
# Security White Paper

Version 1.7
(November, 2018)

**- FOR KYOCERA CUSTOMERS ONLY -**

## CONTENTS

**PDF Navigation Tips**

**Internal Link**: [Ctrl] + Click *Contents* page or internal links (underlined text) to go to that page. To return to page you were on, press [Alt] + [←].
**External Link**: Click URL to open webpage.
**Search**: Type the word in [Find] textbox, and press [Enter]. Press right arrow [▶] to move to next occurrence.

### Target Audience

This white paper is intended for Kyocera customers, and other stakeholders, who are interested in learning how KYOCERA Fleet Services (KFS) can benefit their organization. Security of information assets handled by KFS is discussed throughout this document, as this is of paramount importance to both Kyocera and our customers.

### Version Notice

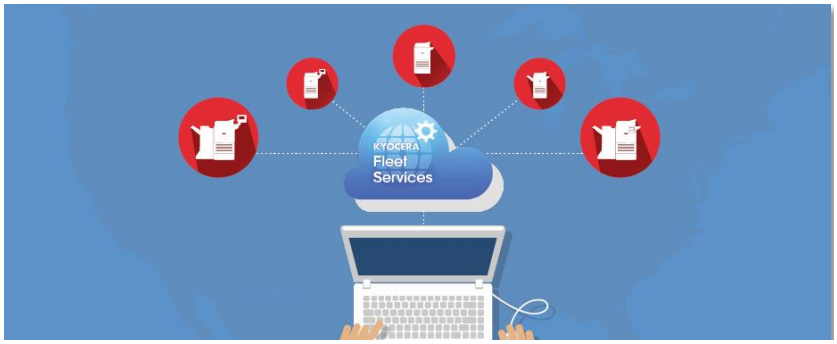
KFS is constantly evolving, so changes to system functionality may be incorporated into later versions of this white paper, without prior notice.

## Introduction

In today's networked office environments remote management of printers and multifunctional products (MFPs) is more cost effective than ever before. Advanced software tools capture device metrics by leveraging the World Wide Web. From a laptop or workstation, service providers have real-time visibility into exactly how a fleet is operating, locally and/or globally.

Why is remote device management important? Harnessing the continuous flow of usage data is a proven way to optimize fleet uptime and dramatically increase workgroup productivity. Furthermore, the intelligence gathered from device metrics enables a service provider to quickly respond to their customers' present and future technology needs.

Prior to widespread use of the Internet, device monitoring was an expensive proposition; a dedicated telephone line to each device and proprietary server software was required. Fast forward to the 21st Century and cloud-based solutions eliminate costly on-premises installation by sharing "on-demand" resources over the internet. Versatile, reliable and secure cloud-based solutions are now commonplace, such as Dropbox, Google Drive™, Apple® iCloud®. These file sharing and storage services offer anytime, anywhere access to valuable information assets.




Adoption and implementation of KYOCERA Fleet Services (KFS) offers our customers the same opportunity to utilize a state-of-the-art cloud platform, where extensive device analytics and controls streamline every aspect of fleet management. But how will this information benefit your organization? Is the system secure? This white paper answers these questions, and many others, so you can make an informed decision regarding KFS deployment within your organization.

## What is KFS?

KFS is a cloud-based device monitoring system that is based on the Software as a Service (SaaS) model. With this solution delivery method, there is no software or network infrastructure investment required. Instead, secure cloud services provide the tools for KFS service providers to centrally control devices, everything from device installation and configuration to reporting and troubleshooting. KFS' powerful suite of utilities enables proactive management of Kyocera and non-Kyocera devices alike, from any computer or smartphone with web browser capabilities. Designed with sophisticated security protocols and policies in place, KFS communication pathways are fully protected.

### Proactive Service Model

Implementation of KFS establishes a "proactive" versus "reactive" service model. Key to a proactive model is KFS' support for email notifications that alert technicians to a device event, system error, toner level/order or page counts (triggered by the device). The event is described in the email, to enable swift resolution. For example, rather than an end-user requesting service (reactive), the notified technician calls a key contact (proactive). If a technician is dispatched, they are equipped with the necessary replacement parts and/or consumables.

