KYOCERA Fleet Services

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.

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 5 NetGateway

Chapter 6 Mobile management

Chapter 7 Firmware packages

Chapter 8 Logs

Chapter 9 Devices

Chapter 10 Toner orders

Chapter 11 Maps

Chapter 12 Device summary

Chapter 13 HyPAS applications management

Chapter 14 Task status list

Chapter 15 Snapshots

Chapter 16 Panel screenshot

Chapter 17 Panel note

Chapter 18 Data capture

Chapter 19 Firmware upgrade

Chapter 20 Device restart

Chapter 21 Maintenance mode

Chapter 22 Send file

Chapter 23 Remote panel

Chapter 24 Device Settings

Chapter 25 Backup data

Chapter 26 Notifications

Chapter 27 Dashboard

Chapter 28 Graphical reports

Chapter 29 List reports

Chapter 30 Announcements

Chapter 31 Device Registration Diagnostic Tool

Chapter 32 Data Collection Tool

Chapter 33 System connections

1 Product Overview

KYOCERA Fleet Services (KFS) provides a total device management solution in the cloud. With KFS, you monitor and manage KYOCERA devices and devices by other manufacturers. Some of the remote monitoring features include device counter collection, reporting, device monitoring, consumable status, and ordering. Task management activities include remote firmware upgrades, device diagnostics and troubleshooting, remote setup and maintenance. KFS requires no installation because it operates on a cloud-based platform. A browser and internet connection provide easy access to the service.

Devices are registered in KFS using the Command Center or the Device Registration Diagnostic Tool (DRD Tool). A local device with KFS supported firmware can self-register.

KFS Documentation set

KYOCERA Fleet Services

Guide	Description
KYOCERA Fleet Services User Guide	Describes a comprehensive device management solution in the cloud. You can monitor and manage KYOCERA devices and devices by other manufacturers. Some of the remote monitoring features include device counter collection, reporting, device monitoring, consumable status, and ordering. Task management activities include remote firmware upgrades, device diagnostics and troubleshooting, remote setup and maintenance.
KYOCERA NetGateway User Guide	Describes the settings, configurations, and concepts in NetGateway for registering devices in KFS. It also provides information about local agent installation and use.

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

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

System requirements

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

2 KYOCERA Fleet Services account

When you create a new user account, KFS sends an email with a temporary password and User ID to the user. The temporary password expires in 7 days. The new user should use the temporary password to log in then create a new password when prompted.

Passwords expire one year from the date the password was changed. The system sends a password expiration email notice 14 days before expiration.

KFS locks user accounts for 30 minutes after three failed login attempts within five minutes. Password assistance is not available when the account is locked. A Manager within the same group or a higher level group can unlock a user account.

For expired passwords, select **Password assistance** on the KFS Login screen.

Password policy

The KFS password policy requires that passwords have:

- A minimum of 8 characters
- At least one number (0-9)
- At least one symbol
- At least one uppercase letter
- At least one lowercase letter

Logging in to KYOCERA Fleet Services

You must log in to KYOCERA Fleet Services to remotely manage devices and users. Your credentials are saved in browser's cache for 7 days or until you log out of KFS.

1. Open a supported internet browser, enter the URL for KYOCERA Fleet Services, then press **Enter**.
2. Enter your credentials for **User ID** or **Email address** and **Password**.
3. Select **Login**.

Using password assistance

If you forget your password or your password expired, use password assistance to receive a password by email. This temporary password expires in 7 days.

1. On the Login screen, select **Password assistance**.
2. Enter your **User ID** or **Email address** in the textbox.

3. Select **Submit**.
4. Use the temporary password sent by email to access your account.

After providing the temporary credentials, the system prompts you to create a new password.

Changing user information

Users can edit their own user information. Some settings cannot be changed.

1. In the top banner, select your KFS user account name.
2. Select **Edit user**.
3. In the Edit User dialog box, change available information. Select **Next**.
4. Change the available information. Select **Finish**.

Changing your password

You can change your account password at any time.

1. In the top banner, select your account user name.
2. Select **Change password**.
3. Enter the old password.
4. Enter your new password.
5. Enter your new password, again.
6. Select **OK**.

3 Groups

KFS registers and manages devices in groups within a hierarchical structure. There is no limit to the number of groups, delegated groups, or the number of devices registered in a group. The group hierarchy supports a maximum of 10 levels.

In the Devices and Administration views, you can check details about a group, including user permissions.

Group labels identify the type of group with gray icons for groups and blue icons for delegated groups. For a group/delegated group authorized by a System Administrator or Manager with external access, an external access icon is added to the group label. External access is automatically inherited by the lower group/delegated group.

Child groups are listed under their parent groups. You can view them by selecting the arrow icon next to a parent group.

System Administrators and Managers grant users access authority to devices and groups. Users can be granted access to other groups (delegated and regular groups) in addition to their own delegated group. Your permissions to groups are those groups visible in the Group name list. After selecting one or more groups, you can apply management and monitoring tasks to the devices in the groups.

Delegated groups

Delegated groups manage users and devices. Delegated groups with RHQ permissions may upload firmware packages. System Administrators and Managers can edit user permissions for a delegated group that adds functionality for users of the delegated group. Permissions are inherited from the group above the delegated group and include diverse management and task functions. Permissions are inherited by all lower level delegated groups.

Editing group permissions

System Administrators and Managers can add or reduce permissions for users of delegated groups. Managers can edit permissions for child delegated groups, but not the group they belong to. Permissions are inherited from the group above the delegated group and include diverse management and task functions.

1. In the Administration view, select **Groups**.
2. In the Groups list, select a group.
3. Select **User permissions**.
4. Select permissions you want to authorize for the delegated group user and clear the selection for those role-based permissions you want to remove.
5. Select **Save**.

Group name list

In the Devices and Administration views, you can view groups and delegated groups in a hierarchical display. The Group name list is structured as a tree list. It displays the hyperlinked group name, the number of devices in the group, and an information icon for access to additional group details, including User permissions. When the tree list is expanded, you can view child groups.

In the Devices view, you can select the double left arrow to collapse the Group name list. If the Group name list is collapsed, you can drag the divider to expand it. In full display, it shows three columns: Group name, Devices (Managed/Total) and Total device count (Managed/Total).

In the Devices view, you can modify the number of devices displayed in the Group name list by selecting from one of three options in the Include drop-down menu.

Devices exclusive to this group

Devices registered to the selected group only

Exclusively managed

Devices in the selected group and the regular child groups

All accessible

Devices in the selected group and all the child groups below

Group details

In the Devices and Administration views, you can view the Group details when you select the information icon for a group. In the Devices view, the information icon displays when the group name list is extended. The group name, group label, and group type is displayed at the top of the Details box. For delegated groups, select **User permissions** to see the functions granted by the System Administrator or Manager. The Details box also include the following information:

Management ID

The Management ID created for delegated groups only.

Description

The description of the group.

Registration URL

The URL used to register devices or gateways to KFS.

Access code

The Access code identified with the group and used to register devices or gateways to the specific group.

Customer information

This includes Customer name, Customer ID, Email address and other address information associated with the group.

Counters and consumables

A specified time or a daily schedule when counters and consumables data are updated.

The Details box has two tables that illustrate the relationships of the group with the child groups and the devices within them.

The Groups table contains information on the selected group's child groups.

Exclusively managed

Displays the number of regular child groups.

All accessible

Displays the number of regular and delegated child groups.

One tier below

Displays the number of regular and delegated child groups that are directly one tier below the selected group.

The Devices table contains information about the management state of the devices and how it relates to the selected group.

Exclusive to this group

Devices in the selected group.

All accessible

Devices in the group and its child groups.

Monitored by this group

Devices in the group and regular child groups.

Filtering and searching for groups

1. In the Administration view, select **Groups**.
2. In the Search text box, select a search category, and then enter a search string or select a predefined search option. The following item uses predefined options:

   Group type: Group, Delegated group
3. Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Adding a group

1. In the Administration view, select **Groups**.
2. In the Groups list, select a group. This selected group will be the parent of the group you are creating.

3. Select **Add**.
   a) In the Name box, enter the group name.
   b) For Group type, select **Group**.
   c) For Group label, select from the list of options: **Regional headquarters**, **Sales company**, **Dealer**, **Customer**, or **General**.
   d) In the Description box, enter a description of the Group.
   e) An Access code is used to associate devices with a group. You can use the access code provided or select **Generate** if you want a different access code.
4. Select **Next**.
5. Add contact information for the group, and then select **Next**.
   a) Select a Group then additional users for whom you want to set access privileges. Use the Search text box to find specific users.
6. Select **Next**.
   a) In Device permissions, clear boxes in the Allow column for each KFS feature you want to restrict. By default, all are selected.
   b) For Data captures, select the number of days (1 - 7 days) you want to retain captured printable data.
   c) In Counters and consumables, select from one of the following options:
      - Daily (at time of device registration)
      - Specified time frame and select a time range with a starting time and ending time. The setting uses a 24-hour clock and 15 minute time intervals.
      - Specified time and select a time in the drop-down list. You can specify 1 to 4 unique retrieval times. The time interval is every 15 minutes.
7. Select **Next**.
8. Review the Summary, and then select **Finish**.
   You can use the Back button to go to previous screens and make changes.

Access codes

An Access code is used to register devices and Gateways to a group. Each group uses a unique access code that is created at the same time as the group. When devices or Gateways are registered, the access code associates the device or Gateway being registered with one group. In the Devices view, open the information icon for a group to view the access code associated with the group.

Adding a delegated group

1. In the Administration view, select **Groups**.
2. In the Groups list, select a group. This selected group will be the parent of the group you are creating.

3 Select **Add**.

a) In the Name box, enter the group name.

b) For Group type, select **Delegated group**. System Administrators can add RHQ permissions for Managers of a delegated group by selecting **RHQ permissions**.

c) Select **Edit user permissions**, then review the list of KFS features inherited from the parent delegated group (all selected by default). Clear boxes to remove permissions for users of this delegated group. Changes to permissions apply to all groups below the delegated group.

d) Select **Save** when finished adding or removing permissions.

e) For Group label, select from the list of options: **Regional headquarters**, **Sales company**, **Dealer**, **Customer**, or **General**.

f) (Optional) Enter a Management ID.

g) In the Description box, enter a description for the group.

h) An Access code is used to associate devices with a group. You can use the access code provided or select Generate if you want a different access code.

4 Select **Next**.

5 Add contact information for the group, and then select **Next**.

6 Set the **Language** and **Date format** in the drop-down lists, and then select **Next**.

7 (Optional) Select a **Group manager** using one of the following selections:

- Assign from existing users - select from the Group drop-down list then select a user in the list
- Assign a new user - select **Add** and enter the information to create a new user

8 Select **Next**.

9 Select a **Group** then additional users for whom you want to set access privileges.

Use the Search text box to find specific users.

10 Select **Next**.

a) In Device permissions, clear boxes in the Allow column for each feature you want to restrict. By default, all are selected.

b) For Data captures, select the number of days (1 - 7 days) you want to retain printable data captured with the Data capture feature.

c) In Counters and consumables, select from one of the following options:

- Daily (at time of device registration)
- Specified time frame and select a time range with a starting time and ending time. The setting uses a 24-hour clock and 15 minute time intervals.
- Specified time and select a time in the drop-down list. You can specify 1 to 4 unique retrieval times. The time interval is every 15 minutes.

11 Select **Next**.

12 Review the Summary, and then select **Finish**.

Managing external access roles

System Administrators and Managers can manage users in the External access list.

1 In the Administration view, select **Groups**.

2 In the Groups list, select a group for external access.

3 Select **External Access**.

4 Select the **Manage** icon.

- Select an **External access role** from the drop-down list for the selected user.
- Select items in the list of User permissions. The available permissions for tasks are based on the permissions of the user's group and are limited by the selected role.
- Select **Save**.

5 In the External access list, select the **Delete** icon to remove external access for the selected user.

6 Select **Save**.

Editing group information

System Administrators and Managers can make changes to group information.

1 In the Administration view, select a group.

2 Select **Edit**.

3 Make the changes to the group information.
Management ID can be edited for delegated groups only.

4 To change permissions for a delegated group, select **Edit user permissions**.

5 Select **Save** when finished adding or removing permissions.

6 Review the Summary, and then select **Finish**.

CRM integration

System Administrators and Managers can import Customer Relationship Management (CRM) data contained in a .csv into the KFS database.

The import file must include at least one device per row and one data field per column. The file must contain a minimum of two columns with the headers labeled "Serial number" and the other fields matching options that can be selected from the drop-down menu in the Import dialog. KFS matches registered devices in the CRM data import according to the device Serial number in the database and updates information for the other target fields. There are no restricted characters.

A CRM data import cannot include duplicate Serial numbers or Asset numbers. The import cannot include blank values for serial numbers.

Any manually added or edited Asset number in KFS takes precedence over an Asset number from a CRM data import which takes precedence over an Asset number added or edited in CCRX. For example, a device Asset number edited in KFS cannot be overwritten by the Asset number for the same device that is part of a CRM data import.

A CRM data import may also contain other fields. For devices with Access codes in the data import, the imported devices are registered to the groups associated with the access code. For unregistered devices included in a CRM data import, the other selected fields contained in the CRM data are applied when the device is finally registered.

The management status of a device changes from Pending to Managed when a CRM data import produces a match with a device Serial number. Management status is not changed if the status is other than Pending.

With the import of a new CRM data file, all CRM data for devices in the targeted group is replaced. The imported data is stored in the database for each delegated group. If all entries of the import are invalid, Import is disabled on the Summary page.

An Administrator can change the management status of multiple devices that are linked to a delegated group after import of CRM data.

Importing CRM data

System Administrators and Managers can import and align data from Customer Relationship Management (CRM) data contained in a .csv. You can import multiple devices to upper delegated groups or lower tier groups. The system displays an error when duplicate Asset numbers or Serial numbers are found in the CRM data import or between devices in the import file and existing devices.

1. In the Administration view, select **Groups**.
2. Select a delegated group.
3. Select **Views** > **Imported device data**.
4. Select **Import**.
   a) In **Select a file**, select **Browse** to choose the .csv designated as your CRM data import.
   b) Select **Open**.
   c) For List separator, select a comma or a semicolon to match the import file.

d) In Column matching, select the alignment you want from the imported file. By default, the Serial number is displayed at the top of the list followed by the Asset number.
e) Select the plus sign to add **Location**, **Description**, **Custom field** 1- 3, **Management status**, and **Access code**.
f) Clear **Skip first row as header** if you want to use the first row in the CRM data import file.

5 Select **Next**.
a) Review the Summary.
If errors are found in the selected .csv, they are displayed in red in the summary. Select **Back** to reimport the file after fixing it.
b) Select **Import**.

6 Select **Close** when importing is finished.

After a successful import, select **More details** to view general information about the CRM data import including the file name, last imported timestamp, and the user name.

Imported device data view

Imported device data is displayed in its own view. The list of devices for a selected group is divided into registered and unregistered devices. You can sort the view by selecting the column names. If an imported device is already registered in the target group, then current device data is displayed.

Changing a group to a delegated group

1 In the Administration view, select **Groups**.

2 In the Group name list, select a group.

3 Select **Edit**.
a) For Group type, select **Delegated group**.
b) Select **Edit user permissions** to add or remove permissions for users of the delegated group.
The default permissions are inherited from the parent delegated group. Permissions apply to users in the groups below the delegated group.
c) Select **Save** when finished adding or removing permissions.
d) Select **RHQ permissions** to permit the Group manager to load custom firmware.
e) (Optional) Enter a Management ID.
f) Enter a Description.
g) An Access code is used to associate devices with a group.
You can use the access code provided or select **Generate** to create a different access code.

4 Select **Next**.

5 Add contact information for the group, and then select **Next**.

6 Set the **Language** and **Date format** in the drop-down lists, and then select **Next**.

7 (Optional) Select a **Group manager** using one of the following selections:

- Assign from existing users - select from the Group drop-down list then select a user in the list
- Assign a new user and select **Add** - add new user information

8 Select **Next**.

9 Select a **Group**, then additional users for whom you want to set access privileges. Use the **Search** text box to find specific users.

10 Select **Next**.

a) In Device permissions, clear the **Allow** check box for each KFS feature you want to restrict.

By default, all are selected.

b) In Target devices, select from one of the following options:

- Include all devices
- Include only managed devices

c) For Data captures, select the number of days (1 - 7 days) you want to retain the captured printable data.

d) In Counters and consumables, select from one of the following options:

- Daily (at time of device registration)
- Specified time frame and select a time range with a starting time and ending time. The setting uses a 24-hour clock and 15 minute time intervals.
- Specified time and select a time in the drop-down list. You can specify 1 to 4 unique retrieval times. The time interval is every 15 minutes.

11 Select **Next**.

12 Review the Summary, and then select **Finish**.

Moving groups

System Administrators and Managers can move a group from one group to another.

1 In the Administration view, select **Groups**.

2 Select the group you want to move.

3 Select **Move**.

4 In the New group column, select the destination group. You can select **Search**, enter a group name to find the group, and press **Enter**. Select x to close the Search text box.

5 Select **Next**.

6 Review the Summary, and then select **Move**.

7 Select **Close**.

Deleted groups

KFS maintains deleted groups in the recycle bin for a period of two weeks. During that time, devices cannot be found using Advanced search nor can the devices be included in reports, device lists, and dashboards. Device data is preserved, but it is not updated. The recycle bin is visible only to System Administrators and Managers.

Managers can delete a group but must have permissions and access authority for the specific group.

A deleted group includes the following associated items:

- All affiliated users
- Connected Gateway and Devices
- Report templates (Share to Delegated Group)
- Notification templates (Share to Delegated Group)
- Firmware packages (Custom Firmware)
- Logs (Audit/Email)
- KFS Mobile

If the parent of a group in the recycle bin is deleted, then all child groups are deleted too. The two-week retention period is determined by the date that the parent group was deleted.

After a group is deleted, associated users can neither log in to KFS nor use Password assistance. The user status and device management status are maintained while their associated group is in the recycle bin. If a user's password expires during the time a group resides in the recycle bin, the password will be expired when the group is restored.

On the expiration date, the group is removed from the recycle bin and the KFS database.

Deleting a group

With the exception of the ROOT group, System Administrators and Managers can delete any group they can access. All groups under the deleted groups are also deleted. The deleted group is moved to the recycle bin for two weeks before final deletion. Permanent group deletion can be made in the recycle bin. System Administrators and Managers cannot delete a group they belong to.

1 In the Administration view, select **Groups**.

2 In the Groups list, select a group.

3 Select **Delete**.

4 Select **OK**.

Restored groups

System Administrators and Managers can restore groups from the recycle bin for two weeks after deletion. Managers can restore a group but must have permissions and access authority for the specific group. The restored groups include associated users and devices, email and audit logs, child groups, data and schedule settings. Because the device data is preserved while the group is in the recycle bin, a restored group includes device data.

A restored group includes the following associated items:

- All affiliated users
- Connected Gateway and Devices
- Report templates (Share to Delegated Group)
- Notification templates (Share to Delegated Group)
- Firmware packages (Custom Firmware)
- Logs (Audit/Email)
- KFS Mobile

Restoring groups

System Administrators and Managers can restore groups from the recycle bin in KFS to their former location.

1 In the Administration view, select **Groups**.

2 Select **Recycle bin**.

3 Select a group or groups in the list.

4 Select **Restore**.

5 Select **OK**.

Group branding

Group branding supports customizing the KFS user interface for a dealer or other business. The customization includes the product name, the colors of the elements in the user interface, logo, and favicon. The settings are applied to the child groups. You can restore default branding or Use parent group branding. For the parent group, customized branding must already be saved. The selections made in the Group branding wizard can be previewed in the UI before you finish.

Creating group branding settings

You can create Group Branding settings in KFS. When you select the product logo and favicon, a small preview is provided. On the wizard's second page, hover over the information icon for more detail about the selected color setting. A preview of the color scheme is provided in the top half of the screen.

1. In the Administration view, select a group.
2. Select **Branding**.
   a) In the Quick edit drop-down list, select **Use KFS branding** for the KFS logo, favicon, and text or **Use default group branding** to apply the same branding as the group.

      These settings are commonly used when you want to restore KFS branding, apply Group Branding to a child group, or clear a specific product branding from a group.
   b) Enter the **Product name**.
   c) Use the up and down arrows to set the font size of the product name.
   d) Select **Browse** and select the image file you want for the Product logo, then select **Open**.
   e) Select **Browse** and select the image file you want to use for the Favicon, then select **Open**.
3. Select **Next**.
   a) Select the settings for the color scheme.

      Select colors in each box and use the provided hex color picker to choose a color and the gradient for the branded site.
   b) To clear changes made in the current session, select **Reset recent changes**.
   c) To change to the default blue KFS brand, select **Restore default colors**.
   d) Select **Finish**.
4. Select **OK**.

Remember to refresh the page to apply the new Group Branding settings.

4 Users

Users are created and assigned roles depending on their required tasks, responsibilities, and information requirements. The available functions are based on the user's role and the permissions authorized by System Administrators. Tasks are not supported for Customers or Analysts.

KFS supports five user roles:

System Administrator

Manages the entire service. Has access authority to all groups and users. May perform all monitoring, maintenance, and troubleshooting tasks.

Manager

Manages users under the delegated group to which the Manager belongs. Manages users, service tasks, monitoring, and reporting. Managers with RHQ permissions can upload and publish firmware.

Service

Registers and maintains devices for customers. Service users perform maintenance tasks.

Analyst

Analysts gather data about devices for evaluation. They can run reports and receive notifications for their authorized groups and delegated groups. Analysts can share templates with their delegated groups.

Customer

Customers monitor devices by scheduling and generating reports and notifications for devices in their authorized groups and delegated groups.

User details

System Administrators and Managers can view user details by selecting the information icon in the Users tab in the Administration view. The ID, Name, Role, and User permissions display at the top of the Details dialog. Select **User permissions** to view a list of functions and features authorized by the System Administrator or Manager for the selected user. The Details dialog also provides the following information about the selected user:

Status

Management status: Enabled, Enabled (Locked), Enabled (Expired), Disabled, and Disabled (Locked).

Group

Email address

Receive notifications
No or "send by email"

Phone number

Mobile number

Company name

Language

Date format

Registration date
Date and time this user was registered in KFS.

Privacy statement status
The status of user acceptance of the privacy statement.

Last login
Date and time this user last logged in to KFS.

Accessible groups
The groups accessible to this user.

Searching for users

System Administrators and Managers can search for users.

1. In the Administration view, select **Users**.
2. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following items use predefined options:

   Management status
   Enabled, Disabled, Locked, Expired

   Receive notifications
   On, Off

   Role
   System Administrator, Manager, Service, Analyst, Customer
3. Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Searching for users with advanced search

You can search for users using one or more search criteria or recent search properties. You can combine 5 search properties in Advanced search. The available search properties are dependent on your role.

1. In the Administration view, select **Users**.
2. Under the search text box, select **Advanced search**.
3. In the Advanced Search dialog box, select **Search criteria**.
4. Choose **Select property** and select search properties from the drop-down list. For search properties, you can select from the following:
   - Company name
   - Days since last login
   - Days since user registration
   - Description
   - Email address
   - First name
   - Group name
   - Last name
   - Management status: Enabled, Disabled, Locked, Expired
   - Permissions: More than 20 selections related to KFS functions
   - Privacy statement status
   - Role: System Administrator, Manager, Service, Analyst, Customer
   - User ID
5. If you select Group name as a search property, select the Edit icon to choose individual groups or all accessible groups. If you select **All accessible** under Quick select, then each parent group that you select expands the group tree and selects all of the affiliated child groups. Select **Search** and enter the group name to quickly find a group.
6. In the drop-down list, select a search operator.

   The options are based on the selected property and may include Belongs to, Contains, Does not contain, Equals, Does not equal, Starts with, Ends with, Greater than, Greater than or equal to, Less than, Less than or equal to.
7. Enter a search term in the text box, if required.
8. Select **Search**.

As an alternative search method, select **Recent searches**, then select from the available searches. Clear your entries in the Advanced search by selecting **Reset**.

Creating a user

System Administrators and Managers can create users with permissions.

1. In the Administration view, select **Users**.
   a) In the Group name list, select a delegated group that this user will be added to.

      The group name is displayed on the first page of the Add User wizard.
   b) In the toolbar, select **Add**.
   c) Enter the required information: **User ID**, **Email address**, **First name**, and **Last name**.
   d) Select a status:

      Enable

      The user has access to KFS features.

      Disable

      The user cannot log in to KFS.
   e) Select a role for this user.
   f) Select **Edit permissions** to enable or disable available KFS features.
   g) Select **Save** when finished adding or removing permissions.
2. Select **Next**.
   a) Enter a **Phone number** and **Mobile number**.
   b) For Receive emails, select **Yes** for this user to receive email notifications and reports.
   c) Enter the **Company name**.
   d) Select the Language and **Date** format.
   e) (Optional) Enter a **Description** (256 character maximum).
3. Select **Next**.
4. Select a group or groups to set access permissions. Use the Search text box to find specific groups.
5. Select **Finish**.

External Access Code

An External access code is generated and used by System Administrators and Managers to grant users of one delegated group with external access authority to another group. As an example, a System Administrator can grant a Service user access to another delegated group so the Service user can perform firmware upgrades. A KFS role and role-dependent permissions must be selected for the new users of the group. To view a list of External access users, select the group and then select **External access**. Users can be removed from the External Access list or user permissions can be edited.

For any single user, System Administrators and Managers can generate one or more external access codes. KFS creates an external access code by encrypting the string produced by the combination of User ID and created date and time. A single code can be generated for select users belonging to varied groups. The code expires after 7 days.

External access users are not permitted to use the report templates and notification templates associated with the group.

Generating external access codes

System Administrators and Managers can generate external access codes to grant users access to other groups.

1. In the Administration view, select **Users**.
2. Select the check boxes for the users.
3. Select **External access code**.
   You can sort the list of users by selecting the column name.
4. Select **Copy** to copy the code.
5. Select **Close**.

Adding external access codes to groups

System Administrators and Managers can add external access codes to groups as a way to grant users access.

1. In the Administration view, select **Groups**.
2. Select a group.
3. Select **External access**.
4. Paste the code copied from user information into the External access code box.
5. Select **Add**.
6. Select **Save**.

Editing user permissions

System Administrators and Managers can add or reduce permissions available to the selected user. Permissions include diverse management and task functions. System Administrators edit permissions for Managers, Service users, Analysts, and Customers. Managers can edit permissions for Service users, Analysts, and Customers. Managers cannot edit their own permissions. Permissions are inherited from the group above the delegated group.

1. In the Administration view, select **Users**.
2. Select a user from the list.

3 Select **Edit permissions**.

4 Select the permissions to authorize for the selected user and clear selections for permissions to remove.

5 Select **Save**.

Editing user information

System Administrators and Managers can change user information and permissions. All users can edit their own information. Some user information cannot be changed.

1 In the Administration view, select **Users**.

2 Select a user.

3 Select **Edit**.

4 Make changes to user information, permissions and accessible groups, if available.

5 Select **Finish**.

Moving users to a different group

System Administrators and Managers can move users to a different group. If a selected user is moved to a child group lower in the hierarchy, then they will lose access to the groups above the new location. Be careful not to move users away from a group they require access to.

1 In the Administration view, select **Users**.

2 Select a user or users.

3 Select **Move**.

4 Under the New group list, select the group or search for groups.

Select **Search**, enter all or part of a group name and press **Enter**. Cycle through the available matches by pressing **Enter**.

Select x to close the Search text box.

5 Select **Next**.

6 Review the Summary, and then select **Move**.

Deleting users

System Administrators and Managers can delete users with the exception that Managers cannot delete System Administrators. The notification and report settings and the private report and notification templates are deleted, also.

1. In the Administration view, select **Users**.
2. Select one or more users.
3. Select **Delete**.
4. Select **OK**.

Resetting a user password

System Administrators and Managers can reset a user password. If a user is locked, the account must be unlocked before the password can be reset. When a password is reset, use the temporary password sent by email to access your account. After providing the temporary password, you will be prompted to create a new password.

1. In the Administration view, select **Users**.
2. Select a user or users.
3. Select **Reset password**.
4. Select **OK**.

Changing user status

System Administrators and Managers can enable or disable a user.

1. In the Administration view, select **Users**.
2. In the Group name list, select a delegated group that contains the user.
3. Select a user.
4. Select **Status** from the drop-down list: Enable or Disable.

Unlocking a locked user

System Administrators and Managers can unlock a locked user.

1. In the Administration view, select **Users**.
2. Select the locked user.

3 Select **Unlock**.

Transfer user items to another user

System Administrators and Managers can transfer a user's items to another user who belongs to the same delegated group. The recipient becomes the new owner. The transferable items include Notification templates (Private, Shared, System share), Notification criteria, List report templates (Private, Shared, System share), List report schedules, and Graphical report schedules. You can select target items by function (i.e., Notifications, List reports, Graphical reports).

Transfer is not supported for a recipient that is disabled, has an expired password, or has not logged in to KFS.

5 NetGateway

NetGateway provides a simple method to register KYOCERA devices, legacy devices, and devices by other manufacturers to KYOCERA Fleet Services (KFS). NetGateway serves as a communication channel between devices and KFS. You can register devices automatically as part of discovery. You can configure periodic device discovery to register devices automatically and update device information for registered devices. A device in pending status can be re-registered in KFS.

The software solution includes a local agent that can be downloaded and installed on a remote computer. With the local agent, you can discover a device that is connected to the computer by a USB cable and register the device in KFS. Local agent retrieves information that is necessary for KFS to monitor or manage the USB-connected device.

