatible tasks will have a "failed" status.

Using check boxes

- From Device list or any group, select the check boxes by individual devices
- From Device list or any group, select the "check all" box (top of the check box column)

This action selects all devices on the current page. Devices on other pages are not selected.

When working with a single device, incompatible tasks will be grayed out/unavailable. With multiple devices selected, depending on the feature, all tasks will be available, but task results will show "fail" for the devices that are incompatible with the task.

When you select a task, the first screen shows the selected devices with check boxes to confirm your selections. You may clear check boxes for individual devices to remove them from the task.

Using device groups

Select a Device group (or the default All devices group), leave all check boxes empty, and select a task from the Create task menu. The first screen will show the number of devices in the group and you can proceed with configuring and running the task. If, however, there are members of the group that are incompatible with the selected task, the task will still run, but fail on the individual devices. You can review details and the overall status of the task in **Tasks > Completed**.

Common features on the tasks tabs

Quick Search

A drop-down list next to the Search box provides a way to select one property (column) to use as a filter. Choices are:

- Descriptive columns (all columns)
- Name
- Serial number
- Description
- Operation type

Search filters apply to all tabs (Active, Scheduled, and Completed).

See **Quick search** for more detail.

Sort

Select any column header to sort the entire list of tasks in ascending or descending alphabetic order. The sort applies across paging selections. The default sort is different for each Tasks tab:

- Active uses **Start time**
- Scheduled uses **Time created**
- Completed uses **End time**

Add/Remove Columns

As with the Devices tabs, there is an option to add/remove columns from the view. Select the + icon and check boxes on the list to add or remove columns. (Appears only when there are tasks to display.)

Details

The right-most column has info icons to select for detailed information about each task. The details screens vary depending on the task tab.

Active tasks

Shows tasks that are currently running. Columns in the Active tab include the following:

- Selection check boxes (if there is data displayed)
- Name
- Operation type
- Serial number of the device (if only one, the group name if a group was used, or a count of the number of devices affected by the task)
- Model name
- IP address
- Description
- Created by
- Time created
- Start time
- Progress
- Time remaining
- Column selection drop-down list and info icons are in the right-most column (if there are active tasks displayed)

Actions you can take on the Active tasks tab: Cancel a task in progress.

Scheduled tasks

Tasks > Scheduled

Shows scheduled tasks (not yet run). Columns on the Scheduled tab:

- Selection check boxes
- Enabled/disabled icons
- Name
- Operation type
- Serial number (if only one, the group name if a group was used, or a count of the number of devices affected by the task)
- Model name
- IP address
- Description
- Created by
- Schedule
- Time created
- Scheduled time for the task to begin or event trigger that will start the task
- Column selection drop-down list and info icons are in the right-most column

Actions you can take on the Scheduled tasks tab: Modify, Delete, Enable, and Disable.

Modifying a task will take you through the same screens and steps as creating the task and set the task to **Enabled** when done.

To delete a scheduled task, select one or more tasks using the check boxes in the first column and select **Delete** to remove them from the list. Confirm in the pop-up dialog box.

You can enable or disable scheduled tasks in two ways:

- Select one or more tasks using the check boxes in the first column and then select the **Enable** or **Disable** button as needed. While you can select multiple tasks this way, they must all be in the same state, or the buttons will be unavailable.
- Select the icon in the second column to toggle between enabled and disabled.

Either method for enabling or disabling scheduled tasks will pop up a confirmation box before completing the action.



Device Manager comes with three pre-configured "sample" Scheduled tasks (Set Sleep Timer, Enable EnhancedWSD, and Enable EcoPrint). Modify or delete these as needed.

Completed tasks

Tasks > Completed

Shows canceled or completed tasks. Columns on the completed tasks page:

- Selection check boxes
- Name
- Operation type
- Serial number of the device (if only one, the group name if a group was used, or a count of the number of devices affected by the task)
- Model name
- IP address
- Description
- Created by
- Schedule
- Time created
- Start time
- End time
- Result (**Succeeded** or **Failed**; a task is marked as failed if at least one operation on one device has failed)
- Column selection drop-down list and info icons are in the right-most column

The info icon in the last column brings up the task summary screen, showing details about the task:

- Task name
- Task status
- Number of devices
- Number successful
- Number failed
- Operation type
- Start time
- End time

- Date created
- Created by
- A list of the devices with individual status notations

A drop-down list at the top of the task summary screen shows a list of the devices affected by the task. Select each device to see more detail about the task.