By more efficiently utilizing human resources, you maximize device uptime, reduce workflow interruptions and reduce the frequency, duration and cost of on-site service calls; in many cases, service issues are resolved over the phone. Using KFS, valuable device usage insights are gained, enterprise-wide efficiencies are realized, and service-level response objectives are met.

## How KFS Works

KFS collects device status and usage data over a secure connection established between the device and KFS Manager. KFS Manager is the backbone of KYOCERA Fleet Services, and relies on the Microsoft® Azure® cloud system. As the control center for key system features, KFS Manager's intuitive web interface enables a service provider to…

- Register and manage users and device groups
- Establish configuration settings
- Check consumable levels
- View real-time device status
- Perform maintenance/diagnostics/troubleshooting
- Restart (reboot) devices
- Upgrade firmware and manage firmware packages
- View device counters and properties
- Generate list and graphical reports

### Hosting Environment

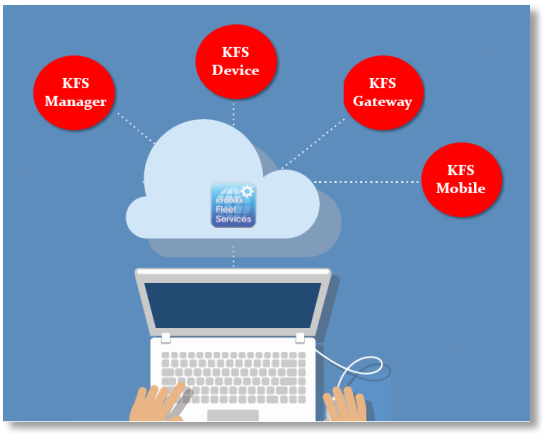
KFS Manager is hosted on Microsoft Azure, a cloud-based platform that provides a highly-secure server* infrastructure to manage KFS applications; Azure was chosen based on Microsoft's industry-leading commitment to the protection and privacy of data.

Microsoft was the first major cloud provider to adopt the new international cloud privacy standard, ISO 27018. In addition to offering multiple layers of security, Microsoft Azure provides complete isolation from all other networks; traffic only flows through customer-configured paths.

**Servers are located in the United States*.

## KFS Components

There are four KFS components – KFS Manager, KFS Device, KFS Gateway and KFS Mobile. While each component plays multiple roles within the KFS system, collectively they have one primary purpose…to provide the information and tools needed to keep a printer fleet running smoothly. To that end, these components enable service providers to optimize operation of Kyocera and non-Kyocera digital imaging systems.




### KFS Manager

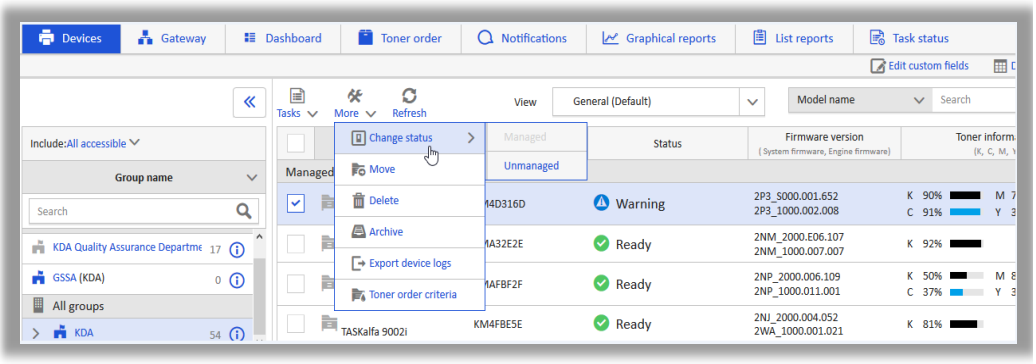
As noted, KFS Manager is the web-based user interface, accessible from a Web browser, that enables remote management of networked printers/MFPs. This component links to KFS Device, KFS Gateway and KFS Mobile and, as such, is considered the backbone of the KFS system.