NetGateway discovers devices that can be registered to a group with a configuration key or with an Access code and KFS Manager authentication (User name and Password). The configuration key is generated for a group and sent by email to the NetGateway user. Once the NetGateway is registered, devices can be registered to the associated group. The Gateway application must be registered in KFS before they can be used to discover devices.

NetGateway uses the Microsoft .NET framework and runs in a browser on a Windows computer. The NetGateway application communicates counter and consumable information through SNMP to the KFS device rest server. Counter and consumable information is set in Group management settings and requires devices that support NetGateway monitoring. KFS does not communicate directly with the devices.

Legacy devices can be monitored for counters and consumables but cannot be remotely managed with KFS tasks. USB devices can be registered as legacy devices.

NetGateway supports a maximum 2000 USB and/or network registered devices.

System Administrator, Manager, and Service users can access the Gateway tab in the Devices view.

You can sort the list by selecting column headings for Group, ID, Description, Connection status, Management status, Application version, Automatic upgrade, and Last update. The Connection status column also provides information about recent Gateway updates based on threshold settings.

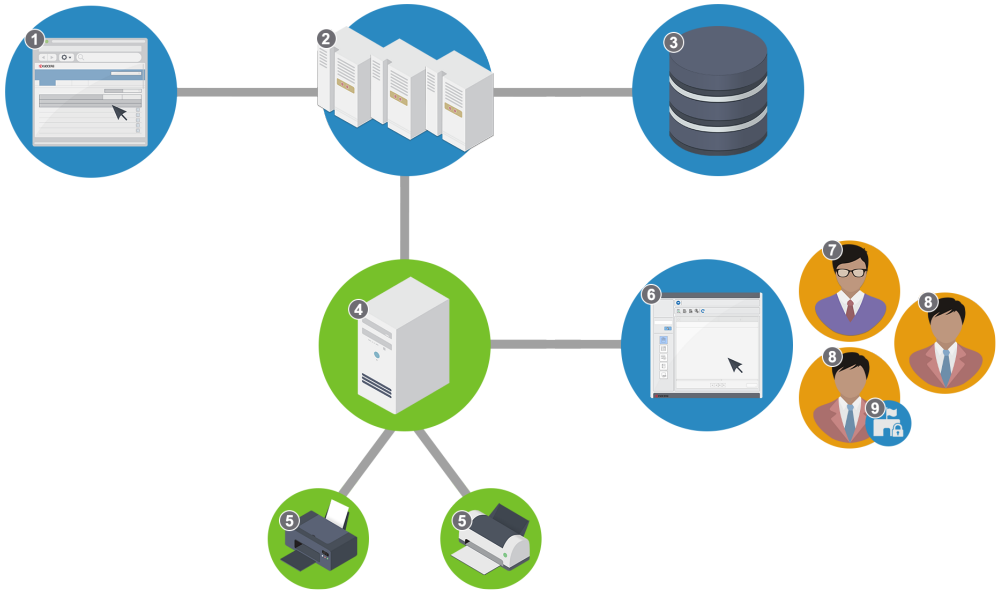
Management status includes the following:

Active

An active Gateway communicates with KFS after it has been registered. For a Gateway with a connection status in monitoring, the Gateway uploads from devices data, such as counters and consumable information, and events, such as paper jam errors. In this case, the Gateway is not available for maintenance tasks.

Archived

An archived Gateway does not communicate with KFS. The devices associated with the archived Gateway are set to offline and the Discovery settings and Gateway logs are retained in KFS. An archived Gateway can be reactivated by re-registering it to the same group.



Gateway	
1 - UI (Manager)	2 - KFS
3 - Database	4 - NetGateway
5 - Devices by other manufacturers and legacy devices	6 - UI (NetGateway)
7 - System Administrator	8 - Manager
9 - RHQ Permissions	

Downloading the NetGateway installer

System Administrators, Managers, and Service users can download the 64-bit NetGateway installer located in the Product downloads page. The installer is saved to your default download location on your computer.

1. In the top banner, select **Product downloads**.
2. Under NetGateway, select **Download**.
3. In your download folder, select the executable file to start installation.

Sending NetGateway by email

In KFS, System Administrators, Managers, and Service users can send the NetGateway installer to specified email recipients. The email includes a download link to access the NetGateway installer, information about what group NetGateway is associated with, and a configuration key that is associated with the selected group in KFS. The download link and the configuration key expire after 7 days.

After the NetGateway installation, the configuration key is used to register NetGateway or devices automatically.

1. In the Devices view, select **Gateway**.
2. Select **More** > **Send Gateway installer**.
3. For Add recipients, enter the recipient's addresses in the email addresses text box. For multiple recipients, separate each email with a semicolon.
4. Select a method.

   Create new

   Select your group, connection mode, device information update interval, and single point of communication in the steps that follow.

   Use existing

   Choose **Select Gateway** then select a gateway and choose **Select**. The chosen gateway is migrated to a new gateway after the configuration key sent in the email is used.

5. For Registration settings, select the **Group** to register Gateway with.

   You can enter a group name in the Search text box to locate a group.
6. (Optional) Enter a **Description** (256 character maximum).
7. Select **New discovery setting** or select the edit icon of an existing Discovery setting to modify.
8. Enter a **Description** (256 character maximum).
9. Select a **Discovery method**. The target varies based on the selected method. Select the plus button to add more addresses, address ranges, or host names.

   By local network

   Discovery on the local network. You can select both IPv4 and IPv6. IPv6 must be configured before it can be used to search for devices.

   By IP address or host name

   Discovery based on an IP address or host name of the devices. You can specify 100 IP addresses or host names.

   By IP address range

   Discovery based on the specified IP address range. You can specify a maximum of 10 IP address ranges.

10 Select **Search for USB connected devices**.

11 Select **Automatically register newly discovered devices**.

12 Enter a **TCP/IP port number** from 1024 through 65535 to match the port on the device.

13 Enter a **Timeout** value from 5 through 120 seconds.

14 Enter a number of **SNMP retries** that the application will attempt after a communication failure.

The valid range is from 0 to 5.

15 For the **SNMPv1/v2** protocol, enter the **Read community name** and **Write community name**.

The read and write community names are sent with all SNMP receive and send requests, and must match the community names on the device.

16 For **SNMPv3** protocol, enter the **User name**, **Password**, and **Context name**.

For SNMP authentication options, select from **SHA1** and **MD5**.
For SNMP privacy options, select from **AES** and **DES**.

17 Select **Enable SSL protocol**.

18 Select **Save**.

You can create a total of 10 discovery settings, which are included in the XML configuration file sent to the email recipient.

19 Select **Send**.

Gateway details

System Administrators, Managers, and Service users can view gateway details in the UI by selecting the information icon. The Details include the following:

ID

The Gateway ID

Gateway type

IB, PC, or NET

Description

The description of the gateway. To add or change the description, enter the description in the text box provided and select **Save** before closing the details dialog box.

IP address

IP address of the Gateway

Host name

Host name of the Gateway

Connection status

Online, Offline, or Monitoring

Management status

Active or Archived

Package version

The version number of the Gateway software. If a yellow icon is displayed, the gateway is out of date.

Application version

Device management identifies the application version.

Platform version

The version of the platform system: x86 (32-bit) or x64 (64-bit).

Registration date

The date and time the gateway was registered.

Last update

The date and time of the last gateway update.

Searching for Gateways

1. In the Devices view, select **Gateway**.
2. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following items use predefined options:

   Gateway type

   IB, PC, NET

   Management status

   Active, Archived

   Connection status

   Online, Offline, Monitoring

   Application version (Older than)

   Package version, other available versions

   Last update (Later than), Last update (Recent)

   24 hours, 7 days, 14 days, 30 days

   Automatic upgrade

   Enabled, Disabled
3. Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Upgrading a Gateway

System Administrators, Managers, and Service users can upgrade a gateway. The current version number displays and a yellow icon indicates the gateway is out of date. You can upgrade only an online gateway.

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select one or more online gateways.
4. Select **Upgrade**.
5. (Recommended) Select **Notifications** if you want to receive an email notification about the outcome of the upgrade.
6. Select **Upgrade**.

Restarting a Gateway

System Administrators, Managers, and Service users can restart one or more gateways. Closing the progress window does not stop the gateway restart process.

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select one or more gateways, and then select **Restart**.
4. Select **Notifications** if you want to receive an email notification.
5. Select **Restart**.

Archiving a Gateway

Administrator and Service users can select and archive multiple gateways.

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select one or more gateways.
4. Select **Archive**.

5 Select **OK**.

Deleting a Gateway

Administrator and Service users can select and delete multiple gateways. The devices that have been registered via Gateway are not deleted from the Manager and their connection status is set to Offline.

1 In the Devices view, select **Gateway**.

2 In the Group name list, select a group.

3 Select one or more gateways.

4 Select **Delete**.

5 Select **OK**.

Device discovery settings

Discovery settings are used for finding network devices and updating information for registered devices. System Administrators, Managers, and Service users can create, edit, and delete discovery settings. Accessed in the Gateway tab, the Discovery settings incorporate Discovery method, Communication Settings, and Device login. You can use the Find devices feature with Discovery settings to find and register devices. You can create a maximum of ten discovery settings for one gateway. Discovery settings are sent to KFS for data synchronization.

Adding discovery settings

System Administrators, Managers, and Service users can create discovery settings that can be saved and reused in KFS, or the selected NetGateway. These settings are used for finding devices on a local network.

1 In the Devices view, select **Gateway**.

2 In the Group name list, select a group.
You can enter a group name in the Search text box to find a group.

3 Select a gateway.
You cannot select multiple gateways.

4 Select **More** > **Discovery settings**.

5 Select **Add**.

6 (Optional) Enter a **Description** (256 character maximum).

7 Select a **Discovery method**.

The target varies based on the selected method. Select the plus button to add more addresses, address ranges, or host names.

By local network

Discovery on the local network. You can select both IPv4 and IPv6. IPv6 must be configured before it can be used to search for devices.

By IP address or host name

Discovery based on an IP address or host name of the devices. You can specify a maximum of 100 IP addresses or host names. You can also add IP addresses or host names by importing them from a .csv. Each row in the .csv must contain only one host name or IP address. A maximum of 100 addresses and host names can be contained in the file. Select **Browse** to find the file.

By IP address range

Discovery based on the specified IP address range. You can specify a maximum of 10 IP address ranges.

8 Select **Search for USB connected devices**.

9 Select **Automatically register newly discovered devices**.

10 Enter the **TCP/IP port number** from 1024 through 65535 to match the port on the device.

11 Enter a **Timeout** value from 5 through 120 seconds.

12 Enter the number of **SNMP retries** that the application will attempt after a communication failure with the device.

The valid range is from 0 to 5.

13 For the **SNMPv1/v2** protocol, enter the **Read community name** and **Write community name**.

The read and write community names are sent with all SNMP receive and send requests, and must match the community names on the device.

14 For **SNMPv3** protocol, enter the **User name**, **Password**, and **Context name**.

For SNMP authentication options, select from **SHA1** and **MD5**.
For SNMP privacy options, select from **AES** and **DES**.

15 Select **Enable SSL protocol**.

16 For SNMP authentication type, select **Local authentication** or **Device settings**.

These settings determine whether device or local computer authentication is used.

17 For Authentication information, enter your **User name** and **Password**.

18 Select **Save**. You can create a maximum of 10 discovery settings.

The saved settings are listed on the Discovery settings page.

Editing discovery settings

System Administrators, Managers, and Service users can modify saved discovery settings for gateways.

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select a gateway.
4. Select **More** > **Discovery settings**.
5. Select the Discovery settings, and then select **Edit**.
6. Change the Discovery settings, and then select **Save**.

Deleting discovery settings

System Administrators, Managers, and Service users can delete discovery settings for Gateways that have been saved in KFS.

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select a gateway.
4. Select **More** > **Discovery settings**.
5. In the Discovery settings list, select one or more discovery settings, and then select **Delete**.
6. Select **OK** to confirm.

Finding devices

You can use existing Discovery settings to find and register devices. It also updates the information, such as the host name of registered devices that fall within the scope of the discovery setting.

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select a gateway that is online.

4 Select **More** > **Discovery settings**.

5 Select a discovery setting.

6 Select **Find devices**.

7 Select **Automatically register newly discovered devices** if you want to register the discovered devices.

8 Select **Find**.

Searching for Gateway discovery settings

1 In the Devices view, select **Gateway**.

2 In the Group name list, select a group.

3 Select a gateway.

4 Select **More** > **Discovery settings**.

5 In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following items use predefined options:

Discovery method

By local network, By IP address or host name, By IP address range

Last discovery (Later than), Last discovery (Recent)

24 hours, 7 days, 14 days, 30 days

6 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Gateway logs

Gateway logs provide information for Service users to resolve Gateway issues. System Administrators, Managers, and Service users can select the gateway logs to be obtained from the Gateway. Gateway logs are obtained based on the Gateway Log Settings.

Retrieving Gateway logs

1 In the Devices view, select **Gateway**.

2 In the Group name list, select a group.

3 Select a gateway that is online.

4 Select **More** > **Gateway logs**.

5 Select **Retrieve**.

The retrieved logs are added to the Gateway logs list. If Retrieve is grayed out, the Connection status of the selected Gateway is offline or monitoring.

Searching Gateway logs

1 In the Devices view, select **Gateway**.

2 In the Group name list, select a group.

3 Select a gateway.

4 Select **More** > **Gateway logs**.

5 In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following items use predefined options:

Timestamp (Later than), Timestamp (Recent)

24 hours, 7 days, 14 days, 30 days

Type

Gateway system logs, Gateway audit logs

6 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Editing Gateway log settings

You can select the type of log information that KFS can retrieve from a gateway.

1 In the Devices view, select **Gateway**.

2 In the Group name list, select a group.

3 Select a gateway.

4 Select **More** > **Gateway logs**.

5 Select **Settings**.

6 Select the **Type of logs**, **Gateway system logs**, and **Gateway audit logs**, and then select **Save**.

Downloading Gateway logs

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select a gateway.
4. Select **More** > **Gateway logs**.
5. Select one or more gateway logs.
6. Select **Download**.
7. Open or save the gateway logs.

Deleting Gateway logs

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select a gateway.
4. Select **More** > **Gateway logs**.
5. Select one or more gateway logs.
6. Select **Delete**.
7. Select **OK**.

Gateway settings

Service users and Managers can modify Gateway settings to set the frequency of Device information update interval and the automatic software upgrade setting. The interval setting has no effect if the gateway has no existing discovery settings.

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select one or more gateways.
4. Select **More** > **Gateway settings**.
5. Select a device refresh interval:

- **6 hours**
- **12 hours**
- **24 hours**.

6 Select **Enable automatic upgrade**.

Daily (at time of Gateway registration)

Checks for gateway upgrades based on the same time of day the gateway was originally registered.

Specified time

Checks for gateway upgrades at the same time of day, as specified by the user.

7 Select **Save**.

Gateway migration

Gateway for Windows can be migrated to NetGateway. The source gateway must be online, and without on hold tasks or network issues. Multiple gateways can be migrated at once. Gateway settings, devices, and discovery settings are part of the migration.

For a 32-bit operating system, the Gateway cannot be migrated to the 64-bit NetGateway. Only 64-bit operating systems are supported for NetGateway upgrades.

You can view messages about the migration at the bottom of the Gateway Migration Summary screen.

Migrating Gateway

System Administrators and Service users can migrate multiple PC Gateways (Gateway for Windows). Gateway migration cannot be made to a computer with NetGateway already installed and registered in KFS.

1 In the Devices view, select **Gateway**.

2 In the Group name list, select a group.

3 Select one or more online PC Gateways.

4 Check the Gateway Migration Summary screen. Select the **Notifications** check box to be notified when the migration finishes.

5 Select **Migrate**. You can wait for the progress window to close or you can select **Close**.

The progress of the migration is not interrupted when you close.

The notification email describes the completed task type and result, migrated gateway id and type, destination gateway id, timestamp information and timezone of KFS, and the product name which refers to the branding information applied to the migrated Gateway.

In the event of a migration failure, check that the 32-bit or 64-bit installer matches your operating system.

Viewing associated devices

You can view the devices associated with a gateway.

1. In the Devices view, select **Gateway**.
2. In the Group name list, select a group.
3. Select a gateway.
4. Select **More** > **Associated devices**.

You can manage the devices displayed in the search results.

6 Mobile management

With KFS, you can manage mobile devices in a delegated group. System Administrators, Managers, and Service users can view, edit, archive, and delete a registered mobile device in KFS. When the mobile device is used for the first time with KFS, it is registered with your User name, Password, and Access code. These login credentials connect the device to the user's delegated group in KFS.

Archiving a mobile device lets you disable that device in KFS. The mobile device appears as Archived in the Administration view. You can archive multiple mobile devices at one time.

Any device registered by the mobile device before the mobile device has been deleted, remains registered in KFS and the device's registration type is changed to None. If you register the same deleted mobile device again, any devices previously associated with the deleted mobile device will not be associated with the re-registered device.

The following mobile details are available:

ID

The Mobile ID.

Group

A registered group in KFS. The Group menu is not available to Service users.

Model name

The model name of the mobile device.

Mobile OS and version

The mobile device operating system and version.

Application version

The version of the KFS mobile software.

Description

The description of the mobile device.

User

The User ID of the person who uses the mobile device.

Registration Date

The date and time the mobile device was registered to KFS.

Searching for mobile devices

You can use search filters to find mobile devices.

1. In the Administration view, select **Mobile**.
2. In the Group name list, select a group.
3. In the Search text box, select a search category, and then enter a search string or select a predefined search option. The following item uses predefined options:

   Management status

   Active, Archived
4. Select the search icon.

   Select x in the Search box to clear the search value and restore the view to the original list.

Archiving mobile devices

You can archive one or more mobile devices.

1. In the Administration view, select **Mobile**.
2. In the Group name list, select a group.
3. Select one or more mobile devices.
4. Select **Archive**.
5. Select **OK**.

Editing a mobile device description

You can edit the description of a registered mobile device.

1. In the Administration view, select **Mobile**.
2. In the Group name list, select a group.
3. Select the information icon for the mobile device.
4. Edit the **Description** (256 character maximum).
5. Select **Save**.
6. Select **Close**.

Deleting mobile devices

You can delete one or more mobile devices.

1. In the Administration view, select **Mobile**.
2. In the Group name list, select a group.
3. Select one or more mobile devices.
4. Select **Delete**.
5. Select **OK**.

7 Firmware packages

The Firmware packages tab is where device firmware .zip files are stored. There are five firmware package release types: Official, Custom, Long-term test, Short-term test, and Evaluation. KYOCERA releases official firmware to the market and custom firmware only to a specific company or dealer. Users have varying permissions for this feature depending on their user role. Analysts and Customers do not have access to Firmware packages.

System Administrators, Managers and Service users can do the following:

- Download firmware packages
- View Readme files

System Administrators and all Managers can do the following:

- Publish firmware one tier down. (System Administrators and RHQ Managers are not restricted to one tier.)
- Unpublish firmware
- Grant Service users access to the non-official firmware

System Administrators and Managers with RHQ permissions can do the following:

- Add, edit, and delete Readme files from unpublished packages

System Administrators can do the following:

- Upload firmware to any group
- Official firmware uploaded to ROOT will automatically publish to the first tier delegated groups
- Edit descriptions of all packages
- Delete firmware from any group

Managers with RHQ permissions can do the following:

- Upload firmware to RHQ delegated groups they have access to
- Must publish Official packages from System Administrators before current group users and child groups get access
- Edit descriptions for packages they upload
- Delete firmware they uploaded

Firmware packages for some devices are digitally signed with public keys in the form of X.509 certificates. You can view the details of firmware packages, and the certificates associated with the firmware packages. You can download firmware packages to your computer.

If the Firmware package metadata is incorrect and unusable, KFS prevents it from being uploaded. In this event, KFS posts an error message.

Uploading firmware packages

System Administrators and Managers with RHQ permissions can upload Firmware packages.

1. In the Administration view, select **Firmware packages**.
2. In the Group name list, select a group.
3. Select **Upload**. The package is uploaded to the selected group and only users with access rights and associated with this group can access a firmware package.
4. Select **Browse** to find a firmware file as a .zip located on your computer.
5. Select a Readme type: **File**, **Text or images**, **Announcement**.
6. Select a Readme from your computer, write a new Readme, or link a Readme to an existing announcement.
7. Select **Upload**.

Adding a Readme

System Administrators and RHQ Managers can add a Readme to an unpublished firmware package after it has been uploaded.

1. In the Administration view, select **Firmware packages**.
2. In the Group menu, select a group.
3. In the Firmware packages list, select the package you want to add the Readme to and select **Add readme** in the Readme column.
4. In the Upload Readme wizard, select a **Readme** type:
   - File
   - Text or images
   - Announcement
5. Select a **Readme** on your computer, write a new Readme file, or link a Readme to an existing announcement.
6. Select **Upload**.

Deleting a Readme

System Administrators can delete a Readme from any unpublished firmware package and Managers with RHQ permissions can delete a Readme from an unpublished firmware package in their group.

1. In the Administration view, select **Firmware packages**.
2. In the Group menu, select a group.
3. In the Firmware packages list, select a **Readme**.
4. In the Readme dialog, select **Delete**.
5. Select **Close**.

Viewing the firmware package list

You can view the firmware packages in KFS.

1. In the Administration view, select **Firmware packages**.
2. In the Group menu, select a group.
3. Review the firmware package details.

Downloading firmware packages

You can download one or more firmware packages as .zip files to your computer.

1. In the Administration view, select **Firmware packages**.
2. In the Group menu, select a group.
3. Select the firmware packages.
4. Select **Download**.

Viewing firmware package details

You can see the details of Firmware packages, including the certificates associated with signed packages.

1. In the Administration view, select **Firmware Packages**.
2. In the Firmware Packages list, select the information icon of the firmware package. If your access rights are limited, then select your group in the Group name list.

   The details display the following information:

   - Package name
   - Package version
   - Group
   - Description

- Readme
- Package type
- Target devices
- Size
- Date created
- Date released
- Release type
- Signed
- Uploaded by
- Publication status
- Published by
- Certificates
- Firmware version

3 Select **Close**.

Readme files

Readme files contain messages with text and images that you can add to firmware packages in KFS. You can add Readme files in the following formats: .jpg, .gif, .png, .pdf, .doc, .docx, .rtf, .html, and .txt. You can link a Readme file to an existing announcement.

Viewing a Readme file

You can view the contents of a Readme file.

1 In the Administration view, select **Firmware packages**.

2 In the Group menu, select a group.

3 In the Firmware packages list, select the Readme from the **Readme** column.

4 In the Readme dialog, view the contents of the Readme file.

5 Select **Close**.

Downloading a Readme file

You can only download the Readme associated with a firmware package.

1 In the Administration view, select **Firmware packages**.

2 In the Group menu, select a group.

3 In the Firmware packages list, select a Readme.

4 In the Readme dialog, select **Download**.

5 Select **Close**.

Searching for firmware packages

You can search for firmware packages.

1 In the Administration view, select **Firmware packages**.

2 In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following categories use predefined options:

Release type

Official, Custom, Long-term test, Short-term test, Evaluation

Package type

Main firmware package, Optional enhancement package, Optional language package

Signed

Yes, No

Publication status

Published, Unpublished

Released (Recent), Released (Later than)

7 days, 30 days, 3 months, 6 months

3 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Searching for firmware packages using advanced search

You can search for firmware packages using multiple criteria with the Advanced search feature. You can combine 5 search properties in Advanced search.

1 In the Administration view, select **Firmware packages**.

2 Under the search text box, select **Advanced search**.

3 In the Advanced Search dialog box, select **Search criteria**.

4 Choose **Select property** and choose a search property from the drop-down list. For search properties, you can select from the following:

- Date created

- Date released
- Description
- Firmware version
- Group name
- Package name
- Package type: Main firmware package, Optional enhancement package, Optional language package
- Package version
- Release type: Official, Custom, Long-term test, Short-term test, Evaluation
- Size (MB)
- Target devices

If you select Group name as a search property, select the edit icon to choose the individual groups or all accessible groups. If you select **All accessible** under Quick select, then each parent group that you select expands the group tree and selects all of the affiliated child groups. Select **Search** and enter the group name to quickly find a group.

5 In the drop-down list, select a search operator. The options are based on the selected property and may include Contains, Belongs to, Does not contain, Equals, Does not equal, Starts with, Ends with, Before, After, Greater than, Greater than or equal to, Less than, Less than or equal to.

6 Enter a search term in the text box, if necessary.

7 Select **Search**.

As an alternative search method, select **Recent searches**, then select from the available searches. Clear your entries in the Advanced search by selecting **Reset**.

Editing firmware package descriptions

System Administrators and Managers with RHQ permissions can edit descriptions for firmware packages if permissions allow.

1 In the Administration view, select **Firmware packages**.

2 In the Firmware packages list, select a firmware package.

3 Select **Edit**.

4 Enter a new description in the Description box (256 character maximum).

5 Select **Finish**.

Granting Service users access to custom firmware

System Administrators and Managers can grant service users access to Custom firmware packages.

1. In the Administration view, select **Firmware packages**.
2. In the Firmware packages list, select a custom firmware package.
3. Select **Edit**.
4. Select **Next**.
5. Select the service users to grant access to the custom firmware. Use the Search text box to find specific users.
6. Select **Finish**.

Signed and unsigned firmware packages

According to Canada's Anti-Spam Law (CASL), any software installation on a device requires express consent. Firmware upgrade involves software installation.

You can upload signed and unsigned packages in the Administration view of KFS. When uploading a firmware package, KFS checks the certificate and condition of the package. If the package has malformed XML or mismatched models, the firmware is rejected, whether or not a certificate is present. If a package has no certificate, the firmware package does not undergo certificate validation. KFS warns you if the package has no certificate.

The device also validates the firmware package during the upgrade. Packages for some newer devices are signed with public keys in the form of X.509 certificates.

Deleting firmware packages

System Administrators can delete any firmware packages. Managers with RHQ permissions can delete firmware packages they uploaded. You cannot delete a package that is in use for a scheduled task.

1. In the Administration view, select **Firmware Packages**.
2. In the Firmware packages list, select the firmware packages you want to delete.
3. Select **Delete**, and then select **OK**.

Publishing firmware packages

If firmware packages are not directly uploaded to a group, groups can gain access to firmware packages if a parent group publishes the package to them, granting them access. System Administrators and Managers have permissions to publish firmware from their group to any child groups. Managers without RHQ permissions can only publish to child groups directly below them. To publish further down, you must navigate to the lower level and repeat the process. RHQ Managers must publish Official packages before their child groups can access it. Readme files of published packages cannot be edited or deleted.

1. In the Administration view, select **Firmware packages**.
2. In the Firmware packages list, select an official or custom firmware package.
3. Select **Publish**.
4. For official firmware package, select **Close**.
5. For custom firmware package, select a group.
6. Select **Next**.
7. Select **Publish**.
8. Select **Close**.

Unpublishing firmware packages

You can unpublish and remove group access to firmware packages. You cannot select a group if the package is not published to that group. Unpublishing firmware packages from a group also unpublishes the package from all of the associated child groups. Pending tasks fail if the firmware packages that are being used are unpublished.

1. In the Administration view, select **Firmware packages**.
2. In the Firmware packages list, select the official or custom firmware package.
3. Select **Unpublish**.
4. For official firmware package, select **Close**.
5. For custom firmware package, select a group.
6. Select **Next**.
7. Select **Confirm**.
8. Select **Close**.

8 Logs

KFS provides logs for delegated group events so Managers and System Administrators can track both operations (Audit logs) and email transmissions (Email logs) sent from KFS. Audit logs contain operations history for the selected delegated group related to user, group, and device events. System Administrators and Managers can check the log to ensure security and operational efficiency. Email logs contain information about emails generated by KFS and stored in the database. This includes the transmission history of emails sent to recipients outside of KFS. System Administrators and Managers can check emails sent to users about specific KFS events such as user registration.

A maximum of 10,000 logs is supported. You can download .csv logs to your computer in zip format. The log file name includes the name of the delegated group and a timestamp.

Audit logs list

You can view the list of Audit logs for a delegated group. In this list, you can view the following information:

Timestamp

The timestamp of the operation.

Type

The type of operation saved as an event in the database.

Result

The outcome of the operation.

Email address

The email address of the user who performed the operation

User name

The name of the user who performed the operation

Audit logs are stored for sixty days. A maximum of 10,000 logs with 50 logs per page view is supported. The downloadable .csv Audit log contains more details about delegated groups and users.

Audit logs details

In the Audit logs list, you can view Audit logs details of a single operation by selecting the information icon. The Audit logs timestamp is displayed at the top of the details dialog box. The details include the following information:

Source IP

The global IP address of the user who performed the operation.

Type

The type of task, operation, or event recorded in the database.

Result

The result of the operation.

Reason

The reason for the outcome as stated in an error or status message.

Email address

The email address of the user who performed the operation.

User ID

The User ID of the user who performed the operation.

User name

The name of the user who performed the operation.

Role

The role of the user who performed the operation.

Delegated group

The name of the delegated group.

Delegated group ID

The ID of the delegated group.

Remarks

Remarks vary based on the type of event.

Searching audit logs

1. In the Administration view, select **Groups**.
2. Select a delegated group.
3. In the toolbar, select **Views** > **Audit logs**.
4. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following items use predefined options:

   Timestamp (Later than), Timestamp (Recent)

   24 hours, 7 days, 14 days, 30 days

   Result

   Successful, Failed

5 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Downloading audit logs

1 In the Administration view, select **Groups**.

2 Select a delegated group.

3 Select **Views** > **Audit logs**.

4 Select **Download**.

Email logs list

You can view the list of email logs for a delegated group. In this list, you can view the following information:

Timestamp

The timestamp of the operation.