A Download option at the bottom of the task details screen lets you download a .csv file with the task details for one or all devices.

Actions you can take on the Completed tasks tab: Retry or Delete a completed task.

Tasks: Retry completed tasks

Tasks > Completed

- 1 In the Completed tasks tab, select the check box for a single task.
- 2 Select **Retry**.
- 3 Depending on the type of task, adjust the settings for the original task.
- 4 You can let the retried task run immediately or configure a schedule. You can also reset automatic retry options on the Schedule screen.

Pre-defined tasks

The **Tasks > Scheduled** screen shows three pre-defined sample tasks:

- Enable EcoPrint
- Enable Enhanced WSD
- Set Sleep Timer

The first two tasks are triggered when any new device is discovered, and can be enabled or disabled. Set Sleep Timer is a scheduled task. The target device group for pre-defined tasks is All devices. You may keep, modify, or delete these sample tasks.

6 Reports

Reports: Configure and run reports

Device Manager provides the ability to create a report for devices and groups based on several reporting types. Users can add, edit, delete, enable, and disable scheduled reports. Within the selected report template, they can select devices or group, format, generation frequency, email recipients, report range parameters, and manually generate a scheduled report.

A report may contain statistically approximated data (similar but not equal to the actual result) if the polling interval for device alerts is more than 60 minutes. To reduce the polling interval, go to **System > Smart Polling**.

The default report templates are:

- Device Properties
- Device Counters
- Error total for last 30 days
- Consumable (Toner)
- Downtime

The Downtime report consists of two sub-report files in the zip archive: Downtime duration by device, and total Downtime duration in a selected time period. All duration values for errors, alerts, and reasons are reported in and are rounded to the nearest hour. This report depends on polling time and can vary depending on polling accuracy. A shorter polling time increases the report's accuracy.

The following errors will be considered as Out of Operation in this report:

- Device offline
- Device not connected
- Cover open alert on device
- Paper jam alert on device
- Out of toner alert on device
- Out of paper alert on device
- "Call for Service" alert on device
- "System Error" alert on device

Access reports that have been saved on the main Reports screen. You can sort the list on any column header, view details by selecting the information icon, search and filter the list.

Reports: Add scheduled report

- 1 Go to **Reports > Scheduled**, and then select **Add**.

- 2 Select a report template.
- 3 If necessary, create a custom template.
 - a) Select **Add**.
 - b) Specify the template name and description, and then select one or more report columns.
 - c) Select **Save**, and then select the new custom template.



- To edit a custom template, select the template, and then select **Edit**. Modify the settings as needed, select **Save**.
 - To delete a custom template, select the template, and then select **Delete > Yes**.
 - You cannot edit or delete the following predefined report templates:
 - Device Counters
 - Device Properties
 - Consumables
 - Error Counts
 - Downtime
-

- 4 Specify the file name, report name, file format, and if applicable, add email recipients, and then select **Next**.
- 5 Specify the range and frequency of the report, and then select **Next**.
- 6 Select either a source device or a group, and then select **Next**.
- 7 Review your settings, and then select **Finish**.

Reports: Delete scheduled report

- 1 Go to **Reports > Scheduled**.
- 2 Select one or more reports, and then select **Delete**.
- 3 Select **Yes**.

Reports: Edit scheduled report

- 1 Go to **Reports > Scheduled**.
- 2 Select the name of the report.
- 3 Select **Edit**.

- 4 Make changes to the settings as needed, and then select **Next** to edit more settings. For more information, see *Add scheduled report*.



If multiple devices had been selected, you will have to find and clear the check box for each one to remove it from the list for your revised report.

- 5 Review your settings on the Confirmation screen, and select **Finish**.

Reports: Enable or Disable report

This option lets you enable or disable scheduled reports. Disabled reports cannot be generated on demand, and will not run on the selected schedule.

- 1 Go to **Reports > Scheduled**.
- 2 Select one or more reports, and then select **Enable** or **Disable**.

The reports will have a disabled icon on the screen.