- Register/unregister/restore device groups; each device is assigned to a group.
- Create user accounts and assign roles, depending on tasks to be performed.
  ***Note***: There are four user roles, Manager, Service, Analyst and Customer.
  ***Important***: Only authorized users can view Device Logs, Counters and Consumables.
- Perform many tasks, such as Notifications, Maintenance, Restart, Reports, Logs, etc.
- Establish communication preferences for all tasks.

### KFS Device

KFS Device is firmware built into the Kyocera printer/MFP that enables communication with KFS Manager and KFS Mobile.

- Sends device logs, counters and status pages to KFS Manager, based on preset requests and schedules.
- Sends device information to KFS Mobile via Bluetooth®, USB or Wi-Fi Direct.
- During device set up, the technician enters the Server Registration URL and Access Code for the applicable group (on the machine); the unit initiates communication with KFS Manager. You can then add the device to KFS Manager's Devices page.



## KFS NetGateway

KFS Gateway is a Windows® application installed locally and used to register two types of devices with KFS Manager–legacy Kyocera devices and third-party devices.

- The secure .NET platform is utilized providing improved registration of devices. Currently JAVA Gateway is also supported.
- Serves as the link between devices and KFS Manager.
- Communicates counters and toner information to KFS Manager.
- Supports remote device maintenance features, including Snapshots and Reports, as well as device tasks, e.g., device restart.
- Supports Device Registration Diagnostic (DRD) Tool for network discovery of devices.
- For USB-connected printers, the Local Agent tool is installed on a PC, enabling the Gateway to find those devices.

***Note***: KFS Gateway is available for download in KFS Manager.

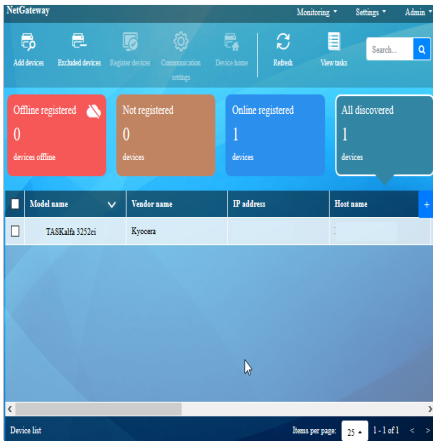



*Fig. 2: KFS NetGateway / Preferences*

## KFS Mobile

KFS Mobile is used to register, collect and upload device data to KFS Manager via a smartphone or tablet.

- You log in to KFS Manager to view device information/ logs, register/unregister devices, capture/upload Snapshots from the device and initiate firmware upgrades.
- Used when KFS Device/KFS Gateway cannot connect to your network, e.g., when monitoring off-line devices, such as USB-connected printers/MFPs.
- Uses peer-to-peer communication, such as Bluetooth and USB, to obtain device information.
- Supports iOS and Android platforms.

## KFS Features

The KFS system's core features are divided into three categories: Monitoring Tools, Management Tools and Other Tools.

***Note***: Feature support depends on whether the device is KFS-ready (Kyocera brand), legacy Kyocera (non-KFS ready) or third-party (different brand). KFS-ready devices support the full range of KFS remote management and monitoring tools. Legacy and third-party devices can be monitored; basic information, such as counters and consumables, is polled from the device's Management Information Base (MIB).

### Monitoring Tools

Monitoring Tools allow you to access real-time information regarding connected devices, e.g., supply status, counters, reports, logs, maps, etc.

Click on any Monitoring Tool listed below to go directly to that section.



#### Dashboard

Dashboard is a key feature of KFS Manager that allows you to view trends in activities, errors, and consumables within a fleet. Across a selected time range (e.g., 24 hours, 7 days, 14 days, 30 days), you can view and analyze different types of data, from Scan and Print volumes to toner levels. This enables you to optimize device uptime, reduce help desk calls and proactively identify gaps.