Type

The type of operation saved as an event in the database.

Result

The outcome of the sent email.

Recipient

The destination email address.

Email address

The email address of the user who generated the entry.

Email logs are stored for sixty days. A maximum of 10,000 logs with 50 logs per page view is supported. The downloadable .csv Email log contains more details about delegated groups and users.

Email log details

In the Email logs list, you can view the details of a single email operation by selecting the information icon. The Email logs timestamp appears at the top of the details dialog box. The details include the following information:

Type

The type of operation or event recorded in the database.

Result

The result of the operation.

Reason

Email address

Recipient

The destination email address.

Subject

The title of the email.

Delegated group

The name of the delegated group.

Delegated group ID

The ID of the delegated group that performed the operation.

Searching email logs

1. In the Administration view, select **Groups**.
2. Select a delegated group.
3. In the toolbar, select **Views** > **Email logs**.
4. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following items use predefined options:

   Timestamp (Later than), Timestamp (Recent)

   24 hours, 7 days, 14 days, 30 days

   Result

   Successful, Failed
5. Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Downloading email logs

1. In the Administration view, select **Groups**.
2. Select a delegated group.
3. Select **Views** > **Email logs**.

4 Select **Download**.

Downloaded email logs include additional information such as the body of the email sent.

9 Devices

In the Devices list, you can view and check detailed information from registered devices connected to a group. The Devices list is refreshed every 30 minutes, with the exception of the default Counter view menu. The maximum number of devices displayed on the devices list is 3000. You can select a device from the Devices list and view the log information.

The Group name list displays Favorites and All groups for easier navigation between favorite devices and groups. You can expand the column to display the Managed and Total counts for devices and total device counts. The information icon displays group details, including User permissions. In Display settings, you can add and arrange the information displayed in the Devices list columns. In the View drop-down list, you can select from the four default device views, General, Counter, Firmware, Maps, plus custom views you have created. For the Counters view, you can add, remove, and reorder the columns in **Column** > **Edit**.

Use Display settings to create and edit views including display order and the threshold for device inactivity.

In Edit custom fields, you can make changes to Custom field 1 - 3, description, and location information for a single device or a group of devices.

To filter devices in the Group name list, select one of the following three options from the Include drop-down menu.

Devices exclusive to this group

Devices registered to the selected group only.

Exclusively managed

Devices in the selected group and the regular child groups.

All accessible

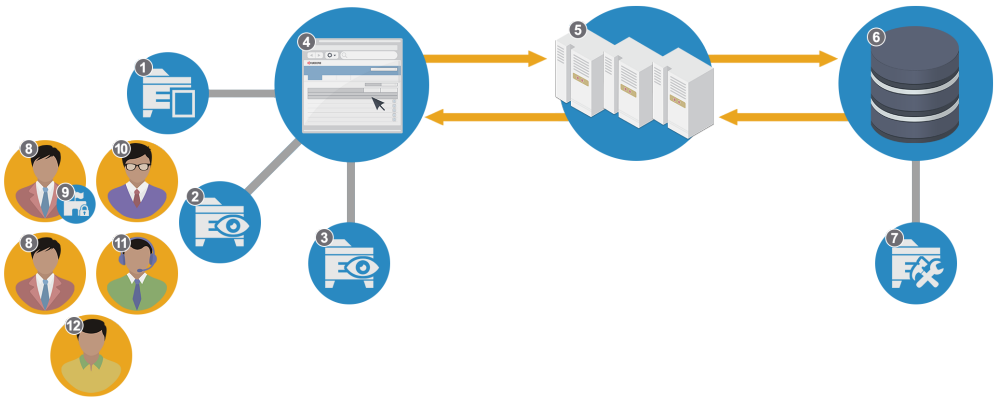
Devices in the selected group and all the child groups below.

Devices list

In the Devices list, you can also customize your device views, including creating a threshold setting for inactive devices. The No recent updates warning applies to Offline or Monitoring device status. The threshold for device inactivity can be set within a range between 3 and 90 days.

For the Counters view, you can edit the columns to add more counter information.

You can only view information from devices that you have permission to access.



Device List	
1 - Device List	2 - Device View Select and Edit
3 - Device View Edit	4 - UI (Manager)
5 - KFS	6 - Database
7 - Custom Device View	8 - Manager
9 - RHQ Permissions	10 - System Administrator
11 - Service	12 - Customer

Advanced search

Use Advanced Search to search for devices in all groups and delegated groups. You can select advanced search criteria to narrow the number of devices. You can select from recent searches. The More details link in the search results shows the selected property, search term, and timestamp of the search.

Searching for devices using search criteria

Configure a maximum of 5 search criteria in Advanced Search.

1. In the Devices view, select **Advanced search**.
2. Select **Search criteria**.
3. Choose **Select property** and choose a search property from the drop-down list. You can use 5 search categories in advanced search. For devices search fields, you can select from the following:
   - Asset number
   - Customer ID
   - Customer name
   - Description
   - Engine firmware
   - Group

- Host name
- IP address
- Location
- Management status: Managed, Unmanaged, Archived, Pending, Not registered
- Manufacturer
- Model name
- Serial number
- Status: Ready, Monitoring, Warning, Error, Offline
- System firmware

4 Select a search operator from the drop-down list. The options include Contains, Does not contain, Equals, Does not equal, Starts with, Ends with.

5 Enter a search string or select a predefined option.

6 Select **Search**.

7 In the Search Results, select **More details** to display the selected property, search term, and timestamp of the search.

As an alternative search method, select **Recent searches**, then select from the available searches. Clear your entries in the Advanced search by selecting **Reset**.

Searching for a device using a serial number

You can search for a specific device using a serial number in the Devices view.

1 In the Serial number text box, enter the **Serial number**.

2 Select the search icon.

In the Device Summary view, the total number of devices is displayed at the top of the list.

Creating a favorites group

You can create a maximum of ten favorite groups. The selected group is listed in the favorites section in the group name list.

1 In the Devices view, select a group.

2 Select the star icon next to the group name in the banner.

Creating custom device views

You can add custom device views and change the order in which the device information is displayed.

1 In the Devices view, select a group.

2. Select **Display Settings**.
3. In Display settings, select the add icon. If the add icon is gray, the maximum of 10 custom settings has been reached.
4. Enter a **View name** (64 character maximum).
5. In Available columns, select the items you want to display, and then select the right arrow to move them to Selected columns.

   To reorder Selected columns, choose an item, and then use the up and down arrows to move the item. By default, Serial number/Model name is included in Selected columns. To remove items from Selected columns, select the item and select the left arrow.
6. Select **Save**.
7. For any selected Display settings, choose how devices are sorted to view by **Management status**, **Status**, or **None** (no sorting).

   Management status is the default status. The Management status types are Managed, Unmanaged, Archived, Pending, and Not registered. The Status types are Ready, Warning, Error, Offline, and Monitoring.
8. Select **Save**.

The devices registered to the group are displayed in the devices list.

Editing custom device views

You can make changes to the device views you created. You cannot edit the default device views.

1. In the **Devices** view, select a group.
2. In Display settings, select a custom view.
3. Select the edit icon.
4. To rename a device view, enter a new **View name** (64 character maximum).
5. In Available columns, select the items you want to display, and then select the right arrow to move them to Selected columns.

   To reorder Selected columns, choose an item, and then use the up and down arrows to move the item. To remove items from Selected columns, select the item and select the left arrow.
6. Select **Save**.

Deleting custom device views

You can delete one custom device view at a time.

1. In the Devices view, select a group.
2. Select **Display settings**.
3. Select a custom view, and then select the delete icon.
4. Select **OK**.

Switching device views

You can change your default view of the devices list. The View drop-down list includes default views for General, Counter, Firmware, and Maps. You can also select custom views which are created and edited in display settings.

1. In the Devices view, select the group.
2. In the View drop-down list, select a view.

Filtering the devices list

You can filter the Devices list using categories in the search list. The type of category depends upon the default or custom views selected in the View list.

1. In the Devices view, select a group.
2. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option.
3. Select the search icon.

   Select x in the Search box to clear the search value and restore the view to the original list.

Tasks menu

Use the Tasks menu to create new device tasks by managing features in KFS. You can access the Tasks menu in the Devices view.

You can manage the following features for online and offline devices from the Tasks menu:

- Firmware upgrade
- Device settings
- Maintenance mode
- Restart
- Retrieve snapshots
- Send file
- Panel note
- Manage HyPAS Applications
- Backup data

More menu

Use the More menu to manage devices, create toner order recommendation thresholds, or export logs. Within a group, you can manage registered devices by performing the following tasks from the More menu:

- Change status
- Move
- Delete
- Archive
- Export device logs
- Toner order criteria

Device management status

Device Management Status determines what users can do with devices. A device must first be registered before device management status can be modified. System Administrators, Managers, and Service users can change the management status of multiple registered devices simultaneously.

The following device management status is supported for devices:

Pending

A registered device that has not been converted to "Managed" or "Unmanaged" status. The device has been registered with an Access code. Once the status changes, a device cannot be returned to a pending status. In the device information, users can monitor device logs and counters. The device cannot be maintained remotely. System Administrators, Managers, and Service users can change the device management status from pending to managed or unmanaged.

Managed

A registered device that is being managed within a group and for which Tasks can be applied. The device has been registered with an Access code and user credentials. Managed devices can receive firmware upgrades, maintenance mode, device settings, send files, and retrieve snapshots. System Administrators, Managers, and Service users can change the device management status from managed to unmanaged or archived.

Unmanaged

A registered device for which only monitoring functions are available. The device cannot be maintained remotely. System Administrators, Managers, and Service users can change the device management status from unmanaged to managed or archived.

Archived

The device can be viewed but no monitoring or maintenance can be performed on the device. Once the device is archived, device management status cannot be changed.

Not registered

The device information is not updated and the device registration is unfinished.

Changing the device management status to Archived

System Administrators, Managers, and Service users can change the device management status to Archived. When the device management status is Archived, the device information is not updated and no notifications are sent from the device.

1. In the Devices view, select a group.
2. Select one or more devices.
3. Select **More** > **Archive**.
   A warning screen displays.
4. Select the box to confirm the choice to archive the device or devices.
5. Select **Archive**.

Changing the device management status to Managed or Unmanaged

System Administrators, Managers, and Service users can change the device management status in KFS.

1. In the Devices view, select a group.
2. Select one or more devices.
3. Select **More** > **Change Status**.
   - For Managed devices, select Unmanaged
   - For Unmanaged devices, select Managed
   - For Pending devices, select Managed or Unmanaged

Moving devices to a different group

System Administrators and Managers can move registered devices from one group to another group. The summary page provides a list of the affected settings.

1. In the Devices view, select a group.
2. Select one or more devices.
3. Select **More** > **Move**.
4. Move the selected devices by selecting a group listed in the New Group column, and then select **Next**.

You can select **Search**, enter a group name to find the group, and press **Enter**. Select x to close the Search text box.

5 Review the Summary, and then select **Move**.

6 Select **Close**.

Deleting devices

You can delete devices depending on your user role.

1 In the Devices view, select a group.

2 Select one or more devices.

3 Select **More** > **Delete**.

4 Confirm your choice in the dialog box that displays.

5 Select **Delete**.

6 Select **OK**.

Exporting device logs of a device

You can export a device logs for a single device. The device logs include consumable, counter, event, and system errors. Analysts and customers cannot view or export device logs.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Device logs**.

4 Select **Export device logs**.

You can download device logs in a .zip format to your computer.

Exporting device logs for multiple devices

You can export device logs for multiple devices to your computer. The device logs include consumable, counter, event, and system errors. Device logs can be downloaded in a .zip format to your computer. Analysts and customers cannot view or export device logs.

1 In the Devices view, select the group.

2 Select the devices.

3 Select **More** > **Export device logs**.

Editing counter view columns

You can modify the columns in the Counter view.

1 In the Devices view, select a group.

2 In the View drop-down list, select **Counter (Default)**.

3 Select **Column** > **Edit**.

4 Select **Add counters** to choose from the available counters. Select **Deselect all** to clear the selected counters.

5 Select **Save**.

6 Use the up and down arrows to set the order of items in the list.

7 Select **Save**.

If you want to return the selected counters to the default, select **Column** > **Reset**.

10 Toner orders

KFS supports detailed toner reporting, ordering, and tracking for all of your devices. You can set up toner notifications for devices that report toner status by a specified toner level. You can set up toner notifications based on the level of individual colors, control the frequency of notification, and select toner for specific devices or groups.

Toner ordering can be set up to be done automatically or on a manual basis. Once the toner order is placed, specified recipients receive an email containing the toner order request. The toner order email includes the Group path, Model name, Serial number, Asset number, Location, Color, Toner name, and Quantity. Detailed toner reports can be viewed in Device log graphs where toner can also be ordered.

You can set toner order replacement for devices and groups. The software provides functionality to predict the number of days until the next toner replacement date. Replacement based on toner level by percentage is also available. This feature is available for devices with Managed or Unmanaged status.

Toner order criteria

System Administrators and Managers can set the recommendation criteria for toner replacement by group. System Administrators, Managers, and Service users can set the recommendation criteria for toner replacement by device. The toner recommendation options include an estimated number of days of remaining toner, the device's toner level, or a combination of both. You can establish thresholds for monochrome devices and for each of the four colors on color devices. Levels cannot be displayed for devices with non-genuine toner.

By default, the toner replacement recommendation is off.

Toner order list

The Toner order list provides information about toner for the devices managed by users with access authority. If the devices meet the toner order criteria, then the toner status displays the Order toner icon (based on the graph). Hover over the icons in the status column to view the state.

Order toner

The toner order criteria meets the preset levels. According to these levels based on device or group specific settings, you should order toner.

Order placed

The toner order criteria threshold was met and toner was ordered. The icon is updated when the order is placed.

Flagged

The toner order criteria threshold has been met or an order has been placed and the user has flagged toner with a remark.

Devices in the Toner order list are organized into three categories based on the whether toner order criteria is met. They include the following:

Recommended

Toner order criteria has been met.

Optional

Toner order criteria has not been met.

Not applicable

Toner order criteria has not been set or device management status is not managed or unmanaged.

Setting toner order recommendations for a group

System Administrators and Managers can set Toner ordering thresholds for a group. The toner order functionality includes the capacity to estimate the number of days remaining toner based on current usage levels.

1. In the Administration view, select the group or groups.
2. Select **Toner order criteria**.
3. Select a color.
4. Enter values for the **Toner replacement prediction** (days), the **Toner level** (percentage), or both.

   The range is 0 to 30 days for the toner replacement prediction and 0 to 100% for the toner level.
5. Repeat for each color.
6. Select **Save**.

Setting toner order recommendations for devices

System Administrators, Managers, and Service users can set Toner ordering thresholds for devices. The toner order functionality includes the capacity to estimate the number of days remaining toner based on current usage levels.

1. In the Devices view, select a group.
2. Select one or more devices.
3. Select **More** > **Toner order criteria**.
4. Select a color.

   By default, all colors and **Use group criteria** are selected. To disable toner order recommendations for any color, clear the check box for that color.

5 Select **Use group criteria** to use the values established for the group or select **Customize**.

6 For Customize, enter values for the **Toner replacement prediction** (days), the **Toner level** (percentage), or both.

The range is 0 to 30 days for the replacement prediction and 0 to 100% for the toner level.

7 (Optional) Repeat for each color.

8 Select **Save**.

Manual toner ordering

Users with access authority to a group can place a manual toner order.

1 In the Devices view, select a group.

2 Select **Toner order**.

3 Select **View** > **Manual orders**.

4 Expand a device by selecting the down arrow.

5 Select toner colors to order for devices.

6 Select **Order**.

7 In the Quantity column, increase or decrease the number for each toner to include in the order.

8 Select **Next**.

9 Select **Me** to receive the email order.

10 Enter email addresses for additional recipients.

You can add multiple email addresses, separated by semicolons.

11 (Required) Enter the **Email subject** to accompany the order.

12 (Optional) Enter any **Remarks**.

13 To include an attachment to accompany the email order, select **Toner order information** then select .csv or .xml format in the drop-down list.

14 Select **Next**.

15 Review the Summary, and then select **Order**.

Automatic toner ordering

Users with access authority to a group can place an automatic toner order.

1. In the Devices view, select a group.
2. Select **Toner order**.
3. Select **View** > **Automatic orders**.
4. Expand a device by selecting the down arrow.
5. Select toner colors to order for devices.
6. Select **Order**.
7. Select **Next**.
8. Select **Me** to receive the email order.
9. Enter email addresses for additional recipients.
   You can add multiple email addresses, separated by semicolons.
10. (Required) Enter the **Email subject** to accompany the order.
11. (Optional) Enter any **Remarks**.
12. To include an attachment to accompany the email order, select **Toner order information** then select .csv or .xml file type in the drop-down list.
13. Select **Next**.
14. Review the Summary, and then select **Order**.

Ordering toner in the toner history list

You can order toner in the Toner History section of Device log graphs.

1. In the **Devices** view, select a group.
2. Select the **Serial number** of a device.
3. Select **Device logs** > **Graphs** > **Type** > **Counters**, **Consumables** or **Both counters and consumables**.
4. Under Toner history list, select **Order**.
5. In the Quantity column, increase or decrease the number of each toner to include in the order.
6. Select **Next**.

7 Select **Me** to receive the email order.

8 Enter email addresses for additional recipients.
You can add multiple email addresses, separated by semicolons.

9 (Required) Enter the **Email subject** to accompany the order.

10 (Optional) Enter any **Remarks**.

11 To include an attachment to accompany the email order, select **Toner order information** then select .csv or .xml file type in the drop-down list.

12 Select **Next**.

13 Review the Summary, and then select **Order**.

Setting toner order flags

Users with access authority to a group can set flags for manual toner orders and add remarks for toner. Multiple toners for available devices can be flagged at once.

1 In the Devices view, select a group.

2 Select **Toner order**.

3 Select the toners for the devices you want to create a flag.

4 Select **Flag** for manual toner orders only.

5 Enter your remarks to associate with the selected toners.

6 Select **Save**.

Editing remarks for toner orders

Users with access authority to devices can edit remarks for toner. You can edit remarks for multiple toners and devices.

1 In the Devices view, select a group.

2 Select **Toner order**.

3 Expand a device by selecting the down arrow.

4 Select the toners to edit for devices.

5 Select **Remarks** > **Edit**.

6 Enter the remarks you want to associate with the toner.

7 Select **Save**.

Deleting remarks for toner orders

Users with access authority to devices can delete remarks for toner listed.

1 In the Devices view, select a group.

2 Select **Toner order**.

3 Expand a device by selecting the down arrow.

4 Select the toner with the remarks you want to remove.

5 Select **Remarks** > **Delete** to delete the remark.

6 Select **OK**.

11 Maps

Maps provide a graphical representation of the location of users and devices within a physical area such as a map of an office. You can view the maps created for a group in the map list.

System Administrators, Managers, Analysts, Service users, and Customers can create a maximum of 100 maps for each group, edit, delete maps, and change the default map for a group. You can select a map as the default map in a group. The first map that you create for a group is automatically set as the default map.

With KFS, you can choose how the map icons are displayed in the map Display settings. You can select **Edit** to change the positions of the map icons, and then select **Save** to save your changes.

Map icons

You can add icons to maps to show where existing devices in the group, users, physical locations, and links are located on the map. In the Maps (Default) view, you can select map icons under Edit in the selected map. You control where map elements are displayed.

You can add descriptions to icons except for MFPs, printers, and links. The Model name, Serial number, and status of MFPs and printers are displayed under their icons.

You can use the following map icons.

Description	Icon
MFP You can search for the available MFP devices in the Search field.	
Printer You can search for the available printers in the Search field.	
Links Use this icon to add a link to other maps from the same device group.	

Description	Icon
Monitor	
Server	
Building	
Male user	
Female user	
Group of users	
Rotate right Use this icon to rotate the map background in a clockwise direction.	
Rotate left Use this icon to rotate the map background in a counter-clockwise direction.	

Description	Icon
Flip horizontal Use this icon to flip the map background image horizontally.	
Flip vertical Use this icon to flip the map background image vertically.	

Creating a map

You can add a map and change how the map icons are displayed. You can add one or more icons on the map.

1. In the Devices view, select the group.
2. In the View drop-down list, select **Maps (Default)**.
3. Select **Upload**.
4. Enter a **Title** (64 character maximum), and a **Description** (256 character maximum).
5. Select **Browse**, and then select the map image file from your computer.
6. Select **Upload**.
7. In the map list, select the name of the map.
8. Select **Edit**.
9. Select **MFP**, and then drag the device to a location in the map.
10. Select **Printer**, and then drag the device to a location in the map.
11. Select **Links**, and then drag the link to a location in the map.
12. For each icon, enter a name after you drag it to the map or double select to add a name for an icon already placed on the map.

    The following map icons are available:

    - Monitor
    - Server
    - Building
    - Male user

- Female user
- Group of users

13 To filter devices in the map, select **Filter**.

14 Enter a **Model name** or **Serial number** and select the search icon.

15 Use the **Transform image** icons to position the map image.

16 Select **Browse** to replace the map image.

17 Select **Save**.

Editing a map

1 In the Devices view, select a group.

2 In the View drop-down list, select **Maps (Default)**.

3 Select a map.

4 Select **Edit**.

5 Select **MFP**, and then drag the device to a location in the map.

6 Select **Printer**, and then drag the device to a location in the map.

7 Select **Links**, and then drag the link to a location in the map.

8 For each icon, you can enter a name for it.

The following map icons are available:

- Monitor
- Server
- Building
- Male user
- Female user
- Group of users

9 To filter devices in the map, select **Filter**.

10 Enter a **Model name** or **Serial number** and select the search icon.

11 Use the **Transform image** icons to position the map image.

12 Select **Browse** to replace the map image.

13 Select **Save**.

Deleting maps

1. In the Devices view, select a group.
2. In the View drop-down list, select **Maps (Default)**.
3. Select one or more maps.
4. Select **Delete**.
5. Select **OK**.

Changing the default map

1. In the Devices view, select a group.
2. In the View drop-down list, select **Maps (Default)**.
3. Select a map.
4. Select **Change default**.
5. Select **OK**.

Refreshing the map list

1. In the Devices view, select a group.
2. In the View drop-down list, select **Maps (Default)**.
3. Select **Refresh**.

Filtering and searching for a map

You can use search filters to display a list of maps by category or use the filters to search for a map.

1. In the Devices view, select a group.
2. In the View drop-down list, select **Maps (Default)**.
3. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following categories use predefined options:

   Last update (Later than), Last update (Recent)

   24 hours, 7 days, 14 days, 30 days

4 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Viewing maps

You can open a map and view the map details. You can view the map image, devices, users, and links to other maps.

1 In the Devices view, select a group.

2 In the View drop-down list, select **Maps (Default)**.

3 Select a map.

4 Scroll up or down to zoom in or zoom out the map.

5 Review the map image, devices, users, group of users, and links on the map.

6 Select the **Model name** of the device in the map to view the Summary page.

Exporting a map as a PDF

1 In the Devices view, select the group.

2 In the View drop-down list, select **Maps (Default)**.

3 Select the map.

4 Select **Download**.

Modifying the map display settings

You can change how the map elements appear in a map from the map display settings.

1 In the Devices view, select a group.

2 In the View drop-down list, select **Maps**.

3 Select the map.

4 Select **Display settings**.

5 In the Type drop-down list, select from the following map icons:

- MFP
- Printer

- Links
- Monitor
- Server
- Building
- Male user
- Female user
- Group of users

6 Select from the available **Display** options. The available display options are dependent on the selected type.

7 Select the **Icon size**.

8 Select **Save**.

12 Device summary

The Device Summary displays device properties information, an image of the device, device logs, with a list of the five most recent events, system errors, counters, and consumables. You can customize device properties. Select **Display settings** and choose the items to display and the order of the items. Customers and Analysts cannot view device logs, counters, and consumables.

To display a large number of consumable levels in the Device summary, select **Other consumable information**.

The Device Summary includes the following device and network properties information:

- Manufacturer and model name
- Device image and options
- Asset number:
  - Select **Edit** to change, enter a new Asset number and then select **Save**.
  - Select **Reset** to clear an existing asset number from the database after the device is restarted.
- Maintenance kit information
- Firmware information: includes all firmware on the device
- Toner information: includes the toner color, level, part number, and the toner serial number
- Status
- Network: IP and MAC address
- Connection status: includes a timestamp for the device connection or disconnection
- Device logs:
  - A table of the five most recent system errors and events
  - Counters: a graph of counters for colors
  - Consumables: a graph of toner levels for supported colors

Reordering the device summary

You can choose and arrange the information displayed on the device summary page.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Display Settings**.
4. Select the information to include or exclude.
   Select the box at the top to choose or clear all items.

5 In the Order column, use the up and down arrows to set the order.

6 Select **Save**.

Viewing, sorting, and filtering device logs

You can view the error, event, and notes log information for a device.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Device logs**.

4 Sort the listing by selecting the column headings: Type, Category, Start time, End time, Color life counter, and Description.

5 In the search Type drop-down list, select a search category, and then enter a search string or select a predefined option. The following items use predefined options:

Type

System error, Event, Note

Start time (Later than), Start time (Recent), End time (Later than), End time (Recent)

24 hours, 7 days, 14 days, 30 days

6 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Adding a note to device logs

System Administrators and Service users can add notes to the list of Device logs. The note is displayed in the Device logs list.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Device logs**.

4 Select **Add note**.

5 In the Add Note dialog, enter a **Category** (64 character maximum), and a **Description** (256 character maximum).

6 Select **Add**.

Viewing graphs of counters and consumables

System Administrators and Service users can view counters and consumables information in a graphical format. When you select both counters and consumables, the Y-Axis (left side) displays counter volume, Y-Axis (right side) displays toner level by percentage, and the X-axis displays the time value.

You can view a maximum of 10 counter types in the graph. The selected counters persist through multiple sessions. Counters and consumables are retrieved on a daily basis.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Device logs** > **Graphs**.
4. To magnify the counters and consumables graph view, scroll anywhere on the graph.

   To reset the view to 100%, select **Zoom to 100%**.
5. To manage counters and consumables in the graph, select or clear check boxes in the Legend.
6. To add counters to the Legend, select **Add counters**, select from the model-dependent options, and then select **Save**.
7. In the Type list, select a type:

   Counters

   The graph displays counters only.

   Consumables

   The graph displays consumables only. Selected counters are not displayed.

   Both counters and consumables

   The graph displays both counters and consumables.

   Early warning (jam)

   The graph displays the jam location.
8. In the Range list, select a time range:
   - All available data
   - Past 12 months
   - Past 6 months
   - Past 3 months
   - Past 30 days
   - Past 7 days

Viewing graphs of early warning jams

System Administrators and Service users can view early warning jam information in a graphical format. The legend provides the 10 fixed locations of jams with the current jam location noted with an icon.

In the graph, the Y-Axis (left side) displays the number of jams, the Y-Axis (right side) displays counters. The X-axis displays the time value of 30 days. Counters are retrieved on a daily basis. The range selection is unavailable.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Device logs** > **Graphs**.
4. In the Type menu, select the **Early warning (jam)**.
5. To manage the display of jam locations for managed devices in the graph, select or clear check boxes in the Legend.

Counters

You can view counters for devices. The counter display varies by device. Counters are updated on a daily basis. To find the most recent update, refer to the timestamp in the Last counter update column in the **Devices** > **Counter (Default)**.

Viewing counters from device properties

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Counters** in the toolbar to view counters supported by the selected device based on Function, Paper size, Duplex, Multiple pages per sheet, Scanned, Life count, Usage, and Other. Black & White, Sum, Full color, Two colors, Single color, Total, and Page count, Level 1, Level 2, and Level 3 are also shown based on the selected device.

Device, network, and registration information in more details

In the More details section, you can view general information about the device, its network connection, registration, and other information.

Device includes Model name, Print speed, and Equipment ID.

Network includes MAC address, Host name, IP address, Network type, Subnet mask, and Default gateway. For multiple network wired and wireless connections, the available IP address, Subnet mask, and Default gateway are displayed for each connection.

Registration includes Registration type, Remote component ID, Management status, and Registration date.

Communication path includes Single point status, Gateway ID, and Single point last update.

Other includes Last update, which is a timestamp for the most recent device update. You can edit Custom fields 1-3, Description, and Location.

Adding an asset number

System Administrators and Managers can add or edit an asset number for a device.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Edit** in the Asset number.
4. Enter an **Asset number** (64 character maximum).
5. Select **Save**.

Edit custom fields

You can specify custom information to display in KFS by editing the Custom fields (there are 3). When device management status is Not registered you cannot edit custom fields, device information is not migrated from other devices, and device registration is not finished.

You can select multiple devices and edit values in the custom fields of the selected devices.

You can update the following fields with this feature:

Custom fields 1 - 3

You can add custom information to each of the three custom fields.

Description

You can enter a description for the selected devices (256 character maximum).

Location

You can enter a location for the selected devices (256 character maximum).

Editing custom fields for multiple devices

You can edit the custom field and apply the changes to selected devices.

1. In the Devices view, select a group.
2. Select one or more devices.

3 Select **Edit custom fields**.

4 Enter descriptions in the available text boxes.

5 Select **Save**.

Panel status

Panel status enables users to view the Panel message and Alerts for remote devices. Panel status requires a connection to devices that are managed and online. It cannot be obtained at the same time as Snapshots, Panel screenshot, Firmware upgrade, Data capture, Panel note, Restart, Send file, Device settings, HyPAS, and Maintenance mode. Multiple users can view Panel status at the same time.