7 System

Smart Polling

System > Smart Polling

Smart Polling collects specific information from all devices registered and discovered by Device Manager on a configurable schedule. It supports polling for the following information:

Name	Description
Device information	Includes host name, mac address, serial number, system description, system location, capabilities, firmware versions, application lists, other device properties and settings
Counters	Includes all device counters (i.e. fax, printer, copier, letter, statement, etc.)
Toner level	Includes toner colors, current levels, capacities, and container names.
Device alerts	Includes all device error codes and their severities. Each of the four polling categories has a configurable polling interval. The polling configuration for a device can be checked in the Polling Intervals section of Device Properties.
	There are two additional intervals for Device alerts, in addition to the intervals provided for the other three categories, of 1 and 5 minutes. Longer intervals put less stress on the network and PC resources, but result in outdated information in Device Manager. Default intervals for each category are: <ul style="list-style-type: none">• Device Information: 6 hours• Device Alerts: 5 minutes• Counters: 60 minutes• Toner Level: 60 minutes

The Smart Polling screen displays an estimated (polling) request level based on the interval selections and number of devices managed by Device Manager.



If you want more timely notifications and task triggers, adjust the polling intervals to make them shorter. Expect polling delays when running

concurrent operations on the network that require a heavier load such as firmware upgrade.

SMTP

Configure SMTP server settings for Device Manager to use when sending notification emails. A Test Email button provides a way to check the settings and connection.

Testing SMTP Settings

You can test the SMTP connection with the Test Email feature. If SMTP settings have not been established, you are prompted to add them.


- 1 Select **System** > **SMTP**.
- 2 Verify the settings for the SMTP server.
- 3 Select **Test Email**. The system displays the success or failure of the test.
- 4 Select **Close**.

Security

Selecting a protocol type

- 1 Select **System** > **Security** > **HTTP Protocol**.
- 2 Select from the following protocol types:

Protocol type	Actions
HTTP	A message appears that the browser connection to the server may not be secured. Select Close > Apply .

Protocol type	Actions
HTTPS	<ol style="list-style-type: none"> Select a minimum TLS version. For HTTPS, browse for a certificate file in .pfx format. Select Apply. <hr/>  <ul style="list-style-type: none"> For HTTPS, specify the certificate password, and then click OK. The application restarts after the certificate is uploaded. For HTTPS (local self-signed certificate), the application generates a self-signed certificate and sends a notification when it is either generated or renewed. <hr/>
HTTPS (local self-signed certificate)	

The application saves the selected settings and restarts all services. After restarting, the newly changed protocol is available on the same port.

Password policy

System > Security > Password Policy

The password policy is configurable to align with a company's security requirements.

Field name	Range	Default value
Use password policy	Check box	Selected
Minimum password length	Check box	Selected
Length value	4-64 characters	4 characters
Uppercase letters	Check box	Cleared
Minimum uppercase letters	1-5	1
Lowercase letters	Check box	Cleared
Minimum lowercase letters	1-5	1
Numbers	Check box	Cleared
Minimum numbers	1-5	1

Field name	Range	Default value
Symbols Minimum symbols	Check box 1–5	Cleared 1
Reset password after initial login	Check box	Selected
Password validity time	<ul style="list-style-type: none"> One month Three months One year No expiration 	Three months
Prompt user to reset password if it will expire in	<ul style="list-style-type: none"> One day One week Two weeks 	Two weeks

Select or clear items to change policy requirements, and select **Apply** when finished.

Login/Logout

System > Security > Login/Logout

Configure the requirements for how and where users log in to Device Manager, account locking, and timeout settings from the Login/Logout page.


Name	Default value	Description
Local login required	Cleared	<p>If Device Manager is installed on the same computer that you use to access it, no login will be required. Device Manager goes directly to the devices list page; logoff disabled.</p> <p>When accessing Device Manager from another computer, you must always log in. Logoff enabled.</p>
Allow remote access	Selected for Device Manager Standard Cleared for Device Manager Lite	Indicates whether remote access is allowed.
Delay between consecutive logins	Selected	Require a delay between login attempts (deter brute-force login attacks).

Name	Default value	Description
Delay between attempts	2 seconds	Delay period before re-login after failed login attempt. The range is 1–5 seconds.
Lock account access	Selected	Lock account after specified number of consecutive failed login attempts.
Consecutive failed logins	3	The number of failed login attempts before account lockout. The range is 1–10.
Account locked (minutes)	30	The lockout period after which a user is automatically unlocked. The range is 10–120 minutes in increments of 10.
Automatic account logout	Selected	Inactivity timeout enforced.
Period of inactivity (minutes)	10	Inactivity period before timeout.

Selecting **Apply** for a change to the login requirement does not restart Device Manager services. The changed login is applied the next time you start a Device Manager browser session.