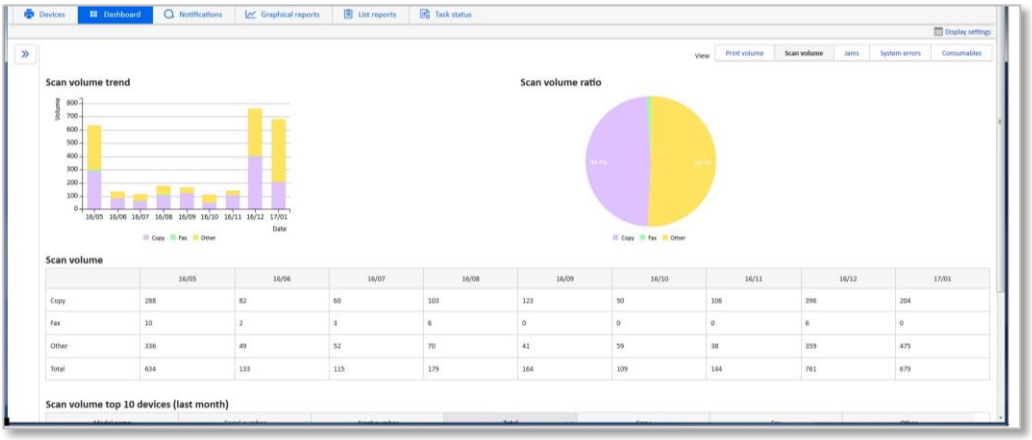



*Fig. 3: KFS Manager Dashboard*

For instance, Scan and Print volumes on one device may exceeds the recommended monthly volumes for that unit. This enables right-sizing, where devices are matched to throughput requirements.

## Counters

From the Counters screen, you can view the following printed-page information:

- Serial number
- Model name
- Function
- Black & White pages
- Full-color pages
- Two-color pages
- Single-color pages
- Total scanned pages

***Note:*** Device counters are automatically polled by KFS Manager up to four times per day; once per day is the default.

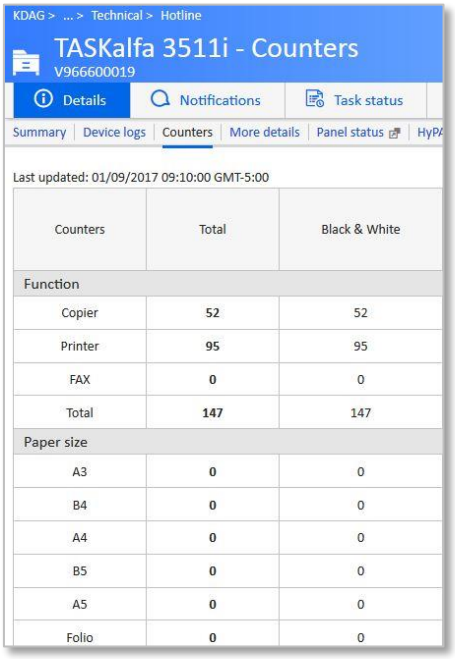



*Fig. 4: Device Counters*

## Device Logs

View all system events in list form, to easily determine fleet status. If there is an error condition, the Description field provides guidance to help resolve the issue.

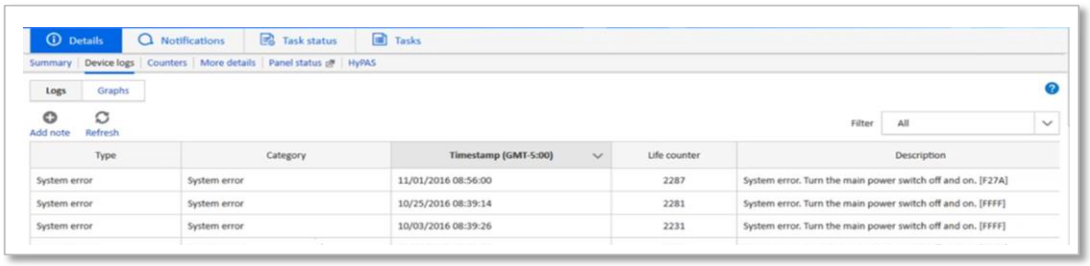



*Fig. 5: Device Logs*

## Email & Audit Logs

- 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 can check emails sent to users about specific KFS events, such as user registration.
  ***Note***: Email logs are stored for three (3) months.
- Audit logs contain operations history for selected Delegated groups. The Audit log list contains a timestamp, type of operation, result of operation, email address and user name of the individual who performed the operation. Additional details are available, e.g., IP address of user who performed the operation, user role within KFS, etc.
  ***Note***: A maximum of 10,000 logs is supported. You can download logs from KFS to your computer as CSV files.