Checking and updating device panel status

You can see the Panel message and Alerts for online devices.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Panel status**.

4 Select **Refresh** to update the panel status.

13 HyPAS applications management

You can manage Hybrid Platform for Advanced Solutions (HyPAS) applications. HyPAS offers both Java-based and web services-based software that provide a more open and flexible platform. HyPAS enables advanced integration with implemented systems. System Administrators can install and uninstall HyPAS applications on a single device or multiple devices, activate and deactivate HyPAS applications on a single device or multiple devices, and view HyPAS Applications task. The device must be online to perform these actions. HyPAS applications can be activated with a key or on a trial basis.

You cannot perform the following tasks on a device when a HyPAS operation is active on the device: Panel Message, Panel Screenshot, Panel Note, Firmware Upgrade, Maintenance Mode, Restart, Snapshots, Send File, and Data Capture.

Installing a HyPAS application

System Administrators and Managers can install a HyPAS application on single and multiple devices. A total of 16 HyPAS applications can be installed on a device.

1. In the Devices view, select a group.
2. Select one or more devices.
3. Select **Tasks** > **Manage HyPAS Applications** > **Install Application**.

   If you selected multiple devices, you can deselect any of those devices in the first screen of the Install Application wizard, then select **Next**.
4. Select **Recent** and select an application in the list of 10 most recently uploaded packages and select **Next**.

   As an alternative, you can select **Upload new package** and select **Browse**, and then select a HyPAS application package.
5. In Schedule, select **Install now** or **Install later (based on local time zone)** which requires the date and time for installing the application.
6. In Retry, select **Enable** and enter values for the Interval (minutes) between 5 and 60 and Number of attempts between 1 and 10.
7. Select **Next**.
8. Enter a **Task name** (64 character maximum), and a **Description** (256 character maximum).
9. Select **Notifications** to receive an email notification about the installation task result, and then select **Next**.
10. Review the Summary, and then select **Install**.

11 Select **Close**.

Activating a HyPAS application

System Administrators and Managers can activate an installed HyPAS application on single and multiple devices. For application activation, the devices must be online.

1 In the Devices view, select a group.

2 Select one or more devices.

3 Select **Tasks** > **Manage HyPAS Applications** > **Activate Application**.

4 Select the application for activation, and then select **Next**.

You can use search for an application with one of the following search filters: Application name, Application version, or Status.

5 To activate an application with a license key provided in a .csv, select **Browse**, find and select the file.

The License keys mapping dialog previews the contents of the .csv. The file should include the device serial number and application license key.

6 Check the data in the .csv preview and select **OK**.

If your file uses a header row, select the check box for **The file has headers**.

If the fields are unaligned, use the drop-down lists to select the columns from the file import that you want to use as Serial number and License key.

7 To activate an application that does not require a License key or offers a trial period, select **Try without a key**.

8 In Schedule, select **Activate now** or **Activate later (based on local time zone)** which requires the date and time for activating the application.

9 In Retry, select **Enable** and enter values for the Interval (minutes) between 5 and 60 and Number of attempts between 1 and 10.

10 Enter a **Task name** (64 character maximum), and a **Description** (256 character maximum).

11 Select **Notifications** to receive an email notification about the activation task result, and then select **Next**.

12 Review the Summary, and then select **Activate**.

13 Select **Close**.

Viewing HyPAS applications on a device

System Administrators and Managers can view a list of installed HyPAS applications on a target device. Check the Last update to see when the list was last refreshed. The device must be online so users can successfully use the HyPAS features.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **HyPAS**.
4. To view the most current HyPAS applications list, select **Refresh**.

Viewing HyPAS application task details

System Administrators and Managers can view the details of a HyPAS application task in the Task Status view.

1. In the Devices view, select **Task Status**.
2. You can view and sort details about all tasks.
3. Select the information icon of a HyPAS application task to view details of the task which includes a link to the device summary page.
4. Review the **Details**, and then select **Close**.

Deactivating a HyPAS application

System Administrators and Managers can deactivate installed HyPAS applications from single and multiple devices. For HyPAS application deactivation, the devices must be online.

1. In the Devices view, select a group.
2. Select the devices.
3. Select **Tasks** > **Manage HyPAS Applications** > **Deactivate Application**, and then select **Next**.

   If you selected multiple devices, you have the option to deselect some or all of the devices in the first screen of the Deactivate Application wizard.
4. Select an application for deactivation, and then select **Next**.

   You can use the Search function to find an application with one of the following search filters: Application name, Application version, or Status.
5. In Schedule, select **Deactivate now** or **Deactivate later (based on local time zone)** which requires the date and time for deactivating the application.
6. In Retry, select **Enable** and enter values for the Interval (minutes) between 5 and 60 and Number of attempts between 1 and 10.
7. Select **Next**.
8. Enter a **Task name** (64 character maximum), and a **Description** (256 character maximum).

9 Select **Notifications** to receive an email notification about the deactivation task result, and then select **Next**.

10 Review the Summary, and then select **Deactivate**.

11 Select **Close**.

Uninstalling a HyPAS application

System Administrators and Managers can uninstall a HyPAS application from single and multiple devices. For removing HyPAS applications, the devices must be online.

1 In the Devices view, select a group.

2 Select the devices.

3 Select **Tasks** > **Manage HyPAS Applications** > **Uninstall Application**.

4 Select an active application to uninstall, and then select **Next**.

You can use search for an application with one of the following Search filters: Application name, Application version, or Status.

5 In Schedule, select **Uninstall now** or **Uninstall later (based on local time zone)** which requires the date and time for uninstalling the application.

6 In Retry, select **Enable** and enter values for the Interval (minutes) between 5 and 60 and Number of attempts between 1 and 10.

7 Select **Next**.

8 Enter a **Task name** (64 character maximum), and a **Description** (256 character maximum).

9 Select **Notifications** to receive an email notification about the uninstallation task result, and then select **Next**.

10 Review the Summary, and then select **Uninstall**.

11 Select **Close**.

14 Task status list

In the Task status list, you can view created tasks. KFS supports a maximum of 10,000 tasks. In the Task status list, you can sort columns by selecting the column name.

Access task details using the task information icon. You can download detailed status or results from this screen, depending on the type of task.

The Task status list includes the following information:

Operation type

The feature for which a task is created.

Task name / Description

The name and description of the task.

Serial number / Model name

The Serial number and the Model name of the target device for the task.

Status / Timestamp

The available status types are Failed, Successful, On hold, Canceled, Processing and Waiting. The timestamp indicates the task start time, end time, or scheduled time.

Created by

The user who created the task.

Information icon

The information icon provides details of the created tasks according to the types of tasks and supports downloading the task status.

Viewing detailed task status

You can view the detailed task status in the Task status list.

1. In the Devices view, select **Task status**.
2. Select the information icon for a task.
   The information varies by the type of task.
3. Select **Close**.

Downloading task status information

You can download and save the task status information for Retrieve snapshots, Maintenance mode, and Device settings from KFS to your computer. The task status information is downloaded in a .zip and opened as .csv or .txt.

1. In the Devices view, select a group.
2. Select **Task status**.
3. Select the information icon for a task.
4. Review the **Details**, and then select **Download results** for Retrieve snapshots and **Download detailed status** for Maintenance mode and Device settings.
5. Select **Close** to return to the Task status list.

Filtering and searching the task status list

1. In the Devices view, select **Task status**.
2. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option.

   Operation type

   Firmware upgrade, Device settings, Maintenance mode, Restart, Retrieve snapshots, Send file, Panel note, Install HyPAS application, Uninstall HyPAS application, Activate HyPAS application, Deactivate HyPAS application, Adjust maintenance actions, Import backup data, Export backup data

   Status

   On hold, Waiting, Processing, Successful, Failed, Canceled

   Timestamp (Later than), Timestamp (Recent)

   24 hours, 7 days, 14 days, 30 days
3. Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Refreshing the task status list

You can refresh the task status list. Only the tasks listed in the table are refreshed.

1. In the Devices view, select **Task status**.
2. Select **Refresh**.

Editing a task

You can edit tasks if the status of the task is failed, canceled, or on hold. Options vary depending on the type of task. HyPAS tasks cannot be edited.

1. In the Devices view, select **Task status**.
2. Select the task, and then select **Edit**.
3. Change the settings for the selected task.
4. Review the Summary, and then apply changes.

Canceling tasks

An on hold task can be canceled by System Administrators, Managers, and Service users. The task is not deleted and the status is changed to canceled.

1. In the Devices view, select **Task status**.
2. Select **On hold** tasks.
3. Select **Cancel**.

Deleting tasks

You can delete one or more tasks you created if the task status is failed, on hold, or successful. Deleted tasks are removed from the task list but are maintained in the database.

1. In the Devices view, select **Task status**.
2. Select the tasks.
3. Select **Delete**.
4. Select **OK**.

15 Snapshots

KFS provides a Snapshots feature for automatic or manual retrieval of status pages, reports, and logs from a device. Snapshots show the current state of a device. KFS stores a total of 100 snapshots per device.

The Snapshots feature also supports Retrieve Settings and Automated Retrieval Settings. You can configure the types of snapshots that are retrieved from the device. Automated Retrieval Settings controls the daily retrieval of snapshots daily, and the types of snapshots to retrieve.

You can retrieve snapshots from multiple devices. You can also view, download, and delete multiple snapshots directly from KFS. Snapshots can be images or text.

Previewing snapshots

You can view the contents of a snapshot. You can only view snapshots with the following file types: .jpg, .png, .gif, .txt, .xml, and .log.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks** > **Snapshots**.
4. Select a snapshot file, and then select the view icon.
5. Select **Close** when finished previewing the snapshot.

Filtering and searching snapshots

You can use search filters to narrow the scope of displayed snapshots.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks** > **Snapshots**.
4. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following categories use predefined options:

   Type

   Status page, Service status page, Network status page, Maintenance report, Application status page, Event log, USB log, FAX report, Image, On-demand USB log, Configuration list

Timestamp (Later than), Recent

24 hours, 7 days, 14 days, 30 days

Method

Manual, Automatic

5 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Retrieving snapshots from a single device

You can obtain snapshots from a device that is directly registered in KFS.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks** > **Snapshots**.

4 Select **Retrieve**.

You can preview the contents of a snapshot file by selecting the icon in the Method column.

Retrieving snapshots from multiple devices

You can retrieve snapshots from two or more devices.

1 In the Devices view, select a group.

2 Select one or more devices.

3 Select **Tasks**, and then select **Retrieve snapshots**.

4 (Optional) You can deselect some of the selected devices in the first screen of the Retrieve Snapshots wizard, then select **Next**.

5 Select the snapshots you want to include, and then select **Next**.

6 In Schedule, select **Retrieve now** or **Retrieve later (based on local time zone)** which requires the date and time for retrieving the snapshot.

7 In Retry, select **Enable** and enter values for the Interval (minutes) between 5 and 60 and Number of attempts between 1 and 10.

8 Enter a **Task name** (64 character maximum), and a **Description** (100 character maximum).

9 Select **Notifications** to receive an email notification about the task result, and then select **Next**.

10 Select **Next**.

11 Review the Summary, and then select **Retrieve**.

12 View the progress of task processing, and then select **Close**.

Retrieving on-demand USB logs

You can retrieve a USB log from a remote device by using snapshots. The device is locked while the log is retrieved.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks** > **Snapshots**.

4 Select **On-demand USB log**.

5 Select **Yes**.

Modifying snapshot retrieval settings

You can modify the settings for retrieving snapshots.

1 In the Devices view, select the group.

2 Select the **Serial number** of a device.

3 Select **Tasks** > **Snapshots** > **Retrieve settings**.

4 Select the logs, reports, and pages you want to include.

5 Select **Save**.

Modifying automated retrieval settings

You can use Automated Retrieval Settings to select the types of snapshots and retrieve them on a daily basis. If you select daily, then all selected snapshots are retrieved at the same time each day which is displayed.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks** > **Snapshots** > **Automated retrieval settings**.

4. Select **Daily** to retrieve snapshots daily.
5. Select logs, reports, and pages for the snapshot.
6. Select **Save**.

Downloading snapshots

You can download snapshots from KFS to your computer.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Task Status**.
4. In the Search drop-down list, select **Operation type**, then select **Retrieve snapshots**, and select the search icon.
5. Select the information icon of a device and snapshot.
6. Select **Download results**.
7. Select **Close**.

Deleting snapshots

You can delete snapshots from KFS.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks** > **Snapshots**.
4. Select a snapshot, and then select **Delete**.
5. Select **OK**.

Uploading snapshots

You can upload one or more snapshots from your computer to KFS. You can only upload snapshots that support the following file types: .zip, .jpg, .gif, .png, .pdf, .doc, .docx, .rtf, .html, .txt, .odt, .ods, and .odp.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.

3 Select **Tasks** > **Snapshots** > **Upload**.

4 Select **Browse**, and then select a file from your computer.

5 Select **Upload**.

You cannot upload a snapshot that exceeds 15 MB.

Editing a snapshot description

You can change the description of a snapshot in KFS.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks** > **Snapshots**.

4 Select a snapshot and select **Edit description**.

5 Change or add a description for the snapshot.

6 Select **Save**.

16 Panel screenshot

Panel screenshot provides KFS users with the capacity to view a remote device panel. At the target device, a request to start the Panel screenshot must be accepted, then a continuous view of the panel is shown in KFS.

Multiple KFS users can view a Panel screenshot. No other KFS functions are available for the device during a Panel screenshot. A short delay occurs between the start of the capture and the display of the first panel image, as well as for all subsequent refreshes.

Using panel screenshot

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Panel screenshot**.
5. Select **Take a panel screenshot**.
6. After the customer confirms the request, you can view the panel of the customer's device.
7. Select **Stop** to end the Panel screenshot function or **Update status** to update it.

Viewing, rejecting, and downloading panel screenshots

You can take a panel screenshot to view the device panel at the customer site. You can also reject and download a panel screenshot.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Panel screenshot**.
5. Select **Take a panel screenshot**.

   You can only view the device panel after the customer confirms your request.
6. Select **Stop** to withdraw the request or reject the panel screenshot.

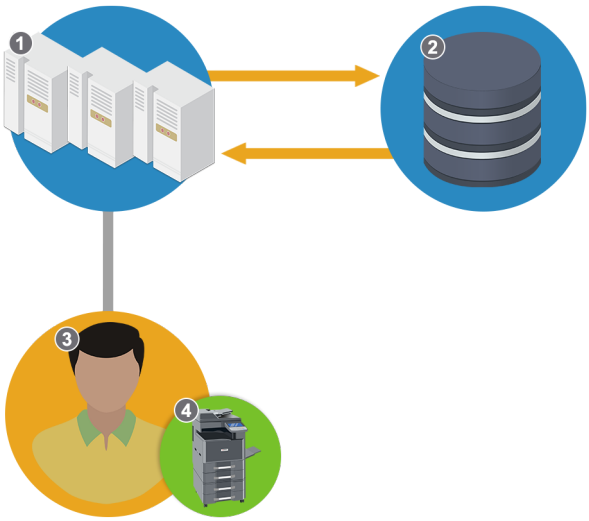
7 Select **Update status** to update a panel screenshot.

8 Select **Save** to download a panel screenshot.

KFS downloads the panel screenshot as a .png.

17 Panel note

Using the Panel note feature, you can post messages on the display panel of a remote device. A panel note contains a title and a message. Panel notes can display various types of information, including device status and support information. You can use this feature to send instructions to the customer or to announce an upcoming visit. Panel notes are supported for devices that are managed and online.



Panel Note	
1 - KFS	2 - Database
3 - Customer	4 - KFS Device

Adding a new panel note

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Panel note**.
5. Select **Add**.
6. Select **Create from** > **New**.

7 In the Title box, enter a panel note title (30 character maximum).

8 In Note, enter a note (256 character maximum).

9 Select the **Save** check box to save it as one of your five preset panel notes.

10 To configure the posting schedule, select **Once** or **On Interval**.

If you select **Once**, you can post a panel note one time.

If you select **On Interval**, you can repeatedly post a panel note at specific time intervals by selecting one of the following:

- 1 minute
- 3 minutes
- 5 minutes
- 10 minutes
- 30 minutes

Select the end date and end time when the panel note posting should stop.

11 In Notifications, select the **Enable** check box, if you want to receive an email notification.

12 In the Email address text box, enter the email address for each user. Separate additional email addresses with semicolons.

13 Select **Send**.

KFS saves the new panel note in Saved notes. A user can save 5 panel notes.

The target device displays the new panel note on the device panel, according to the specified schedule. You cannot post a panel note to offline or unmanaged devices. The device also saves the new panel note in the device history. If the device is restarted, the panel note is displayed again on the device panel.

Posting a new panel note

You can add and display a panel note to the device panel.

1 In the Devices view, select a group.

2 Select a device.

3 Select **Tasks** > **Panel note**.

4 Select **Add**.

5 Select **Create from** > **New**.

6 In the Title box, enter a panel note title (30 character maximum).

7 In Note, enter a note (256 character maximum).

8. Select the **Save** check box to save it as one of your five preset panel notes.
9. To configure the posting schedule, select **Once** or **On Interval**.

   If you select **Once**, you can post a panel note one time.

   If you select **On Interval**, you can repeatedly post a panel note at specific time intervals. Select the interval based on one of the following:

   - 1 minute
   - 3 minutes
   - 5 minutes
   - 10 minutes
   - 30 minutes
   - 1 hour
   - 8 hours

   Select the end date and end time when the panel note posting should stop.
10. Select **Next**.
11. Enter a **Task name** (64 character maximum), and a **Description** (256 character maximum).
12. In Notifications, select the **Enable** check box to receive email notifications.
13. In the Email address text box, enter the email address for each user. Separate additional email addresses with semicolons.
14. Select **Send**.

The target device displays the selected panel note on the device panel, according to the specified schedule. You cannot post a panel note to offline or unmanaged devices. The device saves the panel note in the device history. If the device is restarted, the panel note displays again on the device panel.

Posting saved and shared panel notes

You can select a saved or shared panel note and display it on a device panel.

1. In the Devices view, select a group.
2. Select a device.
3. Select **Tasks** > **Panel note**.
4. Select **Create from**.
5. Select one of the following:

   Saved notes

   You can post one of the 5 latest panel notes that you have saved to KFS Manager. Each user can save a total of 5 panel notes.

Shared notes

You can post a panel note that is shared by other users within the group or shared as a system.

6 Select the down arrow in Select note, and then select a panel note.

7 In the Title box, enter a panel note title (30 character maximum).

8 In Note, enter a note (256 character maximum).

9 Select the **Save** check box to save it as one of your five preset panel notes.

10 In Send, configure the posting schedule, select **Once** or **On Interval**.

If you select **Once**, you can post a panel note one time.

If you select **On Interval**, you can repeatedly post a panel note at specific time intervals. Select the interval based on one of the following settings:

- **1 minute**
- **3 minutes**
- **5 minutes**
- **10 minutes**
- **30 minutes**
- **1 hour**
- **8 hours**

Select the end date and end time when the panel note posting should stop.

11 In Notifications, select the **Enable** check box to receive email notifications.

12 Enter the email address for each user. Separate additional email addresses with semicolons.

13 Review the Summary, and then select **Send** to send the file immediately.

The target device displays the selected panel note on the device panel, according to the specified schedule. You cannot post a panel note to offline or unmanaged devices. The device saves the panel note in the device history. If the device is restarted, the panel note displays again on the device panel.

Saved notes and shared notes

Saved notes are the panel notes that you have saved in KFS. Each user can save a maximum of 5 panel notes. You can select, edit, and post a panel note from Saved notes to the device panel.

Shared notes are the panel notes shared with other users within the group. You can select, edit, and post a panel note from Shared notes to the device panel. You can also copy and save a panel note from Shared notes to Saved notes.

Sharing panel notes

You can share panel notes with other users and save a shared panel note in your own list for further editing and use.

Sharing a panel note as Groups lets any user who belongs to the current group, or any child groups under the current group, access the panel note. Sharing a panel note as System lets all KFS users access the panel note. No other users can access a panel note that is saved as Private.

Adding a shared panel note to saved notes

You can add a shared panel note to your own list of panel notes in KFS.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Panel note**.
5. Select **Add**.
6. In the Create from box, select **Shared notes**.
7. In Select note, select the panel note.

   You can edit the Title and the Note of the selected panel note.
8. In the Title box, enter a Panel note title (30 character maximum).
9. In Note, enter a Note (256 character maximum).
10. Select the **Save** check box to save it as one of your five preset panel notes.
11. Select the **Notifications** check box to receive email notifications.
12. In the Email address text box, enter the email address for each user. Separate additional email addresses with semicolons.
13. Select **Send**.

KFS saves the panel note from Shared notes to Saved notes.

Managing a panel note

You can edit or delete a panel note in Manage Notes.

1. In the Devices view, select a group.

2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Panel note**.
5. Select **Manage notes**.
6. Select **Saved notes**, and then select a panel note.
7. Select **Edit**.
8. In the Title box, enter a panel note title (30 character maximum).
9. In the Note box, enter a message (256 character maximum).
10. In Share, select one of the following settings:

    Private

    No other users can access the panel note.

    Groups

    Any user who belongs to the current group, or any child groups under the current group, can access the panel note.

    System

    All users can access the panel note.

11. Select **Save**.

In Manage Notes, you can select and delete panel notes.

Removing a panel note from the device panel

You can remove the last panel note sent to the device.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Panel note**.
5. Select **Remove** to remove the displayed panel note.

KFS removes the panel note from the device panel. The removed panel note is saved in KFS.

The customer can also remove the panel note at the device panel by selecting **Close**. KFS does not track panel notes removed by the customer.

If the device is restarted, a panel note removed by KFS does not display on the device panel while a panel note removed by the customer is displayed again.

18 Data capture

With Data capture, System Administrators, Managers, and Service users can obtain printable data from a registered device. You must request permission at the device panel before data capture can start. You can view the details of the captured data, cancel an ongoing data capture task, download a copy of the captured data, or delete captured data from KFS. The data capture list displays the following information:

File name

The file name of the printable data.

Timestamp

The date and time when the data capture is performed.

Created by

The name of the user requesting the data capture.

Size

The file size of the printable data.

Truncated

The data capture is truncated because the 15 MB limit has been exceeded. Any data captured after 15 MB is discarded. Ten printable files can be saved per device for 1 to 7 days after the capture date.

Filtering and searching captured data

You can use search filters to display a list of captured data by category or use the filters to search for captured data.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Data capture**.
5. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option. The following uses predefined options:

   Timestamp (Later than), Timestamp (Recent)

   24 hours, 7 days, 14 days, 30 days

Select x in the Search box to clear the search value and restore the view to the original list.

Capturing device data

You can capture printable data by working on the device panel and in KFS.

1. In the Devices view, select the group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Data capture**.
5. Select **Start**.
6. On the device panel, press **Accept** to the request for the data capture.
7. On the computer, print the file.
8. At the device panel, press **Accept** to send the data file to KFS in .zip format.
   When you open the compressed file, the data capture file type is .capt. It can be viewed in a text editor or sent to developers for further investigation.

To stop data capture, select **Cancel** in KFS. The data capture can be accepted or rejected on the device panel.

Downloading captured data

You can download captured data to your computer. Once downloaded, extract the file and view it in a text editor.

1. In the Devices view, select the group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Data capture**.
5. Select the captured data, and then select **Download**.
6. (Optional) Select the check box to **Delete the files from KFS?**
   If the check box is clear, the .capt file type is saved in KFS.
7. Select **OK**.

Deleting data captures

You can delete one or more printable data file from KFS.

1. In the Devices view, select the group.

2 Select the **Serial number** of a device.

3 Select **Tasks**.

4 Select **More** > **Data capture**.

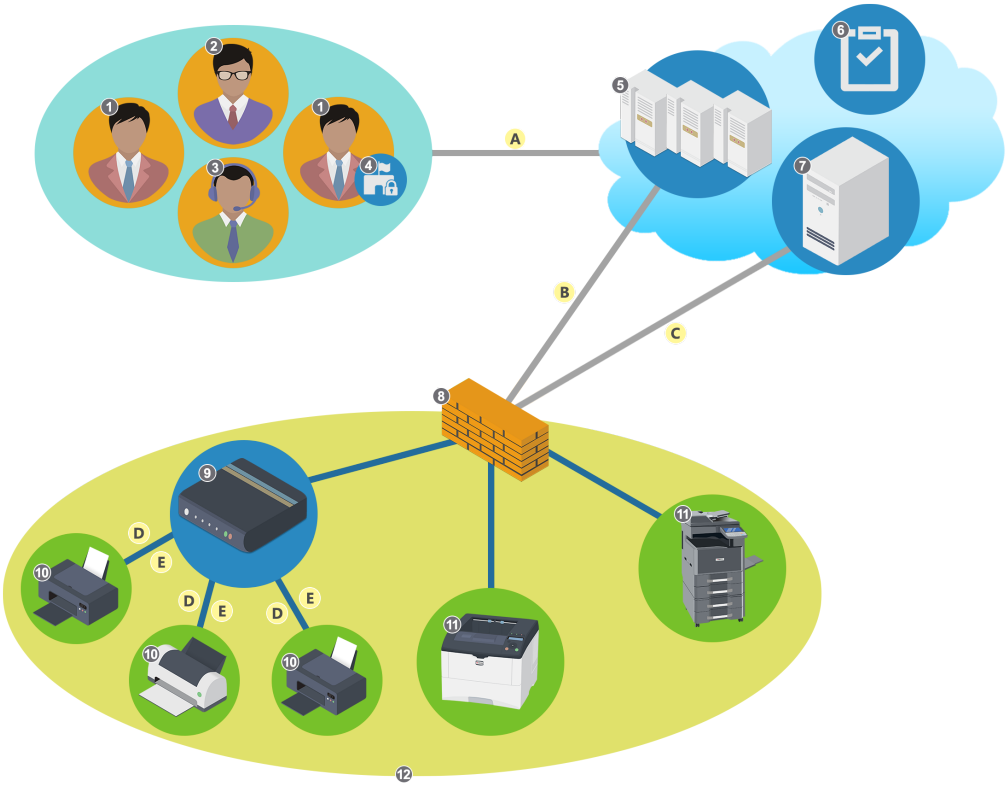
5 Select one or more data files.

6 Select **Delete**.

7 Select **OK**.

19 Firmware upgrade

System Administrators, Managers, and Service users can upgrade all firmware for a device. Firmware can be upgraded for single or multiple devices at the same time. If more than one device is selected for upgrade, the devices must belong to the same model group. Firmware upgrades can be performed immediately or scheduled for a later time. You can check the firmware version of all the devices in a group. You can also check if the firmware package has a signed certificate.



Firmware Upgrade Overview	
1 - Manager	2 - System Administrator
3 - Service	4 - RHQ Permissions
5 - KFS	6 - Firmware File Repository
7 - XMPP Server	8 - Firewall
9 - NetGateway	10 - Device from outside vendor
11 - KFS Device	12 - Small/Medium/Large office

A. User selects the firmware package for a KFS device in the KFS UI. Communication with KFS is secured through HTTPS.
B. KFS uses the XMPP protocol for communication and sends the firmware upgrade command to NetGateway or Device.
C. The NetGateway or device downloads the firmware package via HTTPS.
D. The NetGateway sends the firmware upgrade command to devices.
E. The device downloads the firmware package from the NetGateway and upgrades the firmware.

Upgrading firmware

You can upgrade the firmware of one or more devices of the same model.

1. In the Devices view, select a group.
2. Select the devices. You can select multiple devices of the same model.
3. Select **Tasks** > **Firmware upgrade**.
4. If you selected multiple models, select the models you want to upgrade and select **Next**.

   Some devices may have known issues with their installed firmware versions. Devices with these known issues should be restarted before performing the upgrade.
5. Select a firmware package.

   If you select a model with custom firmware, select **Show other types of packages** to display all available packages for the model.
6. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option.

   The following items use predefined options:

   Release type

   Official, Custom, Long-term test, Short-term test, Evaluation

   Released (Recent), Released (Later than)

   7 days, 30 days, 3 months, 6 months
7. When a package contains a Readme, select the **I have read the upgrade Readme** box.
8. Select **Next**.
9. If the selected device uses custom firmware, select **OK** to overwrite the custom firmware.
10. In Schedule, select **Upgrade now** or **Upgrade later** (based on local time zone), which requires the date and time of the scheduled upgrade.
11. In Retry, select **Enable** and enter values for the Interval (minutes) from 5 to 60 and Number of attempts from 1 to 10.

12 Enter a **Task name** (64 character maximum), and a **Description** (256 character maximum).

13 Select **Notifications** to receive an email notification about the results of the restart task, and then select **Next**.

14 Review the Summary, and then select **Close** for a scheduled upgrade, or select **Upgrade** to run the upgrade immediately.

15 The firmware package will overwrite the existing firmware.

20 Device restart

With Device restart, you can restart multiple devices or network components remotely. You can restart a device, or a network component immediately or on a set schedule. You cannot restart a device that is offline.

You can also view a list of restart tasks by selecting Task status in the Devices view. From the list of tasks, you can edit, cancel, delete, and check the details of a task or refresh the list of tasks. You can only edit a device restart task if the task status is failed, canceled, or on hold. You can search the Task Status list based on the operation type.

Creating a restart task

To remotely restart a device, you must first create a restart task. You can restart multiple devices or network components.