Configuring SCEP server settings

- 1 Go to **System > Security > Configure SCEP**.
- 2 Select the preferred CA server type, and enter the correct CA server URL.

 If necessary, select **Use proxy server** to configure your proxy server settings.
- 3 Select the preferred HTTP timeout.
- 4 If necessary, enable automatic re-enrollment, and configure the following settings:

Renewal period

Select the number of days for updating all certificates.

Certificate verification level settings

Select the preferred verification behavior.

Verification check interval

Select the number of days for revocation of certificates.

5 Select **Apply**.

If necessary, select **Test server connection** to check the connection with the SCEP server.

Issued Device Certificates

You can see the status and usage information for certificates that were imported into Device Manager.

The following information are displayed:

Currently active certificates

Imported certificates matched to installed device certificates detected on the discovered devices.

Certificate not in use

Unexpired certificates imported to Device Manager but with no match to detected installed device certificates.

Expired certificates

Expired certificates imported into Device Manager that are past their validity date.

Total certificates

Total number of imported certificates.

Importing SCEP certificates

If some devices already have device certificates installed which were issued by a CA, the user can import those device certificates into Device Manager for automatic renewal/re-enrollment.

1 Go to **System > Security > Issued Device Certificates**.**2** Select **Import previous certificates**.**3** Select the drop or upload area, navigate to the preferred file, then select **Upload file**.

Device Manager expects the certificate package to be a .zip archive with .pfx certificate files only, without subfolders and files of different format.



- If the uploaded package does not match the required format, an error message will be displayed.
- You can only upload one .zip package at a time.

If necessary, you may also enter the .pfx password.

4 Select **Import**.**5** Select **Close**.

To save the task results as a .csv file, select **Download results**.

The operation will only succeed if all the certificates were successfully imported into the Device Manager system, else it will fail.

After the import task is finished, all certificates are matched to detected device certificates installed on all devices.

Exporting SCEP certificates

- 1 Go to **System > Security > Issued Device Certificates**.
- 2 Select **Export SCEP certificates**.
- 3 Enter the password for all certificates.



If you do not enter a password, the Download button is disabled.

- 4 Select **Download**.

A .zip file is downloaded with the format,
`SCEPDeviceCertificates_<CurrentDateTime>.zip`.

The file name for exported certificates uses one of the following:

- IP address
- MAC address
- Host name

Removing all certificates

You can remove all certificates that are available in Device Manager and installed on devices. Device Manager drops mapping between imported certificates and certificates installed on the devices and deletes certificates from the Device Manager DB. These certificates are also excluded from monitoring and automatic renewal.

- 1 Go to **System > Security > Issued Device Certificates**.
- 2 Select **Unenroll all certificates > OK**.

Cleaning certificates

You can remove expired and unused certificates. These certificates are also excluded from monitoring and automatic renewal.

- 1 Go to **System > Security > Issued Device Certificates**.
- 2 Select **Clean certificates > OK**.

System Settings

System Users

You may create up to 500 Device Manager users to login and use the system. After 500 users, the Add button is unavailable. Available user roles are: Read Only, User, and Admin. The Read Only role can only view settings; the role does not see the System Tab, and many tabs and menus are disabled. The User role does not have privileges to manage system settings, and so does not see the System tab.

System Users: Add users

System > System Settings > Users

- 1** Select **Add**.
- 2** Enter a **Username** (up to 64 characters).
- 3** Enter a **Password** that adheres to the password policy for the system (it will be displayed under the Password field). Reenter the password in **Confirm password**.

If the password fails to meet any of the policy rules, that rule turns red to guide you.
- 4** Enter an **Email address**.
- 5** Select a **Role**.
- 6** Select **Save**.

The Users list shows the new user with Password expiration date and Password expiration status unpopulated. If your system has Reset password after initial login selected, users must change the password the first time they login. After this initial login change, the system populates the two expiration fields.

System Users: Edit users

System > System Settings > Users

- 1** Go to the Users tab.
- 2** Select the user to edit.
- 3** Select **Edit**.
- 4** Make changes as needed and select **Save**.



If you change the User's password and the system has **Reset password after initial login** selected, the user will be forced to change their password again when they log in, and they may not reuse the last password.



You cannot change the name and role of the default admin account (Admin).

System Users: Unlock users

System > System Settings > Users

If a user has locked their account, they can wait until the timeout period expires (**System > Security > Login/Logout**) or contact an Admin to reset.