## Reports

Build graphical or list reports to view color usage, page volume, toner levels, etc. When generating reports, there are over 30 templates to choose from. Run reports on a scheduled or periodic basis.

- **Counters**: Create reports for Counter and Print volume for chargebacks. Reduces administrative costs and errors that are possible with manual counter reporting.
- **Consumable Management**: Create reports with simple predictions of the replacement timing of consumables and remaining levels.
- **Status Check** (preventative maintenance): Create reports with error statistics.
- **Usage Analysis**: Create reports that show usage to help identify over- and under-utilized systems, providing guidance on unit replacement/redeployment. This ensures that the fleet meets each workgroup's application and volume needs (load balancing). With historical usage data, estimates on toner usage can be anticipated across the entire fleet. ***Note***: If preset thresholds are met, and Toner Order is enabled, an alert for low toner (on the Toner Order Page) will be indicated. This notification prompts the user to review and place an order via email, thus helping to ensure uninterrupted workflow.

***Note***: A toner replacement forecast for Kyocera-brand toners is available when toner has been replaced at least three times or there is at least three months of historical data. The calculation for the forecast is made within the last five days, and the predicted date of replacement is within 10 days of the actual date. Once a forecast is available, it will be updated only after new information from the device is available. If no updates are received from the device, the forecast will not change.

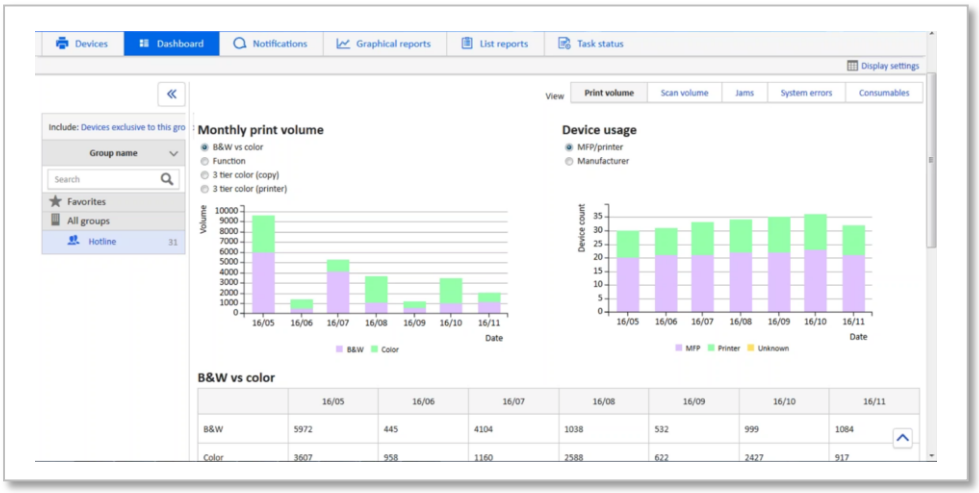



*Fig. 6: Dashboard Graphical Reports*

## Device Properties

From the Details screen, you can view the following Device Properties:

- Manufacturer
- Model name
- Installed accessories
- Asset number
- Firmware versions
- Toner information
- Status
- Network addresses
- Connection status

***Note***: Display of Device Properties is customizable, so you can view the desired information, and place in chosen order.