1. In the Devices view, select the group.
2. Select the devices.
3. Select **Tasks** > **Restart**.
4. In Type, select **Device** or **Network**.
5. In Schedule, select **Restart now** or **Restart later (based on local time zone)** which requires the date and time for restarting the device.
6. In Retry, select **Enable** and type values for the Interval (minutes) between 5 and 60 and Number of attempts between 1 and 10.
7. Select **Next**.
8. Type a **Task name** (64 character maximum), and a **Description** (256 character maximum).
9. Select **Notifications** to receive an email notification about the task, and then select **Next**.
10. Review the Summary, and then select **Close** if the task is scheduled or select **Restart** to restart the device immediately.

21 Maintenance mode

Using Maintenance mode, you can manage devices that are directly registered in KFS. With this feature, you can create or update maintenance mode configurations and apply them to a device or devices in the same model group. You can also edit, delete, and share maintenance mode configurations.

You can use two types of maintenance mode configurations:

Actions

Maintenance mode configurations that can have additional settings.

Settings

Maintenance mode configurations that can have varying setting combinations.

Viewing maintenance mode configurations

You can view the maintenance mode configurations that you saved for a device. You cannot view the configurations created by other users. The configurations displayed are specific to the logged in user, and are not specific to any device.

1. In the Devices view, select the group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Maintenance mode** > **Saved configurations**.

Creating a maintenance mode configuration with actions

You can create a maintenance mode configuration with selected actions that you can later apply to one or more devices in the same model group.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Maintenance mode** > **Saved configurations**, and then select **Add**.
5. Select **Actions**, and then select **Next**.
6. Select the target model, and then select **Next**.

7. Type a configuration name (100 character maximum).

   If you create a configuration using a name of an existing configuration created by another user, an error is shown.

8. Select a category and one or more actions, and then select **Next**.

9. Select an action, edit the properties, and then select **Next**.

10. Review the Summary, and then select **Save**.

    You can view the maintenance mode configuration that you created in saved configurations.

Creating a maintenance mode configuration with settings (source device)

You can create a maintenance mode configuration with selected settings through the source device settings.

1. In the Devices view, select a group.

2. Select the **Serial number** of a device.

3. Select **Tasks**.

4. Select **Maintenance mode** > **Saved configurations**, and then select **Add**.

5. Select **Settings**, and then select **Next**.

6. Select **Source device**.

7. Select the group, and then select a device within that group.

8. Select **Next**.

9. Enter a configuration name (100 character maximum).

   If you create a configuration using a name of an existing configuration created by another user, an error is shown.

10. Select a category and one or more settings, and then select **Next**.

11. Select one or more settings, edit the properties, and then select **Next**.

12. Review the Summary, and then select **Save**.

    You can view the maintenance mode configuration you created in Saved configurations.

Creating a maintenance mode configuration with settings (target models)

You can create a maintenance mode configuration with selected settings through the target models settings.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Maintenance mode** > **Saved configurations**, and then select **Add**.
5. Select **Settings**, and then select **Next**.
6. Select **Target models**, and then select a device.
7. Select **Next**.
8. Type a configuration name (100 character maximum).

   If you create a configuration using a name of an existing configuration created by another user, an error is shown.
9. Select a category and one or more settings, and then select **Next**.
10. Select one or more settings, edit the properties, and then select **Next**.
11. Review the Summary, and then select **Save**.

    You can view the maintenance mode configuration that you created in Saved configurations.

Retrieving maintenance mode configurations from a device

You can obtain the maintenance mode configurations from a registered device.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Maintenance mode** > **Recent configurations** > **Retrieve**.

KFS displays current configurations.

Adding shared configurations to saved configurations

You can add multiple shared configurations to Saved configurations.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Maintenance mode** > **Shared configurations**.
5. Select one or more configurations.
6. Select **Add to Saved configurations**.
7. Select **Close**.

The selected shared configurations are added to Saved configurations.

Editing maintenance mode configurations

You can make changes to maintenance mode configurations.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Maintenance mode** > **Saved configurations**.
5. Select a configuration, and then select **Edit**.
6. Make the changes available for configuration.
7. Select **Next**.
8. Review the Summary, and then select **Save**.
   You can view the edited configuration in Saved configurations.

Applying a maintenance mode configuration

You can apply a maintenance mode configuration to a device immediately or schedule it later.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Maintenance mode** > **Recent configurations** > **New**.

5. Select one of the following: Actions, Settings, Saved configurations, or Shared configuration, select one or more actions for the configuration, and then select **Next**.
6. Select the configuration values, and then select **Next**.

   You may have to restart the device or network interface to apply changed settings.
7. Select **OK** to restart your device after the task is performed.

   To abort the task, select **Cancel**.
8. In Schedule, select **Apply now** or **Apply later (based on local time zone)**, which requires the date and time of the scheduled maintenance.
9. In Retry, select **Enable** and type values for the Interval (minutes) between 5 and 60 and Number of attempts between 1 and 10.
10. Select **Next**.
11. Enter a **Task name** (64 character maximum), and a **Description** (256 character maximum).
12. Select **Notifications** to receive an email notification about the task, and then select **Next**.
13. Review the Summary, and then select **Close** for a scheduled task or **Apply** to run the task immediately.

Deleting a maintenance mode configuration

You can delete one or more maintenance mode configurations listed in Saved configurations.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Maintenance mode** > **Saved configurations**.
5. Select the configuration, and then select **Delete**.
6. Select **OK**.

Sharing a maintenance mode configuration

You can share a maintenance mode configuration with other users by groups or system.

1. In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks**.

4 Select **Maintenance mode** > **Saved configurations**.

5 Select a configuration.

6 Select **Sharing settings**.

7 Select from **Groups** or **System**.

8 Select **Apply**.

Creating a private maintenance mode configuration

You can set the maintenance mode configuration to private for your personal use.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks**.

4 Select **Maintenance mode** > **Saved configurations**.

5 Select a configuration.

6 Select **Sharing settings**.

7 Select **Private**.

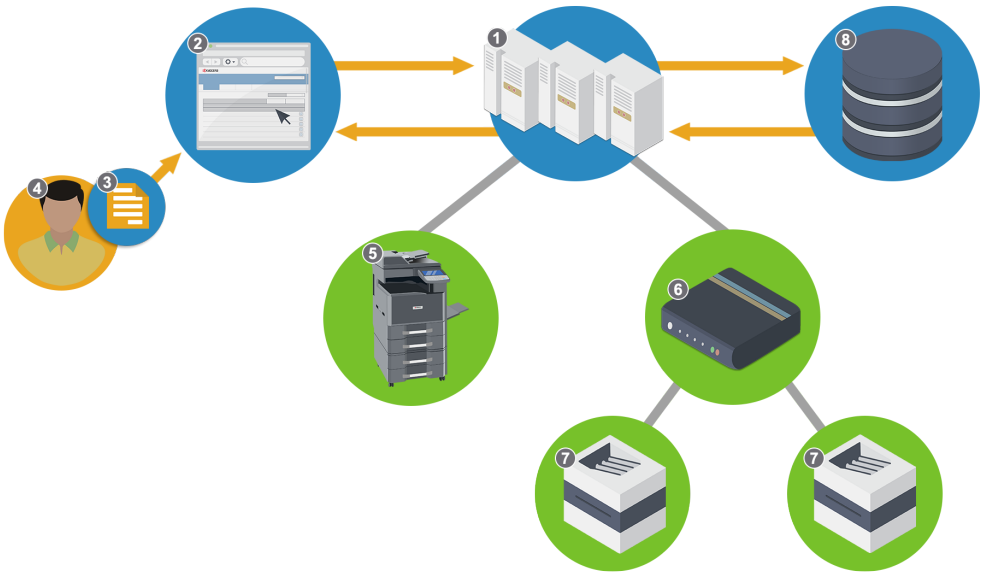
8 Select **Apply**.

22 Send file

The Send file feature lets System Administrators and Service users upload printable files and command files to KFS then download them to remote, registered devices. You can schedule when to send the file or send it immediately. You can store a maximum of 10 files and the maximum file size cannot exceed 15 MB. Depending on the size of the file, it may take a few minutes for the task to finish. The task will timeout if it does not finish within 3 minutes.

This troubleshooting feature enables users to send test files to remote devices. At first, you must upload the printable files to KFS before sending the printable files to a device. Command files using PRESCRIBE can configure target devices.

If you receive a message that you have reached the maximum of 10 stored files, you can access the Send File list, remove files to go under the limit, then retry the Send file task again. You can upload one file at a time.



Send File	
1 - KFS	2 - UI (KFS)
3 - File	4 - Customer
5 - KFS device	6 - NetGateway
7 - Legacy device	8 - Database

Sending files to remote devices

With the Send file task, you can upload a file, or select stored send files, send a file to a remote registered device in real time or at a scheduled time. If you upload a file, KFS timestamps the file using the time from your computer.

1. In the Devices view, select a group.
2. Select a device.
3. Select **Tasks**.
4. Select **Send file**.
5. Select one of the following:

   New

   Browse a new file on your computer. Select **Browse**, select the file, and then select **Next**.

   Recent

   Select a file from recently uploaded files.

   Shared

   Select a file from shared files.
6. For Recent or Shared, select the file in the list, and select **Next**.
7. In Schedule, select **Send now** or **Send later (based on local time zone)** which requires the date and time for sending the file.
8. In Retry, select **Enable** and enter values for the Interval (minutes) between 5 and 60 minutes and Number of attempts between 1 and 10.
9. Select **Next**.
10. Enter a **Task name** (64 character maximum), and a **Description** (256 character maximum).
11. Select **Notifications** to receive an email notification about the task.
12. Select **Next**.
13. Review the Summary, and then select **Close** for a scheduled task or select **Send** to send the file immediately.

    If the file was sent immediately, you must select **Close** to close the status view. The progress of the task is not interrupted when you close.

If you receive a message that the limit of saved printable files has been reached, you can access the Send file list, remove one or more stored files, then retry the Send file task again.

Viewing uploaded files

1. In the **Devices** view, select a group.
2. Select a device.
3. Select **Tasks**.
4. Select **Send file**.
5. Select **Recent files** or **Shared files.**

Send file progress status

You can check the status and result of file transmissions. When executing a Send file task, the target device status must be online or ready. If the target device has any other active task, the task status is set to Waiting. If the selected device does not support the Send file feature, you cannot create a task.

In Send now, the task progress status information includes the following:

- Serial number
- Model name
- Customer ID
- Customer name
- Status
- Progress
- Detailed status

In Send later (based on local time zone), you can check the task progress status information in the Tasks searchable menu by providing the task name.

Sharing settings

You can share printable files between registered groups. Access Sharing settings via Recent files, where all the files you currently created are displayed. You can select one or multiple files and change the sharing setting for the files that are selected.

Users can set the sharing settings based on the following user roles:

System Administrator

Private, System, Group

Manager

Private, Group

Other Roles

Private

Applying sharing settings

You can set and apply sharing settings to the files that are previously uploaded in KFS. The default sharing setting is Private.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks** > **More** > **Send file**.
4. Select **Recent files**.
5. Select one or more files, and then select **Sharing settings**.
6. Select one of the following options:

   Private

   This setting does not allow other users to view the files.

   Groups

   This setting allows all users in the current user's group and all the users in the child groups of the current user's group to access the files.

   System

   This setting allows all users to access the files. They display as Shared files to other users.
7. Select **Apply**.

Sharing printable files

You can share printable files between groups. System Administrators can configure sharing settings as Private, System, or Groups. Managers can configure sharing settings as Private or Groups. When the printable files are changed to Private, they are no longer shared.

Downloading printable files

You can download printable files from KFS to your computer. Multiple printable files can be downloaded at the same time. Files are downloaded with a name that uses 'filename-unix timestamp.file extension'. The filename of the downloaded file may not match the original filename.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.

4 Select **More** > **Send file**.

5 Select **Recent files** or **Shared files**.

Recent files

Files you have uploaded.

Shared files

Files uploaded by you and others.

6 Select one or more files, and then select **Download** to save the files to your computer.

7 Select **Save**.

Deleting uploaded files

You can delete uploaded files in KFS. For this Send file feature, you can delete multiple files.

1 In the Devices view, select the group.

2 Select the **Serial number** of a device.

3 Select **Tasks**.

4 Select **More** > **Send file**.

5 Select the uploaded files to delete.

6 Select **Delete**.

7 Select **OK**.

Filtering and searching uploaded files

You can filter and search files that have been uploaded to KFS. These uploaded files are associated with the Send file feature.

1 In the Devices view, select the group.

2 Select the **Serial number** of a device.

3 Select **Tasks**.

4 Select **More** > **Send file**.

5 Select **Recent files** or **Shared files**.

6 In the Search drop-down list, select a search category, and then type a search string or select a predefined option. The following items use predefined options:

Uploaded date (Older), Uploaded date (Recent)

24 hours, 7 days, 14 days, 30 days

Sharing

Private, Groups, System

7 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

23 Remote panel

Remote Panel provides Administrator and Service users with the ability to perform maintenance functions on remote, online devices. A confirmation request sent to the device panel must be accepted for the operation to start. The Remote Panel session uses Virtual Network Computing (VNC) to manage the remote operation and prevent most other KFS functions while the session is active.

The Remote panel session can be stopped at any time at the device panel.

System Administrators can view Remote Panel access activity in Audit logs.

The confirmation request timeout value is 5 minutes. When a timeout occurs, the confirmation message closes on the device panel and a pop-up UI message reports that the request was not accepted within the allotted time. Remote Panel sessions do not display in the Task list.

The Remote Panel function must be enabled and supported for the online and ready device. Users are granted access authority when Tasks (Remote Panel) is enabled in User permissions.

Remote panel execution logs are stored in the respective Delegated group. The logs contain the group and group path, a timestamp, email address and the user name and email of the executor, the duration of the operation, and the serial and asset number of the device. The logs are maintained for one year. If the group is deleted, the logs are deleted as well.

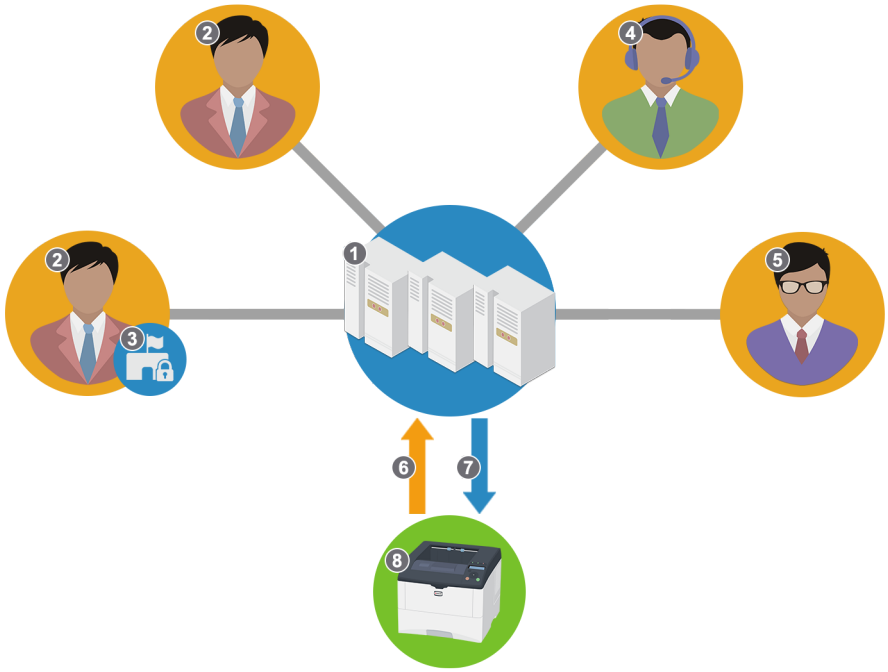
Starting a remote panel session

You can perform a Remote panel session with a supported, online device.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **More** > **Remote panel**.
5. Select **Start remote panel**.
6. Perform KFS functions with access to the remote panel.
7. Select **Stop remote panel** when finished.

24 Device Settings

The Device Settings feature allows System Administrators and Service users to retrieve device settings, create device configurations, and upload and download configurations. You can modify settings for a device, and execute device settings changes immediately or at a later time. You can view the most recent settings for an online device.



Device Settings	
1 - KFS	2 - Manager
3 - RHQ Permissions	4 - Service
5 - System Administrator	6 - Retrieve (Receive)
7 - Set (Send)	8 - KFS Device

Creating device settings

You can create device settings configurations from scratch for a selected device model group. A setting can only be applied to multiple devices if they are the same model.

1 In the Devices view, select a group.

2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Device settings** > **New**.
5. Select **Current configuration**.
   You can create new settings for Default settings, Network settings, or System settings.
6. Choose available settings. Select **Next**.
7. Select a configuration. Add values and information for each configuration.
8. After setting all of the configurations, select **Next**.
9. In Schedule, select **Apply now** or **Apply later (based on local time zone)**, which requires the date and time of the scheduled change.
10. In Retry, select **Enable** and enter values for the Interval (minutes) between 5 and 60 minutes and Number of attempts between 1 and 10.
11. Select **Next**.
12. Enter a **Task name** (64 character maximum) and a **Description** (100 character maximum).
13. Select **Notifications** to receive an email notification about the task, and then select **Next**.
14. Review the Summary, and then select **Close** for a scheduled task or **Apply** to run the task immediately.

Editing a specific device configuration

You can edit the device settings configuration for a specific device.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Device settings** > **Recent configurations**.
5. Select **Retrieve**.
6. Select **Edit** to a device settings configuration.
7. Make changes to the device settings, and then select **Next**.

8. In Schedule, select **Apply now** or **Apply later (based on local time zone)**, which requires the date and time of the scheduled change.
9. Type a **Task name** (64 character maximum) and a **Description** (100 character maximum).
10. Select **Notifications** to receive an email notification about the task, and then select **Next**.
11. Review the Summary, and then select **Apply**.

Deleting saved device configurations

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Device settings** > **Saved configurations**.
5. Select the configuration, and then select **Delete**.
6. Select **OK**.

Sharing a device settings configuration with the system

A System Administrator can share a saved device settings configuration with the entire system.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Device settings**.
5. On the Device settings page, select **Saved configurations**.
6. Select the **Device settings** configuration to share.
7. Select **Sharing settings**.
8. Select **System**, and then select **Apply**.

Sharing a device settings configuration with a group

Managers can share a saved device settings configuration with their group. System Administrators can share a saved device settings configuration and make it available to every user in the child group.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Device settings**.
5. Select **Saved configurations**.
6. Select the **Device settings** configuration to share.
7. Select **Sharing settings**.
8. Select **Groups**, and then select **Apply**.

Adding a device configuration for a single device

If you are a System Administrator, Manager, or Service user, you can create a maximum of ten saved configurations.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Device settings** > **Saved configurations**, and then select **Add**.
5. Select **Source device**.
6. In the Group column, select a group, then select the devices in the Online Devices column.

   You can find and display devices using the following options:

   a) To find a group in a large list of groups, select **Search** in the Group column, type a search term, then use the up and down arrows to move between instances of the search term in the hierarchical structure. The number of occurrences of the search term is displayed as well.
   b) To find a device among many in the Online Devices column, type a search value in the Search box, select the search icon, and select devices.

c) Use the **Device ID** gear icon in the Online Devices column to select a category to sort the list of devices: Serial number, Host name, IPv4 address, MAC address.

7 Select **Next**.

8 Type a **Name** for the configuration (100 character maximum).

9 Select the settings you want included in the configuration, and then select **Next**.

10 Select the Configuration in the drop-down list, edit the properties, and then select **Next**.

11 Review the Summary, and then select **Save**.

Adding a device configuration for target models

If you are a System Administrator, Manager, or Service user, you can create a configuration for a model group. You can save a maximum of ten configurations.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks**.

4 Select **Device settings** > **Saved configurations**, and then select **Add**.

5 Select **Target models**.

6 Select the model name in the list, and then select **Next**.

You can use the Search box to find a specific model. Type a model name, and then select the search icon.

7 Type a **Name** for the configuration (100 character maximum).

8 Select the settings you want included in the configuration, and then select **Next**.

9 Select the **Configuration**, edit the properties, and then select **Next**.

10 Review the Summary, and then select **Save**.

Downloading saved or shared configurations

System Administrators, Managers, and Service users can download single or multiple saved or shared configurations in XML format.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks**.

4 Select **Device settings**.

5 Select **Saved configurations** or **Shared configurations**.

6 Select the settings you want to download, and then select **Download**. KFS downloads the settings in .xml format.

Viewing recent configurations

In the Device Settings view, you can view the recent configurations of a device, if any are available.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks**.

4 Select **Device settings**.

5 Select **Retrieve**. If no recent configurations are available, this selection retrieves the current device configuration.

Modifying sharing settings

When you create a saved configuration, it is set to private by default. You can share saved configurations with groups or system-wide by modifying Sharing settings.

1 In the Devices view, select a group.

2 Select the **Serial number** of a device.

3 Select **Tasks**.

4 Select **Device settings**.

5 On the Device settings page, select **Saved configurations**.

6 Select a configuration.

7 Select **Sharing settings**.

8 In the Sharing Settings dialog, change from **Private** to **Groups** or **System** and then select **Apply**.

Modifying a saved configuration

If you are a System Administrator, Manager, or Service user, you can edit saved configurations.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Device settings**.
5. Select **Saved configurations**.
6. Choose a configuration, and then select **Edit**.
7. Select the settings you want included in the configuration.
   Use Search to find specific settings to change, and then select **Next**.
8. Select a **Configuration**, edit the properties, repeat for other configuration selections, and then select **Next**.
9. Review the Summary, and then select **Save**.

Uploading device settings configuration

If you are a System Administrator, Manager, or Service user, you can upload a device settings configuration by uploading a .xml or .zip file with the configuration settings in MSTE format.

1. In the Devices view, select a group.
2. Select the **Serial number** of a device.
3. Select **Tasks**.
4. Select **Device settings**.
5. Select **Saved configurations**.
6. Select **Upload**.
7. Enter a unique name for the configuration (100 character maximum).
8. Choose the device model from the drop-down list.
9. Browse to the configuration file, and then select **Upload**.

25 Backup data

The KFS Backup data task supports import and export of user-selected data types for a select group of KFS devices. System Administrators, Managers, and Service users who can save and access the import and export backup data on their computers can perform this on-demand task. The backup data cannot be stored in KFS. Some data types are constrained. For example, if you clear the Fax Forward data type, constraints cause Program and Panel Setting to be cleared. Some imports initiate a device restart.

Before an export is performed, a user must accept a backup request that has been sent to the device panel.

Import and export results can be found in the Audit logs.

Backup data can also be accessed from selecting the **Serial number** of a device, selecting **Tasks** and then **More** > **Import backup data** or **Export backup data**.

Importing backup data

You can import various data types from backup data. The import will overwrite existing data on the device.

1. In the Devices view, select a group.
2. Select a device.
3. Select **Tasks**.
4. Select **More** > **Import backup data**.
5. Select **Browse** and select a data file in a .zip format. Data types are stored in the data file.
6. Select the data types. Make sure the selected types match those in the imported data file.
7. Select **Next**.
8. Type a **Task name** and an optional **Description**.
9. Review the Summary, and then select **Import**.
10. Select **View detailed results** to download the results.
11. Select **Close**.

Exporting backup data

You can export various data types to backup data. The export is encrypted and password protected. It can be used to replace data in another device.

1. In the **Devices** view, select a group.
2. Select a device.
3. Select **Tasks**.
4. Select **More** > **Export backup data**.
5. Select the data types you want to export.
6. Select **Next**.
7. Type a **Task name** and an optional **Description**.
8. Select **Next**.
9. Review the Summary, and then select **Export**.
10. On the device panel, select **Confirm the request on the display panel**.
11. To download the backup data after the export finishes, select **Download exported data**. This download is the only method for saving the Export backup data.

You can select **Cancel** to close the confirmation request and cancel the operation.

26 Notifications

KFS can send notifications to users when specific events occur on managed devices or gateways. For example, you can create notifications for a system event, toner level alerts, page count thresholds, toner remaining days, Maintenance kit or other consumable level alerts. The type of device and the selected notification template govern the format and the information included in a notification. If you do not recognize the notification event type, refer to the service guide for the specific device.

Notifications can also be configured to report NetGateway inactivity. For example, if KFS receives no Gateway updates (notification type) within a selected number of days (3 to 100), then the No update alert (Gateway) notification is sent. For this notification type, you can permit the notification to send multiple alerts.

Notifications provide the option to notify you when the event occurs (starts), the event is cleared (ends), or after the event both starts and ends. For example, if you select "starts for an Offline event", you will receive a notification when the device goes offline.

For the error Notification type, you can choose notifications based on each occurrence or for repetitive occurrences. Notifications criteria supports a repeat counter (Alert repetition threshold) for device alerts. You have control of notification frequency for errors or events based within a range of an hour, day, or month. A similar feature for Toner level alerts controls the limit of toner level alerts with a range of 1 to 30 days.

For the Other consumable level alert Notification type, you can choose thresholds for the consumable level as well as add and remove consumables from the criteria.

The Notification template includes the content and format for the email notification.

Notifications can be sent to both the logged-in user and to specific email recipients. Notifications include a summary link.

If a change occurs for a selected group, gateway, target device, or user that affects Notifications criteria, then the status changes from Enable or Disable to a Warning. If your access level changes, none of the Notifications criteria you created will be accessible. You cannot change the status to Enable.

KFS maintains notifications history for 60 days.

Notifications history

With notifications history you can view and manage the notifications that you receive from monitored devices and gateways. Your role as a recipient is defined in the notifications criteria where a user or email address has been added to the notification.

Viewing details of notifications history

1 In the Devices view, select **Notifications** > **History**.

2 Select the information icon for the notification. The notification details display the following information:

Notification type

Notification type

Subtype

Shows the notification subtype, if available.

Device or Gateway

Shows device information and the group associated with the device You can select on the hyperlinked model name to open the Device Summary. If the notification type is gateway related, then it shows gateway information with no hyperlink.

Recipient

Shows the notification recipients

Name

Shows the name of the notification criteria

Timestamp

Shows the date and time when the notification was received

Message

Shows the message sent in the notification

3 Select **Close**.

Filtering and searching notifications history

You can use search filters to narrow the scope of displayed notifications.

1 In the Devices view, select **Notifications** > **History**.

2 Select a group.

3 In the Search drop-down list, select a search category, and then type a search string or select a predefined option.

The following items use predefined options:

Read/Unread

Read, Unread

Priority level

High, Medium, Low, Clear

Notification type

Page count, Event, Toner level alert, Maintenance kit level alert, Toner remaining days, No update alert (Device), No update alert (Gateway), Other consumable level alert

Event

System error, Paper jam, Toner low, Toner empty, Time for maintenance, Unknown toner installed, Waste toner box full, Waste toner box almost full, MK change, Toner change, Staple error, Punch error, Storage memory error, Other error, Offline, Condition-based maintenance alert

Toner level alert. Toner remaining days

Black, Cyan, Magenta, Yellow

Page count

Copier total, Copier black & white, Copier color total, Printer total, Printer black & white, Printer color total, FAX total, FAX black & white, FAX color total, Other total, Other black & white, Other color total, Combined total, Black & white total, Color total, A3 total, B4 total, A4 total, B5 total, A5 total, Folio total, Ledger total, Legal total, Letter total, Statement total, Banner 1 total, Banner 2 total, Other 1 total, Other 2 total, Large total, Single-sided total, Duplex total, Large (duplex) total, Double select total, 1 in 1 total, 2 in 1 total, 4 in 1 total, Copier scan total, Copier scan black & white, Copier scan color total, FAX scan total, FAX scan black & white, FAX scan color total, Other scan total, Other scan black & white, Other scan color total, Scan total, Scan black & white, Scan color total, Life count total, Color life count total

Maintenance kit level alert

Maintenance kit A - E, Cassette 1 - 7, MP Tray, Document Processor, Z-Fold unit, Inserter 1, Inserter 2

Received (Later than), Received (Recent)

24 hours, 7 days, 14 days, 30 days

Other consumable level alert

Other, Unknown, Waste toner, Ink ribbon, Waste ink, OPC, Developer, Fuser oil, Solid wax, Ribbon wax, Waste wax, Fuser, Corona wire, Fuser oil wick, Cleaner unit, Fuser cleaning pad, Transfer unit, Fuser oiler, Water, Waste water, Glue water additive, Waste paper, Binding supply, Banding supply, Stitching wire, Shrink wrap, Paper wrap, Staples, Inserts, Covers

4 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Marking notifications as read or unread

You can change the read or unread status of notifications.

1. In the Devices view, select **Notifications** > **History**.
2. Select the group.
3. Select one or more notifications.
4. Select **Mark notifications**, and then select **Read** or **Unread**.

Setting the priority level for notifications

You can change the priority level of one or more notifications.

1. In the Devices view, select **Notifications** > **History**.
2. Select the group.
3. Select one or more notifications.
4. Select **Set priority**, and then select **High**, **Medium**, **Low**, or **Clear**.
   You can also set the priority level by selecting the flag icon for the one or more notifications.
5. Select **Clear** to remove the priority level from one or more notifications.

Deleting notifications history

You can delete notifications.

1. In the Devices view, select **Notifications** > **History**.
2. Select a group.
3. Select one or more notifications, and then select **Delete**.
4. Select **OK**.

Notifications criteria

You can configure notifications for yourself or others from a gateway, a device or a group of devices and configure options for selected notification types. Managers with access to notification criteria can view, edit, delete or change the status of users' notification criteria.

You can edit or delete the notification criteria that you create. You can also enable or disable notification criteria. The status of notification criteria automatically becomes a warning if any of the following actions occur to a user, in a device or group:

Device move

A device with notification criteria is moved to a different group which a user cannot access.