- 1 Go to the Users tab. Locked out users have a red lock symbol next to the username in the list.
- 2 Select one or more locked users using check boxes.
- 3 Select **Unlock**, and then select **Yes** on the confirmation dialog.

System Users: Delete users

System > System Settings > Users

- 1 Go to the Users tab.
- 2 Select one or more users to delete using check boxes.
- 3 Select **Delete**, and then select **Yes** on the confirmation dialog.

License agreement

Select the License tab to read KYOCERA End User License Agreement terms. Select **Download** to save a copy in PDF.

Database connection: SQL

System > System Settings > Database Connection

Follow these steps to configure access to the SQL database used for Device Manager data:

- 1 Go to **System > System Settings > Database Connection**.
- 2 Select **Edit**.
- 3 Select **Continue** on the warning screen.
- 4 Enter settings for connection to MS SQL database (installed separately): server, port number, user ID, and password (required for TCP connection to remote SQL server).
 - Device Manager connects to the MS SQL DB and checks for an existing DB. It creates one if necessary.

- If there is an existing DB, Device Manager checks the version and runs migration scripts.

5 Select **Test Connection** to validate settings.

6 Select **Apply**.

For both Test Connection and Apply, if Device Manager cannot make a connection, it displays a red "Test failed" banner with a link. Selecting the link shows the detail on why the connection failed. Change your connection settings and try to connect again.



Device Manager server can establish a secure connection to remote and external databases. If the database is configured for a secure connection and forces it, Device Manager establishes a secure connection. No special setting is needed in the Device Manager database connection, just the hostname/port 1433 and user/login. Configure and enable TLS on MS SQL Server to establish a secure connection between Device Manager and the database server.

Database connection: Firebird

System > System Settings > Database Connection

The Database Connection settings for Firebird databases are not editable.

When you select **Edit** on the Database connection page if Firebird is in use, Device Manager displays a warning that the database can only be configured during the initial setup of the Device Manager application.

Importing Net Admin data

System > System Settings > Database Connection

You can import your data from Net Admin into Device Manager by following these steps:

Pre-requisite: Create a new Net Admin database backup from the application.

1 Navigate to the Database Connection tab in System Settings.

2 Select the **Edit** icon in the upper right corner.

3 Select **Continue** on the warning pop-up.

4 Select **Import Data**.

The Import Data button is not available if Device Manager already has devices listed.

5 Upload the backup file on the Import Data screen.

The backup will be a zip file that contains the "data.sql" file.

6 Select **OK**.



- 7 Select the red Import button on the Confirm Import screen.
You can view the progress of the import.
- 8 When completed, you have an option to download the results of the import.
- 9 Select **Go to Login** to restart Device Manager with your newly imported data.



The results file contains the following information in a .csv file:




- Number of devices that were imported
- Number of devices that were skipped
- Number of devices that were found in the file
- Number of users who were imported
- Number of users who were skipped
- Number of users who were found in the file
- Result of importing SMTP settings
- Result of importing security settings






Data imported from Net Admin backup

The following table shows what data is imported into Device Manager from Net Admin.

Property	Parameters
Security	Security protocol type  The protocol type can be HTTP or HTTPS.
SMTP	SMTP server name
	SMTP port number
	Login
	Password
	Sender email address
Users	User name
	Password
	Email address
	Role  Only User roles are imported into Device Manager.

Property	Parameters
Device	Device ID
	Serial number
	Model name
	Base model name
	Asset number
	IP address
	Host name
	MAC Address
	Description
	Manufactured
	Location
	Print speed
	Deleted view
	 If the printer is unmanaged in Net Admin, then set this parameter to NOW.
	Color
	 Use for Device Color support.
	Duplex
	 Use for Device Duplex support.
	TCP/IP port
	Communication timeout
	SNMP connection retries
	SNMP type

Property	Parameters
	Secure protocol (SSL)
	Authentication type
	Read community name
	Write community name
	User name
	Password
	User name  Use for Authentication information.
	Password  Use for Authentication information.
	SNMP authentication
	SNMP Privacy
	Command Center password
	System firmware
	Scanner firmware
	Fax port 2 firmware
	Panel firmware
	NIC firmware
	Engine firmware
	Fax system firmware
	Total memory
	Black toner level  Shows only the current toner level.

Property	Parameters
	Cyan toner level  Shows only the current toner level.
	Yellow toner level  Shows only the current toner level.
	Magenta toner level  Shows only the current toner level.
	Counters  Up to 125 counters; only the last counters.
	Media input  Shows the list of media inputs such as Name, Size, Type, Capacity, and Level.

Proxy settings

System > System Settings > Proxy Settings

If your network uses proxy settings, specify the following information about the external proxy:

- Host Name
- Port number
- User Name
- Password

Logs

A log is historical data in the Device Manager database that keeps information about tasks, reports, audit log entries, notifications, device alerts, counters, consumables, and firmware packages.

In **System > Logs**, do any of the following:

Clean up now

Manually delete the log storage data that is older than the selected period.



When this action is finished, it cannot be undone.

The following data are permanently deleted:

- Completed and canceled tasks
- Generated reports
- Audit log entries
- Resolved notifications and device alerts
- Counters
- Consumables
- Firmware packages

Log storage period

Automatically delete the log storage data that is older than the selected period every 24 hours from the time Device Manager was installed.



Log storage period and Clean up now functions delete the same type of data.

Export audit logs before deleting

Store audit logs in the file system before deleting in the database.

Receive daily audit log report

Send daily audit log report to Device Manager administrator.

Notify Admins of log operation errors

Send message to Device Manager administrator if an error occurs during log operations.

Download .csv Log

Export log information in a .csv format.

SNMP Trap Server

Device Manager uses a trap server to report error and device conditions to host trap recipients. It requires a Trap IP address from the host, a Trap community name, and alert and error selections made in the Device Settings. If two Trap IP recipient hosts are established in Device Manager, then trap notifications are sent to the systems associated with the IP addresses.

Setting SNMP Traps for a single device

- 1 Select **Devices Properties** for the device.
- 2 Select **General > Device settings**.
- 3 Select **All > SNMP trap**.

- 4 Select the **SNMP Trap recipients** check box.
- 5 Select SNMP trap settings, event errors, and warnings settings.
- 6 Select **Next**.
- 7 On the Confirm Details page, select **Apply**.

SNMP Traps can be set using Device Settings in Multi-Set Configurations.

Setting SNMP Traps for Multiple Devices

SNMP traps support the reporting of device error conditions to Device Manager or external systems. The error reporting is based on settings and schedule created in Device Settings.

- 1 In the Device list, select one or more devices.
- 2 Select **Create task > Device settings**.
- 3 In the Device list, verify the devices and select **Next**.
- 4 Select a **Method**. If you select From source file, you import the settings contained in the selected file.

New

Proceed directly to the Settings screen. You can save these settings to create a new settings template

From source device

Select a source device from the list.

From source file

Browse to select a file that has been saved with SNMP Trap settings.

- 5 Select **All > SNMP trap**.
- 6 Select the **SNMP Trap recipients** check box.
- 7 Select SNMP trap settings, event errors, and warnings settings.
- 8 Select **Next**.
- 9 Select a schedule and select **Next**.
- 10 Modify the **Name** and add a **Description**.
- 11 Select the **Receive notifications** check box.

- 12 On the Confirm Details page, select **Apply**.

Using the SNMP Trap Server

You can start and pause the SNMP Trap server in the System settings. The trap server reports device errors to as many as two defined trap recipients. SNMP trap settings for target devices can be configured in Device Settings. Polling is not required for device errors to be reported immediately. Before using an SNMP Trap server, ensure TCP port 162 is available and not blocked by a firewall. The Trap community name cannot exceed 16 characters.

- 1 Select **System > SNMP trap**.
- 2 In SNMP trap settings, you can pause the SNMP Trap server if it is already running. Select **Stop server**. While the server is paused, you can change the **Trap community** name.
- 3 Select or clear the check box for running the trap server at start up.
- 4 If you change these settings while the status of the SNMP Trap server is paused, select **Apply**.
- 5 Select **Start server**.

Database backup and restore

Database backup options

To view database backup options, go to **System > Backup and Restore**. Select one of the following options:

Manual

Use for one time immediate backup. Select **Back up** to start backup immediately.

Single backup in

Use for one time delayed backup.

Recurring

Use for scheduled periodic backups. Period options are daily, weekly and monthly at a specified time.



- The default backup folder is `\ndm_backup_storage`.
- The default backup file name is `DM_Database_Backup_[timestamp].zip`.

Database restore options

To view database restore options, select **Restore database** from the **System > Backup and Restore** screen. On the Database History screen, the toolbar offers the following options:

Restore

To restore from an existing backup file, select the file from the list and select **Restore**, or use the Upload option to select and upload a saved backup.