Device deletion

A device with notification criteria is deleted.

Gateway archive

A gateway with notification criteria is archived.

Gateway deletion

A gateway with notification criteria is deleted.

Group deletion

A group with notification criteria is deleted.

KFS user move

A user who created the notification criteria is moved to a different group.

Group move

A group with notification criteria is moved to a different group, or a device with notification criteria belongs to a group that is moved to a different group.

Delegated group move

A delegated group with notification criteria is moved to a different group, or a device with notification criteria belongs to a delegated group that is moved to a different group.

Access Authority change

The access authority of the user who created the notification criteria is changed.

Device Status change

The status of a device with notification criteria is changed to Archived or Unmanaged.

Viewing notifications criteria details

1. In the Devices view, select **Notifications** > **Criteria**.
2. Select a group.
3. Select the information icon of a notifications criteria.

Name

Shows the name of the notification criteria.

Template name

Shows the template name.

Notification type

Shows the details of the notifications criteria type.

Source

Shows group, gateway, or device information. For groups, it shows the available groups. For devices, it shows device information and the group associated with the device. You can select a hyperlinked model name to open the Device Summary. There is no hyperlink for a Gateway source.

Recipients

Shows the email addresses of the notification recipients.

Send to group's email address

Shows whether the notification was sent to the group email address.

Send as bcc

Shows whether blind carbon copy was sent.

Created by

Shows the user who created the criteria.

Last update

Shows the date and time of the last notifications criteria update.

Updated by

Shows the user who updated the notifications criteria.

Status

Shows the status of the notifications criteria including details about warning.

4 Select **Close**.

Filtering and searching notifications criteria

1 In the Devices view, select **Notifications** > **Criteria**.

2 Select a group.

3 In the Search drop-down list, select a search category, and then type a search string or select a predefined option.

The following items use predefined options:

Status:

Enabled, Disabled, Warning

Notification type

Page count, Event, Toner level alert, Maintenance kit level alert, Toner remaining days, No update alert (Device), No update alert (Gateway), Other consumable level alert

Event

System error, Paper jam, Toner low, Toner empty, Time for maintenance, Unknown toner installed, Waste toner box full, Waste toner box almost full, MK change, Toner change, Staple error, Punch error, Storage memory error, Other error, Offline, Condition-based maintenance alert

Toner level alert, Toner remaining days

Black, Cyan, Magenta, Yellow

Page count

Copier total, Copier black & white, Copier color total, Printer total, Printer black & white, Printer color total, FAX total, FAX black & white, FAX color total, Other total, Other black & white, Other color total, Combined total, Black & White total, Color total, A3 total, B4 total, A4 total, B5 total, A5 total, Folio total, Ledger total, Legal total, Letter total, Statement total, Banner 1 total, Banner 2 total, Other 1 total, Other 2 total, Large total, Single-sided total, Duplex total, Large (duplex) total, Double select total, 1 in 1 total, 2 in 1 total, 4 in 1 total, Copier scan total, Copier scan black & white, Copier scan color total, FAX scan total, FAX scan black & white, FAX scan color total, Other scan total, Other scan black & white, Other scan color total, Scan total, Scan black & white, Scan color total, Life count total, Color life count total

Maintenance kit level alert

Maintenance kit A - E, Cassette 1 - 7, MP Tray, Document Processor, Z-Fold unit, Inserter 1, Inserter 2

Source

Devices, Groups, Gateways

Last update (Later than), Last update (Recent)

24 hours, 7 days, 14 days, 30 days

Other consumable level alert

Other, Unknown, Waste toner, Ink ribbon, Waste ink, OPC, Developer, Fuser oil, Solid wax, Ribbon wax, Waste wax, Fuser, Corona wire, Fuser oil wick, Cleaner unit, Fuser cleaning pad, Transfer unit, Fuser oiler, Water, Waste water, Glue water additive, Waste paper, Binding supply, Banding supply, Stitching wire, Shrink wrap, Paper wrap, Staples, Inserts, Covers

4 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Creating notifications criteria for devices

You can create notifications criteria that you can apply to specific devices.

1. In the Devices view, select **Notifications** > **Criteria**.
2. Select **Add**.
3. Enter a **Name** for the notification criteria (64 character maximum).
4. Select a **Notification type**:

Event

You can specify notifications based on an event type and the event trigger. You can select one or more events as well as one-time notifications or notifications for event repetitions. The Alert repetition threshold selection establishes the frequency and number of alerts that you receive for chosen events.

Toner level alert

You can set the toner level value that triggers the notification. You can select one or more color toners. To manage the level of redundant toner notifications, select **Prevent multiple alerts** to set the frequency of toner alerts based on values of 1 to 30 days.

Page count

You can specify a counter type and page count value that triggers the notification. You can select one or more counter types.

Maintenance kit level alert

You can create notifications for Maintenance kit and Cassette levels. You can also add or remove selections from the list.

Toner remaining days

You can create toner notifications based on the number of days left. Four color toners are supported. To manage the level of redundant toner notifications, select **Prevent multiple alerts** to set the frequency of toner alerts based on values of 1 to 30 days.

No update alert (Device)

This selection establishes notifications when KFS has not received data from registered devices. The last update field is refreshed for each device when data is received. To create a notification threshold, enter a value based on the number of days without device updates. The range is 3 to 100 days. After you create the notification criteria, the first notification is suppressed if the device data has not been updated for 30 days plus x days where x equals the value you enter in the text box.

No update alert (Gateway)

This selection establishes notifications when Gateway data has not been updated during a specified period. The last update field is refreshed when data is received. To create a notification threshold, enter a value based on the number of days without gateway updates. The range is 3 to 100 days. Select **Allow multiple alerts** to bypass the KFS default that prohibits continuous notification sending until Gateway data is obtained again and date/time information of “Last update” is updated. See Creating notifications criteria for gateways.

Other consumable level alert

This selection lets you create notifications for general consumables based on threshold levels. You can select a variety of thresholds for multiple consumable types within one Notification Criteria. Use the plus and minus icons to add or remove consumable types from the notification.

5 Select **Next**.

6 For Source, select **Devices**.

You can select devices within a group. You can select multiple devices.

7 In the Group column, select a group, then select the devices in the Device column.

You can find and display devices using the following options:

- To find a device among many in the Device column, enter a search value in the Search box, select the search icon, and select the devices
- Use the **Device ID** gear icon in the Device column to choose how devices are displayed in the list: Serial number, Host name, IPv4 address, MAC address

8 Select **Next**.

9 Enter the name of an existing notification template in the Search text box and press **Enter** or select one from the following Template source:

All templates

You can view and select a notification template from all available.

Private

You can view and select a notification template that you created as private in a group.

Share

You can view and select a notification template that is shared in your delegated group.

System share

You can view and select a shared template created by System Administrators. You can also select a default notification template.

As an alternative template selection method, select **New template**.

a) Select a Method by choosing **Create a new template** or **Copy from an existing template**.

   New templates are created as Private templates.

b) Both methods require a Template name and you can create an optional Description.

c) For the copy method, you must select a **Template source** then a **Template**.

d) Both methods lead into the Add Notification Template wizard.

10 For any template in the list, select the **Edit** icon to edit a Notification template through Edit Notification Template wizard.

   You can also delete any template in the list. Select the **Delete** icon to remove the template then select **OK**.

11 Select **Next**.

12 Select **Me** to receive the notification as well as display your email address in the notification.

13 For System Administrators and Managers:

a) Select **Add users** to add other users.

b) Select **Email search**, enter the complete email address of a user, and then select the **Search** icon.

c) Select a group from which to add users.

   You can use the search text box to find users.

d) Select any other users in the list.

   You can also select **Clear all** or **Select all**.

e) Select **Add**.

14 For Analysts, Customers, and Service users:

a) Select **Add users**.

b) Enter the email address of a user and then select the **Search** icon.

   If found in the application, the user is added to the list.

c) To include additional users, go through the steps again.

15 Select **Send to group's email address** to send notifications to the email associated with the group.

16 Select **Send information-only emails** to users outside KFS or without access to the group. The email content will not contain links. Enter the email address for each user. Additional email addresses should be separated by a semicolon.

17 Select **Send as bcc** to hide the email addresses of all recipients in the notification email.

18 Select **Next**.

19 Review the Summary, and then select **Finish**.

Creating notifications criteria for groups

You can create notifications criteria that you can apply to all devices in groups.

1. In the Devices view, select **Notifications** > **Criteria**.
2. Select **Add**.
3. Enter a **Name** for the notification criteria (64 character maximum).
4. Select a **Notification type**:

Event

You can specify notifications based on an event type and the event trigger. You can select one or more events as well as one-time notifications or notifications for event repetitions. The Alert repetition threshold selection establishes the frequency and number of alerts that you receive for selected events.

Toner level alert

You can set the toner level value that triggers the notification. You can select one or more color toners. To manage the level of redundant toner notifications, select the **Prevent multiple alerts** check box to set the frequency of toner alerts based on values of 1 to 30 days.

Page count

You can specify a counter type and page count value that triggers the notification. You can select one or more counter types.

Maintenance kit level alert

You can create notifications for Maintenance kit and Cassette levels. You can also add or remove selections from the list.

Toner remaining days

You can create toner notifications based on the number of days left. Four color toners are supported. To manage the level of redundant toner notifications, select **Prevent multiple alerts** to set the frequency of toner alerts based on values of 1 to 30 days.

No update alert (Device)

This selection establishes notifications when KFS has not received data from registered devices. The last update field is refreshed for each device when data is received. To create a notification threshold, enter a value based on the number of days without device updates. The range is 3 to 100 days. After you create the notification criteria, the first notification is suppressed if the device data has not been updated for 30 days plus x days where x equals the value you enter in the text box.

No update alert (Gateway)

This selection establishes notifications when Gateway data has not been updated during a specified period. The last update field is refreshed

when data is received. To create a notification threshold, enter a value based on the number of days without gateway updates. The range is 3 to 100 days. Select Allow multiple alerts to bypass the KFS default that prohibits continuous notification sending until Gateway data is obtained again and date/time information of “Last update” is updated.

Other consumable level alert

This selection lets you create notifications for general consumables based on threshold levels. You can select a variety of thresholds for multiple consumable types within one Notification Criteria. Use the plus and minus icons to add or remove consumable types from the notification.

5 Select **Next**.

6 For Source, select **Groups**. This selects all the devices in the selected groups. You can select multiple groups.

7 In Quick select, you can select groups based on the following options:

All accessible

All child groups and the delegated groups under them.

Exclusively managed

All child groups but not delegated groups under them.

Off

No filter for the group.

8 In Search, enter a group name then use the up and down arrows to move between instances of the search term in the hierarchical structure. The number of occurrences of the search term is displayed as well.

9 Select **Next**.

10 Enter the name of an existing notification template in the Search text box and press **Enter** or select one from the following Template source:

All templates

You can view and select a notification template from all available.

Private

You can view and select a notification template that you created as private in a group.

Share

You can view and select a notification template that is shared in your delegated group.

System share

You can view and select a shared template created by System Administrators. You can also select a default notification template.

As an alternative template selection method, select **New template**.

a) Select a Method by choosing **Create a new template** or **Copy from an existing template**.

   New templates are created as Private templates.

b) Both methods require a Template name and you can create an optional Description.

c) For the copy method, you must select a **Template source** then a **Template**.

d) Both methods lead into the Add Notification Template wizard.

11 For any template in the list, you can select the **Edit** icon to edit a Notification template using the Edit Notification Template wizard. You can also delete any template in the list. Select the **Delete** icon to remove the template then press **OK**.

If the notification type is Other consumable level alert, only Default template (Consumables) can be selected.

12 Select **Next**.

13 Select **Me** to receive the notification as well as display your email address in the notification.

For Analysts, Customers, and Service users:

a) Select **Add users**, enter the email address of a user, then select the **Search** icon.

   If found, the user is added to the list. To include additional users, go through the steps again.

For System Administrators and Managers:

a) Select **Add users** to choose other users.

b) Select a group from which to add users.

   You can use the search text box to find users.

c) Select **Email search** and enter the email address of a user, then select the **Search** icon.

d) Select any other users in the list.

   You can also select **Clear all** or **Select all**.

e) Select **Add**.

14 Select **Send to group's email address** to send notifications to the email associated with the group.

15 Select **Send information-only emails** to users outside KFS or without access to the group. The email content will not contain links. Enter the email address for each user. Additional email addresses should be separated by a semicolon.

16 Select **Send as bcc** to hide the email addresses of all recipients in the notification email.

17 Select **Next**.

18 Review the Summary, and then select **Finish**.

Creating notification criteria for gateways

1. In the Devices view, select **Notifications** > **Criteria**.
2. Select **Add**.
3. Enter a **Name** for the notification criteria (64 character maximum).
4. For Notification type, select **No update alert (Gateway)**.
5. For the notification threshold, enter a value based on the number of days without gateway updates. The range is 3 to 100 days.
6. Select **Allow multiple alerts** to bypass the KFS default that prohibits continuous notification sending until Gateway data is obtained again.
7. Select **Next**.
8. For Source, select **Gateways**.
9. In the Group column, select a group, then select one or more gateways in the Gateway column.

   You can find and display groups and gateways using the following options:

   To find a group in a large list of groups, select **Search** in the Group column, enter a search term, then use the up and down arrows to navigate within the hierarchical structure. The number of occurrences of the search term is displayed as well.

   To find gateway in the Gateway column, enter a search value in the Search box, select the search icon, and select the gateway.

   Use the **ID** gear icon in the Gateway column to choose how the gateways are displayed in the list. Select Gateway ID, Host name, or IPv4 address.
10. Select **Next**.
11. Select **Default template (for Gateway)**.
12. Select **Next**.
13. Select **Me** to receive the notification as well as display your email address in the notification.

    For Analysts, Customers, and Service users:

    a) Select **Add users**, enter the email address of a user, then select the **Search** icon.

       If found, the user is added to the list. To include additional users, go through the steps again.

    For System Administrators and Managers:

    a) Select **Add users** to choose other users.
    b) Select a group from which to add users.

You can use the search text box to find users.

c) Select **Email search** and enter the email address of a user, then select the **Search** icon.

d) Select any other users in the list.

You can also select **Clear all** or **Select all**.

e) Select **Add**.

14 Select **Send information-only emails** to users outside KFS or without access to the group.

The email content will not contain links. Enter the email address for each user. Additional email addresses should be separated by a semicolon.

15 Select **Send report only if there are results** to eliminate receipt of no result reports.

16 Select **Send as bcc** to hide the email addresses of all recipients in the notification email.

17 Select **Next**.

18 Review the Summary, and then select **Finish**.

Editing notifications criteria

You can edit the settings in the Notifications criteria that you created.

1 In the Devices view, select **Notifications** > **Criteria**.

2 In the View by menu, select a group or **Private**.

The View by menu is displayed only for System Administrators and Managers.

3 Select a Notifications criteria, and then select **Edit**.

4 You can modify any of the following items:

- **Name**
- **Notification type**
- **Source**
- **Template source**
- **Template**
- **Recipients**

5 Review the Summary, and then select **Finish**.

Deleting notifications criteria

1 In the Devices view, select **Notifications** > **Criteria**.

2 In the View by menu, select a group or **Private**.

The View by menu is displayed only for System Administrators and Managers.

3 Select a notifications criteria.

4 Select **Delete**.

5 Select **OK**.

Changing the status of notifications criteria

1 In the Devices view, select **Notifications** > **Criteria**.

2 In the View by menu, select a group or **Private**.
The View by menu is displayed only for System Administrators and Managers.

3 Select the notifications criteria.

4 Select **Change Status**, and then select **Enable** or **Disable**.

Notification templates

Using Notification templates you can specify the contents and layout of notifications received from a device. You can create a notification template to customize the information that you receive, and then save the template as a personal template. You can edit, copy, or delete the notification templates you created.

Manager, Service users, and Analysts can share notification template with users who belong to their groups. Manager, Service users and Analysts can edit, copy, or delete notification templates shared with a delegated group which they belong to. Additionally, Managers can share notification templates with other delegated groups for which they have access authority. Managers can edit, copy, or delete notification templates in those groups. System Administrators can edit, copy, or delete any notification template in the system. A notification template that is being used in one or more notifications criteria cannot be deleted. The use of the template in a Notifications Criteria is called a Reference.

System Administrators, Manager, Service users, Analysts, and Customers cannot use the same existing template name that they created. Any user can use an existing template name created by another user.

System Administrators can view all notification templates in the system. Other users can view notification templates shared to the delegated groups they belong to.

Viewing notifications template details

You can view the details of a notifications template.

1 In the Devices view, select **Notifications** > **Manage templates**.

2. In the View by menu, select the group, **System share**, or **Private** based upon your permissions and your role.
3. Select a group.
4. Select the information icon for a notifications template. The notifications template details display the following information:

   Template name
   Shows the template name.

   Description
   Shows the description of the template.

   Subject
   Shows the subject of the template.

   Message
   Shows the details of the notifications template.

   Share
   Shows the sharing setting of the template with other groups and the system.

   Created by
   Shows the user who created the template.

   Last update
   Shows the date and time of the last template update.

   Updated by
   Shows the user who updated the template.

   Reference
   Shows how many Notifications Criteria use the template.
5. Select **Close**.

Filtering and searching for notifications templates

You can use search and filter Notifications templates in KFS.

1. In the Devices view, select **Notifications** > **Manage templates**.
2. Select the group.
3. In the Search drop-down list, select a search category, and then type a search string or select a predefined option.
   The following items use predefined options:

Share

Private, Share, System share

Last update (Later than), Last update (Recent)

24 hours, 7 days, 14 days, 30 days

4 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Creating a notifications template

You can create and customize a notifications template.

1 In the Devices view, select **Notifications** > **Manage templates**.

2 Select **Add**.

3 Enter a **Template name** (64 character maximum), and a **Description** (256 character maximum).

4 To share a Notification template, select **Share template**.

a) For System Administrators, select **Share to system** or **Share to group**.

b) For Managers, select **Share with own group** or **Share with other group**.

Service users and Analysts can share to the delegated group they belong to.

Share template is not available to Customers.

5 Select **Next**.

6 In Email contents, place the cursor in the **Subject** or **Body** text box.

7 Select a parameter or link from the drop-down list below the Body text box, and then select the up arrow button to add it to the Subject or Body of the notification template.

You can enter a description and add the parameter or link in the Body to ensure the content is easier to understand.

8 Select a Mail format:

HTML

Email notification in .html format.

Plain text

Email notification in plain text format.

9 Select **Next**.

10 Review the Summary, and then select **Finish**.

As a security measure, users are prevented from adding some .html tags when **HTML** is selected as the Mail format.

Editing notification templates

You can edit the contents of the notifications templates that you created.

1 In the Devices view, select **Notifications** > **Manage templates**.

2 In the View by menu, select the group, **System share**, or **Private** based upon your permissions and your role.

3 Select a template, and then select **Edit**.

4 You can edit the following options:

- Template name
- Description
- Email contents
- Mail format

5 Select **Next**.

6 Review the Summary, and then select **Finish**.

Copying a notification template

You can use the Copy Notification Template wizard to create a new notification template.

1 In the Devices view, select **Notifications** > **Manage templates**.

2 In the View by menu, select the group, **System share**, or **Private** based upon your permissions and your user role.

3 Select a template, and then select **Copy**.

4 You can edit the following options:

- Template name
- Description
- Share template
- Email contents
- Mail format

5 Select **Next**.

6 Review the Summary, and then select **Finish**.

Deleting notifications templates

You can delete one or more notification templates that you created.

1. In the Devices view, select **Notifications** > **Manage templates**.
2. In the View by menu, select a group, **System share**, or **Private** based upon your permissions and your role.
3. Select one or more notification templates.
4. Select **Delete**.
5. Select **OK**.

27 Dashboard

You can use the Dashboard feature to view analysis information of devices registered to a group. You can view the usage in the customer environment. Using the Dashboard you can view the devices with issues and toner reports for devices.

The following Dashboard analysis information is available:

Print volume: You can view print volume reports.

- Monthly print volume
- Device usage
- B&W vs color/ Function / 3 tier color (copy) / 3 tier color (printer)
- Top 10 devices (last month)
- Inactive devices (under 200 pages) (last month)

Scan volume: You can view scan volume reports.

- Scan volume trend
- Scan volume ratio
- Scan volume
- Scan volume top 10 devices (last month)

Jams: You can view paper jam reports.

- Last x months jams, top 5 models
- Last 6 months jams trend
- Last x months jams, top 10 devices

System errors: You can view system error reports.

- Last x months system errors, top 5 models
- Last x months system errors, top 10 error codes
- Last x months system errors, top 10 devices

Viewing scanner volume statistics

You can view scanner usage statistics of devices from the Scan volume view.

1. In the Devices view, select **Dashboard**.
2. On the Dashboard page, select **Scan volume**.

In the Scan volume view, you can view the following scanner usage reports:

- Scan volume trend
- Scan volume ratio
- Scan volume
- Scan volume top 10 devices (last month)

Viewing system errors statistics

You can view system errors statistics of devices from the System errors view.

1. In the Devices view, select **Dashboard**.
2. On the Dashboard page, select **System errors**.

In the System errors view, you can view the following:

- Last x months system errors, top 5 models - 1 month, 3 months, or 6 months
- Last x months system errors, top 10 error codes
- Last x months system errors, top 10 devices

Viewing paper jam statistics

1. In the Devices view, select **Dashboard**.
2. On the Dashboard page, select **Jams**.

In the Jams view, you can view the following:

- Last x months jams, top 5 models - 1 month, 3 months, or 6 months
- Last 6 months jams trend
- Last x months jams, top 10 devices

To see additional information about jams in a device, select **More details**.

Viewing print volume statistics

You can view printer usage statistics of devices from the Print volume view.

1. In the Devices view, select **Dashboard**.
2. On the Dashboard page, select **Print volume**.

In the Monthly print volume graph, you can view the following print volume reports:

- B&W vs color
- Function
- 3 tier color (copy)
- 3 tier color (printer)

In the Device usage graph, the following viewing options are available:

- MFP/printer
- Manufacturer

In the Print volume view, you can also view the following printer usage reports:

- Top 10 devices (last month)
- Inactive devices (under 200 pages) (last month)

28 Graphical reports

With Graphical reports, you can generate visual reports that contain information about selected devices or groups, and then send the reports to specified recipients. There are four types of reports: Meter reading, consumables management, preventive maintenance, and usage analysis. You can configure the graphical reports to be generated and sent to the recipients at a scheduled time or immediately. Producing some graphical reports can be time-consuming based on the volume of data selected for the report. For this reason, graphical report scheduling identifies default and recommended file formats based on the selected report. Further, when graphics are in a select graphical report schedule, then the .csv file format is unavailable.

Graphical Reports History

Using Graphical reports history you can manage generated reports. You can prioritize, delete, download, and refresh generated graphical reports. You must create a graphical reports schedule before you can generate, send or download graphical reports. Reports are maintained for 60 days.

Graphical Reports Schedule

In Graphical reports schedule, you can create, edit, and delete schedules, generate reports and enable/disable status. Schedules specify the file type and paper size of the graphical reports you want to generate. You must create a graphical reports schedule before you can generate and send graphical reports. You can also specify from which devices or groups to retrieve the report data, and within which date range you want to retrieve the information. You can also set the delivery frequency of the graphical reports.

The settings for a graphical reports schedule include the following:

- Template
- File formats: .pdf, .docx, .xlsx, .pptx, .csv
- Output size: A4, Letter
- Source: Groups, Devices
- Report Range
- Frequency
- Recipients

Graphical Reports Templates

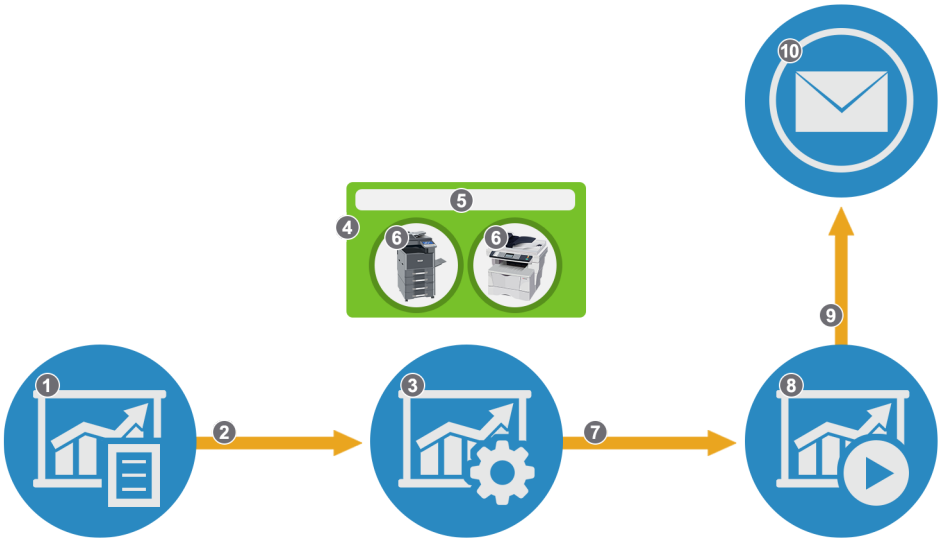
Graphical Reports Templates include 19 predefined report templates. To build Graphical reports, you specify a report template in the graphical reports schedule. You cannot edit templates. You can view the details of a template by selecting the information icon of the template.

You can choose from the following 19 report templates:

Print Color Usage	Model Counts

Copy Color Usage	Manufacturer Counts
Page Volume by Manufacturer	Devices Under 200 Page Volume
Top Page Volume Changes	Group Summary
Top 10 Problem Devices	Days Until Empty
Toner Replacement History	Current Toner Levels
Inactive Devices	Counter Reports
Paper Jam Count	B&W vs Color Print Volume (Total)
New Devices	B&W vs Color Print Volume (by Month)
New Group	

You can change the priority levels of graphical reports.



Graphical Reports	
1 - Graphical Report Template	2 - Used
3 - Graphical Report Schedule	4 - Reporting Targets
5 - Group 1	6 - Devices
7 - Created	8 - Generated Graphical Report
9 - Send	10 - Mailbox (Outside the System)

Viewing the details of a graphical report

You can view graphical report details.

1 In the Devices view, select **Graphical reports**.

2 Select **History**.

3 In the Graphical reports list, select the information icon of the list reports to view the following details:

- Report name
- Name
- Source (can include multiple groups or devices)
- Output size
- File format
- Size
- Recipient
- Generated time
- Created by

4 Select **Close**.

Filtering and searching for graphical reports

1 In the Devices view, select **Graphical reports**.

2 In the Search drop-down list, select a search category, and then type a search string or select a predefined option. The following items use predefined options:

Priority level

High, Medium, Low, Clear

File format

.pdf, .docx, .xlsx, .pptx, .csv

Generated (Later than), Generated (Recent)

24 hours, 7 days, 14 days, 30 days

3 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Setting the graphical reports priority level

1 In the Devices view, select **Graphical reports**.

2 Select the graphical reports.

3 Select **Priority level**.

4 Select a priority level. You can also set the priority level of the graphical reports by selecting the flag icon for the report. The following options are available:

- High (Red)

- Medium (Blue)
- Low (Green)
- Clear (Gray)

Generating graphical reports

1. In the Devices view, select **Graphical reports**.
2. Select **Schedule**.
3. In the View by menu, select the group or **Private**.
   Private is only available to System Administrators and Managers.
4. Select the graphical report schedule.
5. Select **Generate report**.

The email address of the reports scheduler is included in the reports sent to the target user.

Downloading graphical reports

You can download graphical reports from KFS. Graphical reports support the following file types: .pdf, .docx, .xlsx, .pptx, .csv. The reports are downloaded as a .zip.

1. In the Devices view, select **Graphical reports**.
2. Select **History**.
3. Select the graphical reports.
4. Select **Download**.

Deleting graphical reports

1. In the Devices view, select **Graphical reports**.
2. Select **History**.
3. Select the graphical reports.
4. Select **Delete**.
5. Select **OK**.

Enabling or disabling the status of graphical report schedules

You can change the status of the graphical report schedules. The new status changes the status icon for the selected graphical report schedules.

1. In the Devices view, select **Graphical reports**.
2. Select **Schedule**.
3. In the View by menu, select a group or **Private**.
4. Select a graphical report schedule.
5. Select **Change status**.
6. Select **Enable** or **Disable**.

Filtering and searching for graphical report schedules

1. In the Devices view, select **Graphical reports**.
2. Select **Schedule**.
3. In the Search drop-down list, select a search category, and then type a search string or select a predefined option.

   The following items use predefined options:

   Status
   Enabled, Disabled, Warning

   Source
   Devices, Groups

   Last run time (Later than), Last run time (Recent)
   24 hours, 7 days, 14 days, 30 days

   Schedule results
   Successful, Failed, On hold, Processing

   Next run time (Earlier than), Next run time (Later than)
   24 hours, 7 days, 14 days, 30 days
4. Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Viewing the details of a graphical report schedule

1. In the Devices view, select **Graphical reports**.
2. Select **Schedule**.
3. In the View by menu, select the group or **Private**.
4. In the list, select the information icon of a report schedule to display the following information:
   - Name
   - Template
   - Report name
   - File format
   - Output size
   - Source
   - Option
   - Recipients
   - Report range
   - Frequency
   - Last run (result/time)
   - Next scheduled report
   - Created by
   - Last update
   - Updated by
   - Status
5. Select **Close**.