Download

Select a backup file from the list, and select **Download** to save a copy of a completed backup.

Upload

Select **Upload** to open the Upload database backup dialog. Browse to a saved backup file or drag and drop on onto the dialog, then select **Upload** to add that file to the list of available backups. Device Manager validates selected file before upload and displays an error message if the file is invalid.

Rename

Select an available backup from the list and select **Rename**. In the Rename backup file dialog, enter a new name and select **Apply** to change the file name.

Delete

Select one or more existing backups using the check boxes and select **Delete**. Confirm the deletion in the dialog box to complete.

Refresh

Reloads the backup list.

Set backup folder

Select **Set backup folder**, and then specify a new folder path for your backup files. Make sure that the folder is empty or does not exist. If the path is invalid or the folder is not empty, then an error message is displayed. After updating to the new folder, only backup files saved in the new folder are displayed.



There is also a listing of database backup files to select from. Select a row from the history listing to enable the first four options.

Special considerations by database type

Depending on the database type, Firebird or SQL, backup and restore scenarios will have different requirements. Further, you cannot switch between Firebird (internal) and SQL (external) database types using backup and restore. Please consider the following restrictions:

Firebird

If Firebird is selected as the database when installing Device Manager, database backup includes all files plus the Firebird database file.

When reinstalling Device Manager, if Firebird is selected as the database on install, the restore will include all files plus the Firebird database file.

You cannot switch to an SQL (external) database when reinstalling Device Manager if Firebird was used for the original installation. Device Manager will display a pop up that you cannot restore Firebird to SQL. In this case, you must reinstall Device Manager, select SQL as the database type, and populate the SQL DB with new data.

SQL

When creating a backup of the SQL database, Device Manager backs up all files, but displays a message asking you to get a backup of the SQL database separately.

When reinstalling Device Manager where SQL was the installed database, the backup displays a pop up reminding you to make sure that Device Manager is connected to the restored SQL database.

You cannot switch to a Firebird (internal) database when reinstalling Device Manager if SQL was used in the original installation. Device Manager displays a message that you cannot restore SQL to Firebird. In this case, you must reinstall Device Manager, select Firebird as the database type and populate it with new data.

8 Notifications

With this feature, users can:

- Create custom user notifications
- Create and edit notification templates for device events
- View the list of system notifications

Before you begin, make sure that SMTP is configured correctly.

To know if there are notifications available, check the Notifications icon beside the user name. The number of new notifications is displayed below the Notifications icon.

Notifications are categorized into the following:

Devices

Notifications triggered by events on the device.

System

Notifications triggered by events on the Device Manager.

User

Notifications triggered by a user.

Notifications: View notifications

- 1 Select the Notification icon beside the user name.
Recent notifications are shown with their corresponding level of importance. Red, yellow, or green which corresponds to high, medium, or low importance, respectively.
- 2 Select **Show all notifications**.
- 3 In Notifications, select **Devices**, **System**, or **User** to navigate between different types of notification.
- 4 Select the Information icon to view detailed information about the notification.
- 5 If necessary, for selected notifications, do any of the following:

Mark as

Mark the notification as read or unread. Marking the notification read removes it from the Recent Notifications list.

Set importance

Change the importance of the notification to high, medium, or low.

Delete

Remove notifications.

Notifications: Manage device notifications

Create device notifications or edit device notification templates.

- 1** Select the Notification icon beside the user name, and then select **Show templates**.
- 2** In Notification Templates, do any of the following:
 - To add a device notification, select **Add**, specify a template name, and then select **Next**.
 - To edit a device notification, select a template, and then select **Edit**.
- 3** Specify the trigger settings, and then select **Next**.
- 4** Select one or more device properties to include in the notification, and then select **Next**.
- 5** Select one or more devices or device groups, and then select **Next**.
To change the list view from devices to groups, select either **Devices** or **Group**.
- 6** Add email recipients.
 - a) Type the email address, and then select **+Add**.
To remove a recipient, select **X** beside the recipient email address.
 - b) Select **Send to Inbox** to show notifications in the Devices tab.
 - c) If necessary, add one or more email addresses where recipients can reply to.
- 7** Select **Next**.
- 8** Review your notification details, and if necessary, select **Enable notification after confirmation**.
- 9** Select **Apply**.

To delete, select a notification template, and then select **Delete**.



You can delete any notification template including predefined templates, and there is no confirmation or recovery option for this action.