Creating a graphical report schedule for devices

You can create a graphical report schedule for devices to generate and send graphical reports.

1. In the Devices view, select **Graphical reports**.
2. Select **Schedule**.
3. In the View by menu, select a group or **Private**. The View by menu is displayed only for System Administrators and Managers.
4. Select **Add**.
5. Enter a **Name** for the graphical report schedule (64 character maximum).
6. Select a **Template name** (graphical report template). You can enter text in the Search box to find a template.

7 Enter a **Report name** (64 character maximum).

8 Select a **File format** for the graphical report: .pdf, .docx, .xlsx, .pptx, .csv.

Producing some graphical reports can be time-consuming based on the volume of data selected for the report. For this reason, graphical report scheduling identifies default and recommended file formats based on the selected report. Further, when graphics are in a select graphical report schedule, then the .csv file format is unavailable.

9 Select an **Output size**: A4, Letter

10 Select **Next**.

11 For Source, select **Devices**.

You can select the devices in the selected groups. You can select multiple groups.

12 In the Group column, select a group, then select the devices in the Device column.

You can find and display devices using the following options:

To find a group in a large list of groups, select **Search** in the Group column, enter a search term, then use the up and down arrows to move between instances of the search term in the hierarchical structure. The number of occurrences of the search term is displayed as well.

To find a device among many in the Device column, enter a search value in the search box, select the **Search** icon, and select the devices.

Use the **Device ID** gear icon in the Device column to select a category to sort the list of devices: Serial number, Host name, IPv4 address, MAC address.

13 For Option, select **Add target information**.

14 Select **Next**.

15 Select a **Report range**.

Last x days

Select the number of days before the generated time

Date range

Select the Start and End date

Recent x months

Select the Start and End days

16 Select a **Frequency**.

On scheduled intervals

Daily, Weekly, Monthly

At scheduled time

Date and Time

On demand

Immediately

17 Select **Next**.

18 Select **Me** to receive the notification as well as display your email address in the notification.

For Analysts, Customers, and Service users:

a) Select **Add users**, enter the email address of a user, then select the **Search** icon.

If found in the service, the user is added to the list. To include additional users, go through the steps again.

For System Administrators and Managers:

a) Select **Add users** to choose other users.

b) Select a group from which to add users.

You can use the search text box to find users.

c) Select **Email search** and enter the email address of a user, then select the **Search** icon.

d) Select any other users in the list.

You can also select **Clear all** or **Select all**.

e) Select **Add**.

19 Select **Send information-only emails** to users outside KFS or without access to the group.

The email content will not contain links. Enter the email address for each user. Additional email addresses should be separated by a semicolon.

20 Select **Send as bcc** to hide the email addresses of all recipients in the notification email.

21 Select **Next**.

22 Review the Summary, and then select **Finish**.

Creating a graphical report schedule for groups

You can create a graphical report schedule for groups to generate and send graphical reports.

1 In the Devices view, select **Graphical reports**.

2 Select **Schedule**.

3 In the View by menu, select the group or **Private**.

The View by menu is displayed only for System Administrators and Managers.

4 Select **Add**.

5 Enter a **Name** for the graphical report schedule (64 character maximum).

6 Select a **Template name** (graphical report template).
You can enter text in the Search box to find a template.

7 Enter a **Report name** (64 character maximum).

8 Select a **File format** for the graphical report: .pdf, .docx, .xlsx, .pptx, .csv
Producing some graphical reports can be time-consuming based on the volume of data selected for the report. For this reason, graphical report scheduling identifies default and recommended file formats based on the selected report. Further, when graphics are in a select graphical report schedule, then the .csv file format is unavailable.

9 Select an **Output size**: A4, Letter

10 Select **Next**.

11 For Source, select **Groups**.
You can chose devices in the selected groups. You can select multiple groups.

12 In Quick select, you can display devices in the following manner:

Exclusively managed
All child groups but not delegated groups under them.

All accessible
All child groups and the delegated groups under them.

Off
No filtering for the group.

13 In Search, enter a group name then use the up and down arrows to move between instances of the search term in the hierarchical structure. The number of occurrences of the search term is displayed as well. Select a group.

14 For Option, select **Add target information**.

15 Select **Next**.

16 Select a **Report range**.

Last x days
Select the number of days before the date the report is generated within to retrieve data for the report.

Date range
Select the Start and End dates.

Recent x months

Select the Start and End dates.

17 Select a **Frequency**.

On scheduled intervals

Daily, Weekly, Monthly

At scheduled time

Date and Time

On demand

Immediately

18 Select **Next**.

19 Select **Me** to receive the notification as well as display your email address in the notification.

For Analysts, Customers, and Service users:

a) Select **Add users**, enter the email address of a user, then select the search icon.

If found in the service, the user is added to the list. To include additional users, go through the steps again.

For System Administrators and Managers:

a) Select **Add users** to add other users.
b) Select a group from which to add users.

You can use the search text box to find users.

c) Select **Email search** enter the email address of a user, and then select the **Search** icon.
d) Select any other users in the list.

You can also select **Clear all** or **Select all**.

e) Select **Add**.

20 Select **Send information-only emails** to users outside KFS or without access to the group. The email content will not contain links. Enter the email address for each user. Additional email addresses should be separated by a semicolon.

21 Select **Send as bcc** to hide the email addresses of all recipients in the notification email.

22 Select **Next**.

23 Review the Summary, and then select **Finish**.

Editing a graphical report schedule

1 In the Devices view, select **Graphical reports**.

2 Select **Schedule**.

3 In the View by menu, select a group or **Private**.

4 Select the check box of a graphical reports schedule.

5 Select **Edit**.

6 Edit the following options:

- Name
- Template
- Report name
- File format
- Output size
- Source
- Report range
- Option
- Frequency
- Recipients

7 Select **Finish**.

Deleting graphical report schedules

You can delete graphical report schedules.

1 In the Devices view, select **Graphical reports**.

2 Select **Schedule**.

3 In the View by menu, select a group or **Private**.
Private is displayed only for System Administrators and Managers.

4 Select graphical report schedules.

5 Select **Delete**.

6 Select **OK**.

Filtering and searching for graphical report templates

You can filter and search for graphical report templates within a specified category by using keywords or selecting from a predefined set of values.

1 In the Devices view, select **Graphical reports**.

2 Select **Templates**.

3 In the Search drop-down list, select a search category, and then type a search string or select a predefined option.

The following items use predefined options:

Last update (Later than), Last update (Recent)

24 hours, 7 days, 14 days, 30 days

4 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Viewing the details of a graphical report template

1 In the Devices view, select **Graphical reports**.

2 Select **Templates**.

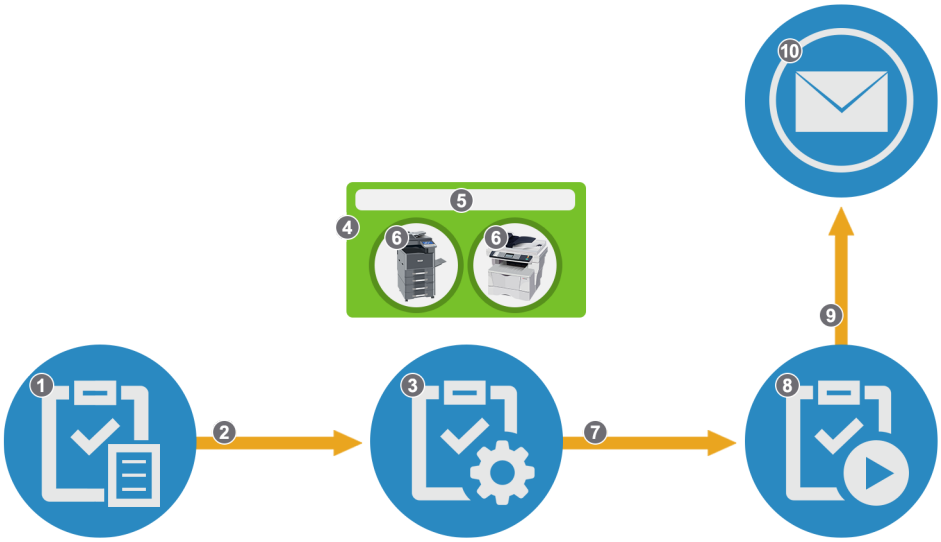
3 Select the information icon of a graphical report template to view the details.

4 Select **Close**.

29 List reports

With List reports, you can obtain data from specific devices, gateways, or groups, and specify how to display the data in KFS or in reports. List reports are run based on a template using a schedule or on-demand. They can be viewed on screen, downloaded in the **List reports** > **History**, or set-up in the template to be emailed to KFS users and non-users. The reports can be viewed on screen because reports are saved in KFS.

With the schedule settings, you can select to generate a list report at a scheduled time or on demand. They can also be sent via email. You can setup KFS to report information for groups and devices on a schedule or on demand. For all users except for System Administrators, selected permissions govern access to List reports. If permissions are removed, the status of Report Schedule items automatically changes to Warning.



List reports	
1 - Report Template	2 - Selected
3 - Report Schedule	4 - Reporting Source
5 - Group 1	6 - Devices
7 - Created	8 - Generated Report
9 - Send	10 - Email (Outside of System)

Viewing list reports details

You can view the details of list reports. If the source includes multiple groups, gateways, or devices, select the information icon to view the list of groups, gateways, or devices.

1. In the Devices view, select **List reports**.
2. In the History list, select the information icon of a list report to view the following details:
   - Name
   - Report name
   - Source (can include multiple groups, gateways, or devices)
   - File format
   - Size
   - Recipient
   - Generated time
   - Created by
3. Select **Close**.

Filtering and searching for list reports

1. In the Devices view, select **List reports**.
2. In the Search drop-down list, select a search category, and then type a search string or select a predefined option.

   Priority level

   High, Medium, Low, Clear

   Source

   Devices, Groups, Gateways

   File format

   .csv, .xml

   Generated (Later than), Generated (Recent)

   24 hours, 7 days, 14 days, 30 days
3. Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Setting the list reports priority level

1. In the Devices view, select **List reports**.

2 Select one or more reports.

3 Select **Set priority**.

4 Select a priority level. You can also set the priority level of the list reports by selecting the flag icon for the report.

The following options are available:

- High (Red)
- Medium (Blue)
- Low (Green)
- Clear (Gray)

Deleting list reports

1 In the Devices view, select **List reports**.

2 Select the list reports.

3 Select **Delete**.

4 Select **OK**.

Downloading list reports

You can download list reports. Multiple list reports can be downloaded at once. All selected list reports (.csv or .xml files) are included in a .zip.

1 In the Devices view, select **List reports**.

2 Select the list reports.

3 Select **Download**.

Report templates

Report templates specify the contents of list reports you want to receive. In List reports, you can select templates when you are creating a report schedule.

The following default system templates are available:

Group Summary

A report template containing the management status of devices for all groups.

Gateway Reports

A report template containing detailed gateway information for the selected group.

Counter Reports

A report template containing device counter information for each device.

Toner Reports

A report template containing device toner information for each device.

Group Property

A report template containing detailed group information.

Group Task Summary

A report template containing task and remote maintenance for a group.

HyPAS applications

A report template containing HyPAS application information for each device.

Group Summary report by brand

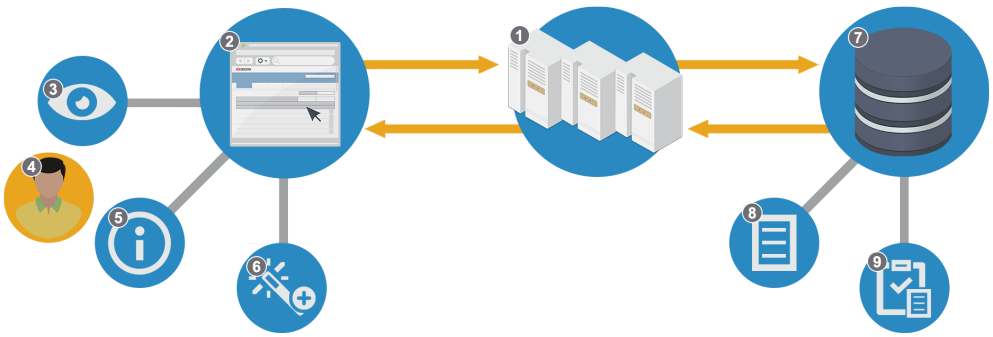
A report containing device manufacturer brand for a group.

Remote panel usage

A report containing the results of Remote panel execution logs for users that belong to the delegated group. Only System Administrators and Managers with group permission can obtain these results. The setting for compress email attachment cannot be changed.

System Administrators can share a list report template to the entire system or to any delegated groups in the system. System Administrators can also edit, copy, or delete shared templates of every delegated group in the system. Managers can only share list report templates with groups they have access to. This includes their delegated group and sub-groups of that group. Managers can edit, copy, or delete shared templates of the delegated groups. Service users and Analysts can share list report templates to users who belong to the same-delegated groups. All users can edit, copy, and delete their list report templates.

You can use a report template in more than one report.



Report Templates	
1 - KFS	2 - UI (Manager)
3 -View	4 - Customer

5 - Details	6 - Add/Edit Wizard
7 - Customer	8 - Default Template
9 - Report Template	

Viewing report template details

1. In the Devices view, select **List reports**.
2. Select **Templates**.
3. Select the information icon of the report template.
   The report template details include the following information:
   - Template name
   - Description
   - Reported fields
   - Share
   - Created by
   - Last update
   - Updated by
   - Reference
4. Review the details of the report template.
5. Select **Close**.

Filtering and searching for report templates

1. In the Devices view, select **List reports**.
2. Select **Templates**.
3. In the Search drop-down list, select a search category, and then type a search string or select a predefined option.

   The following items use predefined options:

   Share

   Private, Share, System share

   Last update (Later than), Last update (Recent)

   24 hours, 7 days, 14 days, 30 days
4. Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Creating report templates

System Administrators can create and share templates with any delegated group or the entire system. Managers can share templates to delegated groups that they are authorized to access.

Service users and Analysts can select **Share template** to save the template to their group. **Share template** is not available for Customers.

1. In the Devices view, select **List reports**.
2. Select **Templates**.
3. Select **Add**.
4. Enter a **Template name** for the report templates (64 character maximum).
5. Enter a **Description** (256 character maximum).
6. Templates can be shared based on your permissions and access authority. To share a report template, select **Share template**, and then select **Share to system** (for system-wide access) or **Share to group**, and select a group.
7. Select **Next**.
8. Select the items in Available columns list, and then select the right arrow to move the items to the Report items list.
9. To arrange the Report items list, select the items and use the up or down arrows.
10. To add counter data obtained from devices, select **Include counter information in the report** and **Include other consumable information in the report**.
11. Select **Next**.
12. Both counter information and other consumable information contain counter data you can choose to include in the report. Select your counter data.
13. Select **Next**.
14. In Change header label, you can rename column header names for the report items.
15. Select **Finish**.
16. If wanted, select **OK** to add the report schedule.

    You cannot select another template when you add the report schedule.

    To view the topics about report schedules, see *Creating a Report Schedule for Devices* or *Creating a Report Schedule for Groups*.
17. If you do not want to create the report schedule, select **Cancel**.

Editing report templates

You can change the settings in a report template.

1. In the Devices view, select **List reports**.
2. Select **Templates**.
3. In the View by menu, select the group, **System share**, or **Private** based upon your permissions and your KFS role.
4. Select the report template.
5. Select **Edit**.
6. Edit the settings for the following:
   - Template name and description
   - Report items
   - Counter information (only when it is included in the report)
   - Change header label
7. Select **Finish**.

Copying report templates

1. In the Devices view, select **List reports** > **Templates**.
2. In the View by menu, select a group, **System share**, or **Private** based upon your permissions and user role.
3. Select the report template.
4. Select **Copy**.
5. Edit the values for the following options:
   - Template name and Description
   - Share template
   - Report items
   - Counter information (only when included in the report)
   - Change header label
6. Select **Finish**.

Deleting report templates

You can delete report templates. You cannot delete a report template that is used by other schedules.

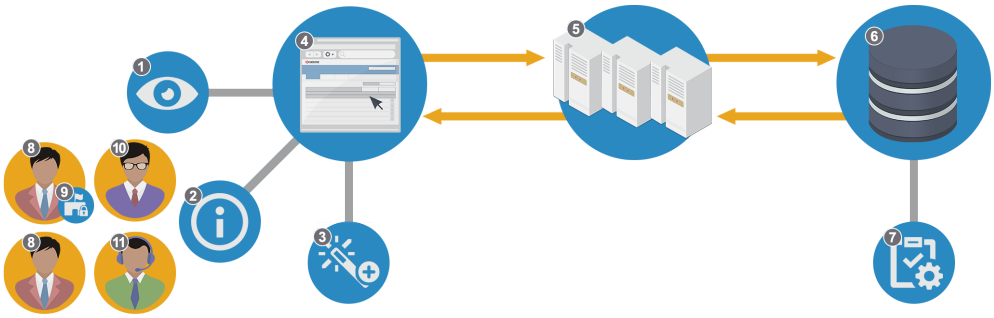
1. In the Devices view, select **List reports**.
2. Select **Templates**.
3. In the View by menu, select a group, **System share**, or **Private** based upon your permissions and role.
4. Select the report templates.
5. Select **Delete**.
6. Select **OK**.

Report schedule

Report scheduling is created with the list reports schedule wizard. You can specify the groups, gateways, or devices from which to generate report data, specify the frequency of report generation, and specify the recipients of the report. The schedule creator's email address is included in the email reports sent to the target user.

You can enable or disable report schedules. If an error occurs with a group, gateway, or device in a report schedule, then the schedule status changes to warning. You can change the report schedule status from warning to enable by resolving the error or condition.

For Gateway report schedules, you can choose a multiple groups or gateways.



Report Schedule	
1 - View	2 - Details
3 - Add/Edit Wizard	4 - UI (KFS)
5 - KFS	6 - Database
7 - Report Schedule	8 - Manager
9 - RHQ Permissions	10 - System Administrator
11 - Service	

Viewing report schedule details

You can view report schedule details for List reports. If the source includes multiple groups, gateways, or devices, select the information icon to view the list of groups or links to the devices.

1. In the Devices view, select **List reports** > **Schedule**.
2. In the list, select the information icon of the desired report schedule.
3. If the file type is .xml, you can select **Download XSD schema** to download the schema file to your default download location. The file can be opened in a text editor.
4. Select **Close**.

Filtering and searching for report schedules

You can search for report schedules in List reports.

1. In the Devices view, select **List reports** > **Schedule**.
2. In the View by menu, select the group or **Private**.
   The View by menu is displayed only for System Administrators and Managers.
3. In the Search drop-down list, select a search category, and then type a search string or select a predefined option.

   The following items use predefined options:

   Status

   Enabled, Disabled, Warning

   Source

   Devices, Groups, Gateways

   Last run time (Later than), Last run time (Recent), Next run time (Earlier than), Next run time (Later than)

   24 hours, 7 days, 14 days, 30 days

   Schedule results

   Successful, Failed, On hold, Processing
4. Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Creating a report schedule for devices

You can create a report schedule for devices which includes selection of a template, devices, date range, report frequency, and the recipients of the report. You can also create a new template.

1. In the Devices view, select **List reports**.
2. Select **Schedule**.
3. Select **Add**.
4. Enter a **Name** for the report schedule (64 character maximum).
5. Select a report template associated with devices (i.e. Toner Reports) or enter the name of an existing report template in the Search text box and press **Enter**.

   All templates

   Displays all report templates the user has access to.

   Private

   Displays report templates the user created and are not shared.

   Share

   View and select a report template that is shared in your delegated group.

   System share

   Displays all report templates available to all users.

   As an alternative template selection method:

   a) Select **New template**.
   b) Select a **Method** by choosing **Create a new template** or **Copy from an existing template**.

      New templates are created as Private templates.

      Both methods require a Template name and you can create an optional Description.

      For the copy method, you must select a **Report template** then select a **Template**. Both methods lead into the Add Report Template wizard.
6. Type a **Report name** (64 character maximum).
7. Select a **File format**: .csv or .xml.
8. By default, the report is sent as a compressed file.

   Clear the **Compress email attachment** box to send the report as an uncompressed file.
9. Select **Next**.

10 For Source, select **Devices**. You can select multiple devices and devices within a group.

11 In the Group column, select a group, then select the devices in the Device column.

You can find and display devices using the following options:

To find a group in a large list of groups, select **Search** in the Group column, enter a search term, then use the up and down arrows to navigate within the hierarchical structure. The number of occurrences of the search term is displayed as well.

To find a device among many in the Device column, enter a search value in the Search box, select the search icon, and select the devices.

Use the **Device ID** gear icon in the Device column to choose how the devices are displayed in the list. Select Serial number, Host name, IPv4 address, or MAC address.

12 Select **Target devices filter type** to filter the target devices in the report. This setting is available only for toner and counter reports.

In the drop-down list, select one of the following:

Last update

Applies to inactive devices which have not received recent updates. The range is 1 to 90 days.

Toner order criteria

Applies to devices with toner ordering required for at least one toner.

Early warning (jam)

Applies to devices which have logged an EWS1, EWS2, or a combination of both warnings.

13 Select **Next**.

14 Select a **Report range**.

Latest date

Uses the most recent date.

Last x days

Select the number of days before the Generated time.

Current month

Select the **Start** and **End** days.

Previous month

Select the **Start** and **End** days.

Date range

Select the **Start** and **End** date and time.

15 Select a **Frequency**.

On scheduled intervals

Daily, Weekly, Monthly

At scheduled time

Date and Time

On demand

Immediately

16 Select **Next**.

17 Select **Me** to receive the notification as well as display your email address in the notification.

For Analysts, Customers, and Service users:

a) Select **Add users**, enter the email address of a user, then select the **Search** icon.

If found in the service, the user is added to the list. To include additional users, go through the steps again.

For System Administrators and Managers:

a) Select **Add users** to choose other users.
b) Select a group from which to add users.

You can use the search text box to find users.

c) Select **Email search** and enter the email address of a user, then select the **Search** icon.
d) Select any other users in the list.

You can also select **Clear all** or **Select all**.

e) Select **Add**.

18 Select **Send information-only emails** to users outside KFS or without access to the group.

The email content will not contain links. Enter the email address for each user. Additional email addresses should be separated by a semicolon.

19 Select **Send report only if there are results** to eliminate receipt of no result reports.

20 Select **Send as bcc** to hide the email addresses of all recipients in the notification email.

21 Select **Next**.

22 Review the Summary, and then select **Finish**.

Creating a report schedule for groups

You can create a list report schedule for groups which includes selection of a template, devices, date range, report frequency, and the recipients of the report. If

the listed templates do not have what you want in the report, you can create a new template and then copy and modify it.

1. In the Devices view, select **List reports**.
2. Select **Schedule**.
3. Select **Add**.
4. Enter a **Name** for the report schedule (64 character maximum).
5. Select a report template associated with groups or enter the name of an existing report template in the Search text box and press **Enter**.

   All templates

   Displays all report templates the user has access to.

   Private

   Displays report templates the user created and are not shared.

   Share

   View and select a report template that is shared in your delegated group.

   System share

   Displays all report templates available to all users.

   As an alternative template selection method:

   a) Select **New template**.
   b) Select a **Method** by choosing **Create a new template** or **Copy from an existing template**.

      New templates are created as Private templates.

      Both methods require a Template name and you can create an optional Description.

      For the copy method, you must select a **Report template** then select a **Template**. Both methods lead into the Add Report Template wizard.
6. Type a **Report name** (64 character maximum).
7. Select a **File format**: .csv or .xml.
8. By default, the report is sent as a compressed file. Clear the **Compress email attachment** box to send the report as an uncompressed file.
9. Select **Next**.
10. For Source, select **Groups**.
11. In Quick select, you can select devices with the following options:

    Exclusively managed

    All child groups but not delegated groups under them.

All accessible

All child groups and the delegated groups under them.

Off

No filtering for the group.

12 Select **Target devices filter type** to filter the target devices in the report. This setting is available only for toner and counter reports. In the drop-down menu, select one of the following:

Last update

Applies to inactive devices which have not received recent updates. The range is 1 to 90 days.

Toner order criteria

Applies to devices with toner ordering required for at least one toner.

Early warning (jam)

Applies to devices which have logged an EWS1, EWS2, or a combination of both warnings.

13 Select **Next**.

14 Select a **Report range**.

Latest date

Uses the most recent date.

Last x days

Select the number of days before the Generated time.

Current month

Select the **Start** and **End** days.

Previous month

Select the **Start** and **End** days.

Date range

Select the **Start** and **End** date and time.

15 Select a **Frequency**.

On scheduled intervals

Daily, Weekly, Monthly

At scheduled time

Date and Time

On demand

Immediately

16 Select **Next**.

17 Select **Me** to receive the notification as well as display your email address in the notification.

For Analysts, Customers, and Service users:

a) Select **Add users**, enter the email address of a user, then select the **Search** icon.

If found in the service, the user is added to the list. To include additional users, go through the steps again.

For System Administrators and Managers:

a) Select **Add users** to choose other users.

b) Select a group from which to add users.

You can use the search text box to find users.

c) Select **Email search** and enter the email address of a user, then select the **Search** icon.

d) Select any other users in the list.

You can also select **Clear all** or **Select all**.

e) Select **Add**.

18 Select **Send information-only emails** to users outside KFS or without access to the group.

The email content will not contain links. Enter the email address for each user. Additional email addresses should be separated by a semicolon.

19 Select **Send reports only if there are results** to eliminate receipt of no result reports.

20 Select **Send as bcc** to hide the email addresses of all recipients in the notification email.

21 Select **Next**.

22 Review the Summary, and then select **Finish**.

Creating a report schedule for gateways

You can create a report schedule for gateways which includes selection of a template, devices, date range, report frequency, and the recipients of the report. You can also create a new template.

1 In the Devices view, select **List reports**.

2 Select **Schedule**.

3 Select **Add**.

4 Enter a **Name** for the report schedule (64 character maximum).

5. Select **Gateway Report template** or enter the name of an existing gateway report template in the Search text box and press **Enter**.
6. Type a **Report name** (64 character maximum).
7. Select a **File format**: .csv or .xml.
8. By default, the report is sent as a compressed file. Clear the **Compress email attachment** box to send the report as an uncompressed file.
9. Select **Next**.
10. For Source, select **Gateways**.
11. In the Group column, select a group, then select one or more gateways in the Gateway column.

    You can find and display groups and gateways using the following options:

    To find a group in a large list of groups, select **Search** in the Group column, enter a search term, then use the up and down arrows to navigate within the hierarchical structure. The number of occurrences of the search term is displayed as well.

    To find gateway in the Gateway column, enter a search value in the Search box, select the search icon, and select the gateway.

    Use the **ID** gear icon in the Gateway column to select how the gateways are displayed in the list. Select Gateway ID, Host name, or IPv4 address.
12. Select **Target Gateways filter type** to filter the target gateways in the report.

    Last update

    Applies to gateways which have not received recent updates within the days specified. The range is 1 to 100 days.
13. Select **Next**.
14. Select **Me** to receive the notification as well as display your email address in the notification.

    For Analysts, Customers, and Service users:

    a) Select **Add users**, enter the email address of a user, then select the **Search** icon.

       If found, the user is added to the list. To include additional users, go through the steps again.

    For System Administrators and Managers:

    a) Select **Add users** to choose other users.
    b) Select a group from which to add users.

       You can use the search text box to find users.
    c) Select **Email search** and enter the email address of a user, then select the **Search** icon.
    d) Select any other users in the list.

You can also select **Clear all** or **Select all**.

e) Select **Add**.

15 Select **Send information-only emails** to users outside KFS or without access to the group.

The email content will not contain links. Enter the email address for each user. Additional email addresses should be separated by a semicolon.

16 Select **Send reports only if there are results** to eliminate receipt of no result reports.

17 Select **Send as bcc** to hide the email addresses of all recipients in the notification email.

18 Select **Next**.

19 Review the Summary, and then select **Finish**.

Editing report schedules

1 In the Devices view, select **List reports** > **Schedule**.

2 In the View by menu, select the group or **Private**.

The View by menu is only for System Administrators and Managers.

3 Select the report schedule.

4 Select **Edit**.

5 Make your changes to the schedule settings.

6 Select **Finish**.

Deleting report schedules

1 In the Devices view, select **List reports**.

2 Select **Schedule**.

3 In the View by menu, select a group or **Private**.

The View by menu is only for System Administrators and Managers.

4 Select a report schedule.

5 Select **Delete**.

6 Select **OK**.

Generating reports

1. In the Devices view, select **List reports**.
2. Select **Schedule**. In the View by menu, select a group or **Private**.
   The View by menu is only for System Administrators and Managers.
3. Select a report schedule.
4. Select **Generate report**.

You can generate a report if the report schedule status has a warning. The report can be accessed in **List Reports** > **History**.

Enabling or disabling report schedule status

1. In the Devices view, select **List reports**.
2. Select **Schedule**.
3. In the View by menu, select a group or **Private**.
   The View by menu is only for System Administrators and Managers.
4. Select a report schedule.
5. Select **Change status**.
6. Select **Enable** or **Disable**.

30 Announcements

With KFS, you can manage and publish announcements for a group. You can use announcements to send important information to a specific group about a device or release. System Administrators and authorized Managers can create, edit, and retract announcements. System Administrators and Managers can send an email notification to a specific group about an announcement. System Administrators can authorize Managers of a delegated group by selecting edit user permissions in Group/Edit. Service users, Analysts, and Customers can view the announcements.