To enable or disable, select a notification template, and then select **Enable** or **Disable**. You can only enable predefined templates if you edit them.

Notifications: Create user notifications

Only users registered in Device Manager can create user notifications. These notifications are not emailed, but are used for sending general messages to all users in Device Manager.

- 1 Select the Notification icon beside the user name, and then select **Create a user message**.
- 2 Specify the subject and message, and then set the importance to **High**, **Medium**, or **Low**.
- 3 Select **Save**.

The new message is displayed in the Recent Notifications list, and can be viewed again after reading in the Notifications Users tab. Importance settings for high, medium, and low appear with red, yellow, and green vertical bars, respectively.

Notifications: Receive task notifications

Some tasks offer to send a notification email on completion. For Device Manager to send email, you must configure SMTP settings.

Notifications: System

To view system generated notifications, select the Notification icon beside the user name, and then select **Show all notifications > System**.

Device Manager generates the following system notifications:

Type	Description	Default importance
Available disk space	Notifications about low disk space. The notification will be created in case if the available disk space on which the Device Manager application instance is deployed is less than 1 GB. Disk space monitoring is started every 10 minutes.	High
New feature	Notifications about newly implemented features in Device Manager.	Medium
Discovery finished	Device discovery task has completed.	Medium
License expiring	Created when Device Manager license is expiring. License expiration is checked when Device Manager starts, and then again every 5 days.	High
System started	Created whenever Device Manager is started.	Low
Task completed	Created when a task completes. Select the link in the notification detail to view the task details.	Medium

To show detailed information of the notification, select the information icon.

9 Miscellaneous

Administrator password change

It is best to change your administrator password when using Device Manager on a remote server, or is configured to require logging in when running locally.

Before you begin, make sure that:

- You are logged in as the administrator. Default administrator user name and password are admin and admin, respectively.
- SMTP is configured correctly. For more information, see the *SMTP* topic.

- 1** Select the drop-down menu at the top right corner beside admin.
- 2** Select **Change Password**.
- 3** Fill in the required authentication credentials.
- 4** Select **Apply**.

General behaviors that apply to multiple actions

Actions that set up tasks: Restart devices, Firmware upgrade, Device settings, and Configurations. They can be configured to run on single or multiple devices. There are two ways to select multiple devices: select the check boxes for each device or select all devices in a Group. You cannot select a Group with Restart devices.

Troubleshooting

When an error occurs in Device Manager, you can save detailed troubleshooting information to be analyzed by an administrator. In your Device Manager installation directory, find troubleshooting.bat and select **Run as administrator**. Save the .zip file.

USB devices

In order for Device Manager to be able to discover printers that are connected to computers by USB cables, install the Local Device Agent (LDA) on each computer with a USB-connected printer. See *Installation and Upgrade Guide* for information about installing LDA.

Connecting a USB device

You can connect a local device via USB to a network computer. The device can then be discovered and managed by the application.

Only the KX driver is supported for devices connected by USB.

- 1** Ensure that Device Manager is installed and operating.
- 2** Select another computer located on the same network as the server.
- 3** Connect the device to the computer with a USB cable.
- 4** On the computer, install the KX driver of the USB model printing device.
- 5** Import a backup of USB devices from Net Admin, or install LDA and discover USB-connected printers.

Import USB devices from Net Admin backup

System > System Settings > Database Connection

- 1** Select **Edit**.
A warning screen is displayed.
- 2** Select **Continue**.
- 3** Select **Import Data**.
- 4** Browse to find a Net Admin LDA backup file.
- 5** Select **Import**, and then select **OK**.
- 6** Select **Apply**.

Discovering USB-connected devices

After installing LDA in host computers with USB-connected devices, you can add these devices in Device Manager.



Before adding a USB-connected device, make sure that:

- Status Monitor is disabled in the host computer.
 - You have the IP address or host name of the host computer.
 - The device is not in sleep mode.
-

- 1** In Device Manager, go to **Devices > List > Add devices > Add devices now**.
- 2** In Discovery mode, select **By IP address or host name**.
- 3** In Target, specify the IP address or host name of the computer with the USB-connected device.
- 4** Review or modify other settings, and then select **Run**.

- 5** Review the results. If necessary, resolve any issues before repeating the process.
In Device list, confirm that the device has been added.



For USB-connected devices listed in Device Manager:

- You cannot edit the location and communication settings.
 - You cannot open the device home page.
 - In the host computer, make sure that LDAService is running and Status Monitor is disabled.
-