The three types of recipients for announcements include the following:

Organization wide

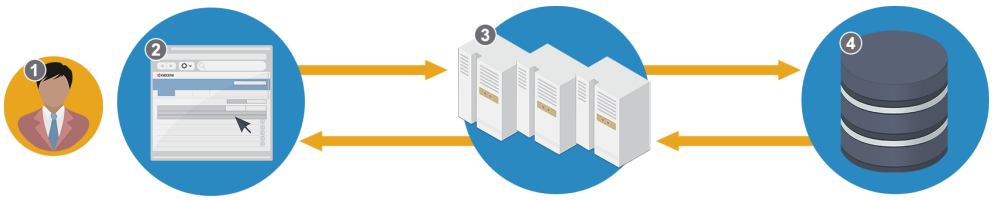
Recipients are users who belong to a group the Announcement creator has access to.

Group wide

Recipients are users who belong to the selected delegated group and its child groups (not listed).

Individual groups

Recipients are users who belong to the selected groups.



Announcements	
1 - Manager	2 - UI (Manager)
3 - KFS	4 - Database

Creating announcements

System Administrators and authorized Managers can create announcements for a specific group in KFS. System Administrators can authorize Managers of a delegated group to create announcements. Each user can select the Announcement Settings level which triggers an email notification for the announcement.

1. In the top banner, select **Announcements**.
2. Select **Create**.

3 Enter a **Title** for the announcement (64 character maximum).

4 Select an importance level for the announcement:

- High
- Normal
- Low

5 Enter or paste the announcement to a maximum of 10 MB encoded data.

The Title and Announcement text boxes are used as the default title and message.

6 Select the language, which opens a new untitled text box.

7 Select **Use announcement title** to use the default title and message.

8 You can type or paste the new Announcement text for the selected language.

9 (Optional) To create an announcement in another language:

a) Select **Add language** and select a language.
b) Select **Use announcement title** or **Custom title**.
For Custom title, enter the title.
c) Enter the localized announcement content in the text box.

10 Select **Next**.

11 In Recipients, select one of the following distributions:

Organization wide

Users belonging to a group the Announcement creator has access to.

Group wide

Users belonging to the selected delegated group and its child groups (not listed).

Individual groups

Users belonging to the selected groups.

12 For Group wide and Individual groups, select the group or groups to be included in the announcement.

You can select **Search**, enter a group name to find the group, and press **Enter**.

13 Select x to close the Search text box.

14 In Notification, select **Send an accompanying email notification** to send an email notification about the announcement to the members in the selected groups.

The email format uses a Blind Carbon Copy (bcc) format to hide the email addresses of all recipients in the notification email.

15 Select **Next**.

16 In Schedule, select **Send now** to send the announcement immediately, or select **Send later (based on local time zone)** to send the announcement based on the date and time you establish.

17 Select **Next**.

18 Review the Summary, and then select **Confirm**.

Creating announcements from existing announcements

System Administrators and authorized Managers can create a new announcement from an existing announcement. You can display a total of 7 unread announcements in the top banner drop-down list.

1 In the top banner, select **Announcements**.

2 Select the announcement, and then select **Create from existing**.

3 Make changes to the Title, Importance, and Announcement.

4 (Optional) To create an announcement in another language:

a) Select **Add language** and select a language.

b) Select **Use announcement title** or **Custom title**.

For Custom title, enter the title.

c) Enter the localized announcement content in the text box.

5 Select **Next**.

6 Make changes to Recipients, Notification, and Group.

7 Select **Next**.

8 Make changes to Schedule.

9 Select **Next**.

10 Review the Summary, and then select **Confirm**. You can view the new announcement on the Announcements page.

Opening announcements view

You can view both read and unread announcements in the Announcements list.

1 In the top banner, select **Announcements**.

2 Select **See all** to open the Announcements view.

Setting announcements importance level

You can set the importance level of the announcements for which you want to receive the email notifications. You will receive email notifications for announcements with a priority greater than or equal to the selected importance level.

1. In the top banner, select **Announcements**.
2. Select **See all**.
3. Select **Settings**.
4. Drag the slider to set the announcement Importance level for email notifications to High, Medium, or Low.
5. Select **Save**.

Retracting announcements

System Administrators and authorized Managers can retract announcements.

1. In the top banner, select **Announcements**.
2. Select **See all**.
3. Select the announcements.
4. Select **Retract**.
5. Select the **Send an accompanying email notification** check box if you want to send an email notification after the announcements are retracted.
6. Select **OK**.

Filtering announcements

You can filter announcements. Only System Administrators and Managers can view recipients.

1. In the top banner, select **Announcements**.
2. Select **See all**.
3. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option.

   The following items use predefined options:

   Read/Unread

   Read, Unread

Importance

High, Normal, Low

Announcement date (Later than), Announcement date (Recent)

24 hours, 7 days, 14 days, 30 days

4 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Marking announcements as read or unread

You can mark announcements as read or unread on the Announcements page. You can mark announcements one by one or all at once.

1 In the top banner, select **Announcements**.

2 Select **See all**.

3 Select the announcements.

4 Select **Mark read**.

5 Select **Read** to mark the selected announcements as read, or **Unread** to mark the selected announcements as Unread.

Email templates

The following email templates for announcements are available:

- CREATE ANNOUNCEMENT

  Subject: [KFS Announcement] <Title>

  Body:

  An announcement has been posted.

  Select the link <hyperlink> to view the announcement.

  Text preview:

  <ANNOUNCEMENT BODY>

  KYOCERA Fleet Services <hyperlink>

- RETRACT ANNOUNCEMENT

  Subject: [KFS Announcement] <Title> - Retracted

  Body:

  An announcement has been retracted.

  Text preview:

<ANNOUNCEMENT BODY>

KYOCERA Fleet Services <hyperlink>

Viewing announcement details

You can view the details of an announcement. System Administrators can view the announcement details in other languages.

1. In the top banner, select **Announcements**.
2. Select **See all**.
3. Select the view icon for the announcement's details.
4. Select **Close**.

31 Device Registration Diagnostic Tool

The Device Registration Diagnostic Tool (DRD Tool) provides fast registration of multiple local network devices to KFS. The application is run from a Windows desktop and can discover network printers over SNMP, review registration status, diagnose issues with XMPP and Proxy settings, KFS authentication as well as communication with the HTTP and XMPP servers.

Device registration is normally performed at a customer site by a Service user. Service users run the DRD Tool from a USB drive inserted into a computer or from the service technician's laptop.

The DRD Tool discovers KYOCERA devices, configures Registration Settings, registers devices with KFS, performs firmware upgrades, and authenticates devices. The DRD Tool has a diagnostic feature to troubleshoot incorrect KFS server settings and connection issues with the XMPP server. The DRD Tool supports a maximum of 100 devices.

Downloading the Device Registration Diagnostic Tool

You can download the Device Registration Diagnostic Tool from KFS to your computer.

1. In the top banner, select **Product downloads**.
2. Scroll to **Device Registration Diagnostic Tool** and select **Download**.
3. In your computer's download folder, extract **DRTool.ZIP**, and then save the files to a DRD Tool folder.

Device registration

The process of device registration involves two servers - one for KFS and one for device registration. When you register devices to the device registration server, each device is assigned to the proper group. With the DRD Tool, users can register devices using their User ID / Email address and Password with an Access code. The groups and devices are then managed through KFS.

The following device registration methods are available:

- New models with firmware that supports WSDL and do not require authentication settings, as the settings are automatically detected.
- Not all devices that support WSDL support registration via WSDL.
- Devices with Command Center RX require a username and password.
- Devices with Command Center require the Command Center password.

  Authentication method depends on the device settings. For example, CCRX devices are registered with the Command Center password.

Registration settings

You can register devices with the DRD Tool using the KFS Registration URL and the access code for the group that the devices belong to. The DRD Tool also supports device registration using User ID / Email address, Password, and Access code. The first method, with just an Access code, registers the device as Pending. The second method, using credentials with the Access code, registers the device as Managed.

Adding registration and unregistration settings

In the DRD Tool, you can create registration settings and then check that they are valid.

1. In the toolbar, select **Registration settings**.
2. If your network uses a proxy server to connect to the internet, enter the proxy server settings under Proxy settings. Select **Start diagnostic** to test that your settings are valid.
3. In Server settings, enter the KFS Registration URL.
4. In User access code (group code), enter the Access code for a KFS group.
5. Select User credentials and then enter your User ID / Email address and Password to register the device to KFS in a Managed state rather than a Pending state.
6. Select **Start diagnostic** to test whether your settings are valid.
7. Select **Unregistration**, and then enter the required settings for unregistration.
8. Select **OK**.

Obtaining the registration settings information

You can copy and save the KFS Registration URL and Access code for the DRD Tool registration settings. This information is required for using the DRD Tool with devices.

1. In KFS, select the group.
2. In the Group name list, select the information icon for the group to open Details.
3. Copy the Registration URL and Access code, and then save this information to use in the Registration settings in the DRD Tool.
4. For any additional groups, copy and save the Access code.

Adding devices to the DRD Tool

You can discover and add devices to the DRD Tool. The DRD Tool searches for and lists devices based on selected parameters.

1. In the toolbar, select **Add devices**.
2. Select a Discovery method: **Search for network printers** or **Search by host name or IP address**.
3. If you select **Search by host name or IP address**, select your search options or accept the default. To search outside the local network, use the IP address or IP address range options.
4. Select **Next**.
5. Set Communication settings and Device login options, and then select **Start**.

   Discovered devices display in a list with an Authentication status column. A green check means you can register the device. A red exclamation mark means the DRD Tool cannot authenticate the device. In this case, update Device authentication settings for the device.

Registering devices

To register devices with the DRD Tool, you must provide Registration settings.

1. In the DRD Tool device list, select each device you want to register.

   You can select multiple devices. You can also select all devices by selecting the header row above the boxes.
2. Select **Register devices**.
3. Select **OK**.
4. When the registration is finished, select **Close**.

Unregistering devices with the DRD Tool

To unregister devices with the DRD Tool, you must provide Registration settings. These settings include the URL of the KFS server and the Access code of the group with the registered devices.

1. In the DRD Tool device list, select the devices you want to unregister.

   You can select all devices by selecting the header row above the boxes.
2. Select **Unregister devices**.
3. Make sure that all the devices you want to unregister are selected, and then select **OK**.
4. When the unregistration process is finished, select **Close**.

Devices may show their registration status as **N/A** after the unregistration process finishes. Select **Refresh** to update the list.

Configuring the XMPP settings

XMPP settings can diagnose potential connectivity issues with KFS. The inability to connect from the customer's network to the XMPP server can cause all of the devices registered in KFS to display as offline and/or unable to perform many tasks and operation. The XMPP protocol is used for messages such as status reports or requests for information between a KFS server and a device. The diagnostic checks the connection with the XMPP server.

1. In the toolbar, select **XMPP settings**.
2. Select **Obtain settings** to load settings from the KFS server.
3. Make changes to XMPP settings.
4. Select **Start diagnostic** to test the connection with the XMPP server.
5. Select **OK**.

Updating device authentication in the DRD tool

The second column in the DRD Tool device list shows Authentication status. Authentication requires that proper credentials be used when adding devices. In this case, the green mark in the Authentication status column indicates authentication was successful and the devices can be registered. For devices with a red exclamation point, authentication did not work with the DRD Tool. In this state, the device is not capable of being registered with a KFS server. Devices without KFS compatible firmware cannot be authenticated with the DRD Tool.

1. To resolve conflicts, select the devices in the DRD Tool devices list that show Authentication failure status.
2. Select **Device authentication**.
3. Make necessary credential changes to User name and Password, or Command Center password.

   If necessary, update your Authentication mode.
4. Select **OK**.
5. Select **Update KFS registration status**.

Modifying device authentication

The DRD Tool can change the values for Device login including User name, Password, Command Center password, and Authentication mode. The DRD Tool uses these settings to communicate with devices that do not have KM-WSDL

capabilities. These settings are required for the DRD Tool to authenticate with a device or for updating when the Authentication status column displays a red exclamation point.

1. Select a device or multiple devices in the DRD Tool device list that displays a red exclamation point in the Authentication status column.
2. Select **Device authentication**.
3. Make necessary credential changes to User name and Password, or Command Center password.

   If necessary, update your Authentication mode.
4. Select **OK**.

Updating registration status

With the DRD Tool, you can update the registration status of devices in the DRD Tool device list. It checks whether the selected devices are registered to a KFS or TDRS server.

1. Select individual devices in the DRD Tool device list.

   You can select all devices by selecting the header row above the boxes.
2. Select **Update KFS registration status**.
3. Select **Close**.

Upgrading firmware with the DRD tool

You can upgrade the firmware for a device or for multiple devices of the same model with the DRD Tool. To perform firmware upgrades from the DRD Tool, TCP ports 800-899 must be available and not blocked by a firewall.

For security reasons, this version of the DRD Tool does not allow firmware upgrades unless you run the program as an administrator with full access rights. Right-click on the program shortcut or .exe and select **Run as administrator**.

1. Select a device or multiple devices of the same model type in the DRD Tool device list.
2. Select **Firmware upgrade**.
3. Select the box to acknowledge the risk associated with a firmware upgrade, and then select **Next**.
4. Select **Browse**, select the firmware package, select **Open**, and then select **Next**.
5. Confirm the appropriate firmware for the devices, and then select **Upgrade**.

Viewing the device home page

You can visit the home page of any device in the device list. The Device home page opens in your default browser.

1. Select a device in the DRD Tool device list.
2. Select **Device home page**.

Saving DRD Tool settings

You can save the current DRD settings in the DRD Tool. These include Registration and Unregistration settings, Communication settings, Device login, Discovery method, and XMPP settings. The DRD Tool automatically saves settings entered which are immediately available on the next use of the application. Saved settings allow you to store multiple sets of settings for use in different servers and configurations.

1. In the toolbar, select **Save settings as**.
2. Type a name for the JSON file, and then select **Save**.

Loading DRD tool settings

You can load DRD settings that have been previously saved using the DRD Tool.

1. In the toolbar, select **Load settings**.
2. Locate and select the JSON file, and then select **Open**.

32 Data Collection Tool

Data Collection Tool (DCT) is a Windows application for Service users to demonstrate the capability of KFS for a customer on the customer's network. The DCT can discover devices and collect devices data. Using DCT you can send collected devices data to KFS. DCT supports a maximum of 1000 devices.

The Data Collection Tool supports a 32-bit and 64-bit operating system version for Windows 7 and above. Your computer's operating system must have a Microsoft .NET Framework version 4.0 and above. You can download and install the Data Collection Tool from KFS to your computer. You can also run the Data Collection Tool on a USB drive.

The device data includes the general device information, counters, consumables, alerts, firmware versions, job logs, and summary.

Data Collection Tool license

The Data Collection Tool is available for KFS users only. You must log in to KFS to download the Data Collection Tool and a license key. This feature works only with the KFS server from which you downloaded the Data Collection Tool. DCT requires your KFS user credentials for login. The Data Collection Tool temporary license is valid for 7 days. The time remaining on the license is displayed in days. If the time remaining on the license is less than one day, the time is displayed in hours.

Data import with Data Collection Tool

Using the Data Collection Tool you can import communication settings and collected device data that are saved from previous sessions. With Import settings, you can import Discovery settings and start new device discovery. With Review collected data, you can also import Discovery settings and collected device data, however, you cannot start device discovery. Collected device data includes Consumables, Counters, Firmware, General device properties, Alerts, Job logs, and Summary.

Data Collection Tool summary view

The Data Collection Tool summary view shows the collected data of all discovered devices in chart diagrams. You can select bar chart and pie chart. The Summary view displays general information about counters, color mode, consumables, brand name, and device status. The pie chart format groups devices by brand name or other criteria. Groups with less than 8% of the total sum of the collected data are grouped to Other category.

The collected data from all discovered devices are displayed in table views where you can specify sorting and filtering options. Use the table header column to sort the displayed data. Specify filtering criteria using the combo box.

Downloading the Data Collection Tool

You can download the Data Collection Tool from KFS to your computer.

1. In the top banner, select **Product downloads**.
2. Scroll down to the Data Collection Tool, and select **Download**.
3. In your computer's download folder, extract **DCTool.ZIP**, and then save the files to a DCTool folder.

Installing and opening the Data Collection Tool

You can install the Data Collection Tool after it has been downloaded from KFS to your computer. Your computer must have Microsoft .NET Framework version 4.

1. In the extracted DCTool folder, select **Data Collection Tool**.
2. On the License page, enter your User ID / Email address and Password.
3. If your login requires proxy settings, select **Use proxy settings**.

   Enter values for Host, Port, User name, and Password.
4. Select **Sign in**.
5. Select **START NEW**.

Discovering devices with the Data Collection Tool

1. In the Data Collection Tool, select **START NEW**.
2. In the Discovery settings, select **Discovery method**.

   By local network

   Discovers devices on your local network (SNMPv3 is not supported).

   By IP address

   Discovers devices by IP address You must provide one or more IP address in IP address. Select the + icon to add another IP address.

   By IP address range

   Discovers devices by IP address range. You must provide one or more IP address ranges by typing the IP address in the starting IP address and ending IP address. Select the + icon to add another IP address range.
3. Select **Start discovery**.
4. To terminate device discovery, select **Stop discovery**.

Updating authentication with the Data Collection Tool

After you have performed a discovery, you can update the Device login and Communication settings for devices selected in the Discovered devices list.

1. In the Data Collection Tool, select the Discovered devices tab.
2. Select the devices in the list.
3. Select **Update authentication**.
4. Edit the Device login and Communication settings.
5. Select **Update**.

Importing collected devices data and discovery settings

1. In the Data Collection Tool, select **RESUME PREVIOUS**.
2. Select an import option:

   Import settings

   Resume using configuration settings from a previous session. You can import the discovery settings.

   Review collected data

   Import previously collected data to view or export results. You can import the discovery settings and all collected data. Use the Data Collection package (.dat) that was created with data export in the Data Collection Tool.

3. Select **Browse**, and then select the .dat.
4. Select **Resume**.

Exporting data with the Data Collection Tool

You can export collected data as one Data Collection package or as individual files as .csv from one or multiple devices. The.csv and packages use a timestamp in the filename. The Data Collection package can be imported in Resume previous.

1. In the Data Collection Tool, select **Data export**.
2. Select the devices.
3. Select **Export**.
4. Select **Data Collection package** (all data related to discovery settings and device information) or from the following list of .csv downloads:

- Consumables
- Counters
- Firmware
- General
- Alerts
- Job logs

5 Select **Browse**, and then select the file path.

6 Select **Export**.

Viewing collected devices data

1 In the Data Collection Tool, select **Collected data**.

2 In the View menu, select one from the following views:

- Alerts
- Consumables
- Counters
- Firmware
- General
- Job logs
- Summary (shows the chart diagrams of the collected devices data)

3 In the Filter view, select search criteria.

The Filter view has several view options with different criteria. The table below lists them.

View	Search filter criteria		
Alerts	Brand name	IP Address	Alerts count
	Model name	Status	
Consum-ables	Brand name	Status	Cyan
	Model name	Toner information	Magenta
	IP address	Black	Yellow
Counters	Brand name	Status	Single color total printed pages
	Model name	Total printed pages	Full color total printed pages
	IP address	Black & white total printed pages	Total scanned pages
Firmware	Brand name	Firmware version	Panel firmware
	Model name	Scanner firmware	NIC firmware

View	Search filter criteria		
	IP address	Fax firmware (port 1)	
	Status	Fax firmware (port 2)	
General	Brand name	MAC address	Panel message
	Model name	System location	Asset number
	IP address	Device type	Sleep timer (minutes)
	Status	Color support	Low power timer (minutes)
	Serial number	Print speed (ppm)	System up time
	Host name	Memory size (MB)	Sleep level
Job logs	Brand name	Status	Send jobs
	Model name	Total jobs	Storage jobs
	IP address	Print jobs	

33 System connections

System connections covers meter exports and connection settings for an external server. The connection settings include your credentials for the external server, dealer id, and database instance. The templates let you specify the counter contents of meter exports. In addition to counter selection, you can edit the counter labels when creating the template.

System Administrators and Managers create and use the templates with meter export schedules for collecting meter readings from select devices. The meter readings exports are in a .csv format and can be downloaded .zip packages. With Meter export download, you can save meter export files to your computer. The export files contain cumulative counters as selected for Function, Paper size, Duplex, Multiple pages per sheet, Scanned, Life count, Usage, and Other. The counter availability varies by device.

Connection settings

Connection settings lets you specify the information and credentials necessary to connect to an external system. After you add the connection settings, you can test the connection within the Add Connection Setting wizard or select **Connection test** in the toolbar. In addition to the connection settings, you must choose your sync by asset number, which determines how the server identifies devices. You must also set the number of days before a non-reporting device is no longer included in reporting. To finish the setting, you must know your credentials for the external server, Database instance, Dealer ID, and Meter source.

Creating connection settings

You can create connection settings to an external system. If you are replacing existing settings, select **Clear** before adding the new settings.

1. In the Administration view, select **System connections**.
2. Select **Connection settings**.
3. In the Group name list, select a group based upon your permissions and your role.
4. Enter a **Name** and an optional **Description**.
5. Select **Next**.
6. Enter your credentials for the external system in **Authentication ID**, **Authentication password**, and **Database instance**.
7. For Sender information, enter your **Dealer ID** and **Meter source**.

8. Select **Connection test** if you want to check the settings with the external server.
9. Select **Close** after the connection test results are displayed.
10. Select **Next**.
11. For Sync by, only the Asset number is available. It determines how the external server identifies the devices.
12. For Device stale days, select the number of days that a device has not sent counters or information to KFS.

    The range is from 1 to 1000 days. The setting ensures that non-reporting devices are excluded from scheduled exports.
13. Select **Finish**.

Clearing connection settings

You can clear connection settings to an external system.

1. In the Administration view, select **System connections**.
2. Select **Connection settings**.
3. In the Group name list, select the group based upon your permissions and user role.
4. Select **Clear**.
5. Select **OK**.

Editing connection settings

You can edit the connection settings to selected external systems.

1. In the Administration view, select **System connections**.
2. Select **Connection settings**.
3. In the Group name list, select the group based upon your permissions and user role.
4. Select **Edit**.
5. Modify the **Connection settings**.
6. After you finish making changes, select **Finish**.

Testing the connection settings to an external system

1. In the Administration view, select **System connections**.
2. Select **Connection settings**.
3. In the Group name list, select the group based upon your permissions and user role.
4. Select **Connection test**.
5. Review the results and select **Close**.

Viewing meter export details

1. In the Administration view, select **System connections**.
2. In Meter exports, select **History**.
3. In the Group name list, select the group based upon your permissions and your user role.
4. Select the meter export.
5. Select **Details**.
6. Select **Summary** to show an overview of the meter export.
7. Select **Device results** to display the meter export results by device.

Filtering and searching for meter export history

1. In the Administration view, select **System connections**.
2. In Meter exports, select **History**.
3. In the Group name list, select the group based upon your permissions and user role.
4. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option.

   The following items use predefined values:

   Timestamp (Later than), Timestamp (Recent)

   24 hours, 7 days, 14 days, 30 days

   Result

   Successful, Partial, Failed

5 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Downloading meter exports

You can download Meter exports as separate files (.csv format) in one .zip download. The filename is generated using ExportResult and the timestamp.

1 In the Administration view, select **System connections**.

2 In Meter exports, select **History**.

3 In the Group name list, select the group based upon your permissions, user role, and the availability of historical meter exports.

4 Select the meter exports.

5 Select **Download**.

Meter export templates

With Meter export templates. you can specify the counter contents of Meter export downloads. In addition to selecting the counters, the template provides the option for editing counter labels. System Administrators create the templates to work with Meter export schedules for collecting meter readings from select devices. The meter readings can be downloaded in a.csv format. In the Meter export download, you can view the selected counters for Function, Paper size, Duplex, Multiple pages per sheet, Scanned, Life count, Usage, and Other. The available counters vary by device.

Viewing meter export template details

1 In the Administration view, select **System connections**.

2 Select **Templates**.

3 In the Group name list, select a group based upon your permissions and user role.

4 In the templates list, select the information icon of a template to display the following information:

- Template name
- Description
- Counter labels
- Created by
- Last update
- Updated by
- Reference

5 Select **Close**.

Filtering and searching for meter export templates

You can filter and search for Meter export templates within a specified category by using keywords or selecting from a predefined set of values.

1 In the Administration view, select **System connections**.

2 Select **Templates**.

3 In the Group name list, select the group based upon your permissions and your user role.

4 In the Search drop-down list, select a search category, and then enter a search string or select a predefined option.

The following items use predefined values:

Last update (Later than), Last update (Recent)

24 hours, 7 days, 14 days, 30 days

5 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Creating meter export templates

1 In the Administration view, select **System connections**.

2 Select **Templates**.

3 In the Group name list, select the group based upon your permissions and user role.

4 Select **Add**.

5 Enter the **Template name** and **Description**.

6 Select **Next**.

7 Select or clear the counters to be included in the export.

8 Select **Next**.

9 For Edit counter labels, rename column headers.

10 Select **Finish**.

Editing meter export templates

1. In the Administration view, select **System connections**.
2. Select **Templates**.
3. In the Group name list, select the group based upon your permissions and user role.
4. Select a **Meter Export Template**.
5. Select **Edit**.
6. Edit the **Template name** and **Description**.
7. Select **Next**.
8. Select or clear the counters to be included in the export.
9. Select **Next**.
10. For Edit counter labels, rename column headers.
11. Select **Finish**.

Deleting meter export templates

1. In the Administration view, select **System connections**.
2. Select **Templates**.
3. In the Group name list, select the group based upon your permissions and user role.
4. Select the templates.
5. Select **Delete**.
6. Select **OK**.

Meter export schedules

Use Meter export schedules to specify a Meter export template and source groups for the collection of meter readings from select devices based on a schedule. During the schedule creation, you can create a new template, select from existing templates, or select and edit existing templates.

Viewing meter export schedule details

1. In the Administration view, select **System connections**.
2. Select **Schedule**.
3. In the Group name list, select a group based upon your permissions and your user role.
4. In the schedule list, select the information icon of a schedule to display the following information:
   - Name
   - Template name
   - Connection setting
   - Source
   - Frequency
   - Last run (result/time)
   - Scheduled next
   - Created by
   - Last update
   - Updated by
   - Status
5. Select **Close**.

Filtering and searching the meter export schedules

1. In the Administration view, select **System connections**.
2. Select **Schedule**.
3. In the Group name list, select the group based upon your permissions and user role.
4. In the Search drop-down list, select a search category, and then enter a search string or select a predefined option.

   The following items use predefined options:

   Status

   Enabled, Disabled, Warning

   Schedule results

   Failed, Successful, On hold, Processing, Partial

   Timestamp (Later than), Timestamp (Recent), Next run time (Earlier than), Next run time (Later than), Last update (Later than), Last update (Recent)

   24 hours, 7 days, 14 days, 30 days

5 Select the search icon.

Select x in the Search box to clear the search value and restore the view to the original list.

Creating meter export schedules

You can create schedules for Meter exports. Schedules use templates and are group specific. Within the scheduling feature, you can modify existing templates or create new ones.

1 In the Administration view, select **System connections**.

2 Select **Schedule**.

3 In the Group name list, select a group based upon your permissions and user role.

4 Select **Add**.

5 Enter a **Name** (64 character maximum).

6 Select a **Connection setting** in the drop-down list.

7 Select **Next**.

8 Select a **Meter export template** in the list or enter the name of an existing meter export template in the Search text box, press **Enter**, and select the Meter export template.

As an alternative template selection method:

a) Select **Edit** to modify an existing template.
b) Select **New template** to create settings for your new template.

9 Select **Next**.

10 Use Quick select to display groups based on the following selections:

Exclusively managed

All child groups but not delegated groups under them.

All accessible

All child groups and the delegated groups under them.

Off

No filter for the group.

11 In Search, enter a group name then use the up and down arrows to move between instances of the search term in the hierarchical structure.

The number of occurrences of the search term is also displayed.

12 Select the Groups in the Source list.

13 Select **Next**.

14 Select a **Frequency**.

On scheduled intervals
Daily, Weekly, Monthly

At scheduled time
Date and Time

On demand
Immediately

15 Select **Next**.

16 Review the Summary, and then select **Finish**.

Running meter export schedules

1 In the Administration view, select **System connections**.

2 Select **Schedule**.

3 In the Group name list, select the group based upon your permissions and user role.

4 Select the schedules.

5 Select **Run**.

6 Select **Close**.

Editing meter export schedules

1 In the Administration view, select **System connections**.

2 Select **Schedule**.

3 In the Group name list, select the group based upon your permissions and user role.

4 Select the schedule.

5 Select **Edit**.

6 Make the changes and select **Finish**.

Changing meter export schedule status

You can change the status of schedules for Meter exports. The Disable setting prevents a meter export schedule from being run. The schedule status can be enabled (green), disabled (gray), or warning (yellow). A schedule cannot run under a warning condition.

1 In the Administration view, select **System connections**.

2 Select **Schedule**.

3 In the Group name list, select the group based upon your permissions and your user role.

4 Select the schedules.

5 Select **Change status**.

6 Select **Enable** or **Disable**.

Deleting meter export schedules

1 In the Administration view, select **System connections**.

2 Select **Schedule**.

3 In the Group name list, select the group based upon your permissions and user role.

4 Select the schedules.

5 Select **Delete**.

6 Select **OK**.

For the KYOCERA contact in your region, see Sales Sites sections here:
ご利用の地域でのお問い合わせ先については、下記リンクから京セラ本支店・営業所の一覧をご覧ください。
https://www.kyoceradocumentsolutions.com/company/directory.html

KFSUGKDEN180.2020.05