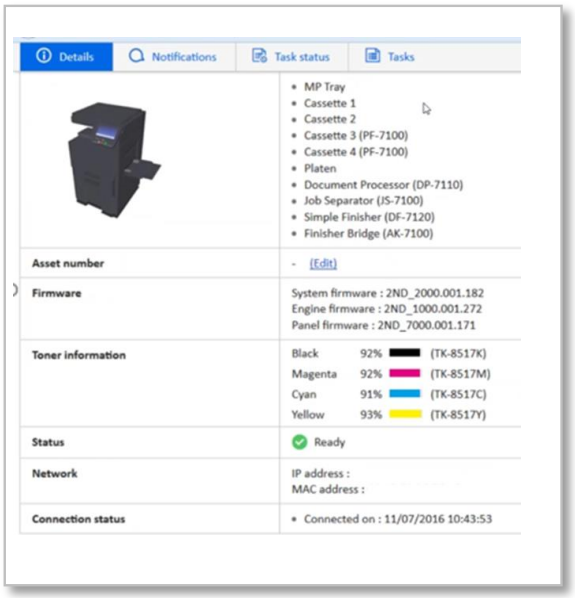



*Fig. 7: Device Properties*

## Panel Status

Viewing Panel Status is another helpful troubleshooting tool that enables a technician to determine exactly what the device's display indicates (in real-time), and if any alerts require attention.

- Multiple users can view panel status at the same time.

***Important***: When a HyPAS task is active on the device, you cannot perform the following operations:

- Panel Note
- Panel Screenshot
- Firmware Upgrade
- Maintenance Mode
- Restart
- Send File
- Snapshots
- Data Capture

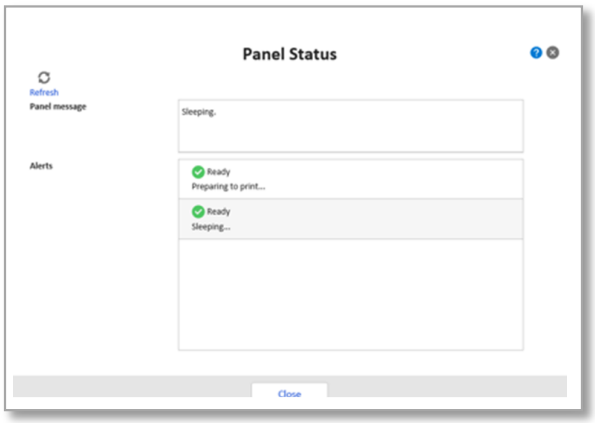



*Fig. 8: Panel Status*

## Notifications

Automatic email Notifications are sent for a System error (service code), Event (e.g., paper misfeed), Counters, and/or consumable levels.

- Toner notification can be displayed in number of days remaining, as well as a percentage value.
- Fast event resolution saves time and money.
- Proactive consumable management and ordering prevents unnecessary workflow interruptions.
- Retrieval of counters can be scheduled, for example, on the first day of every month at 7:00 a.m. The task is completed without user intervention.

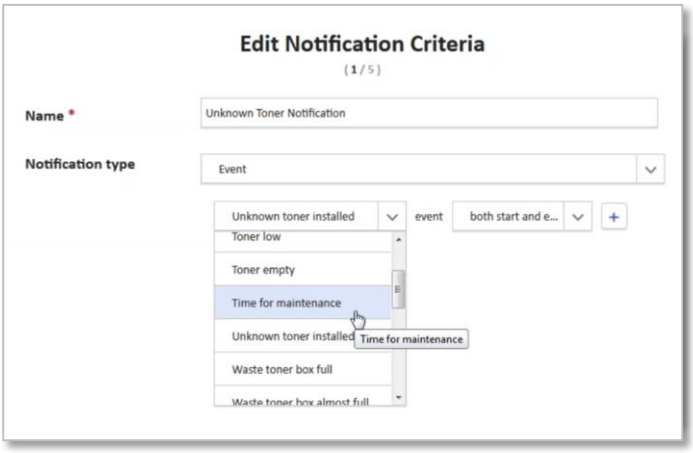



*Fig. 9: Notification Settings*

## Maps

Maps provide a graphical representation of the location of users and devices within a physical area, allowing you to visualize device location and system status on a map.

- Simplifies asset identification, tracking and management.
- Add up to 13 different icons to show where devices, users, physical locations and links are positioned on the map; links take you to another map in the same device group.
- Include descriptions for each printer/MFP and search for the device, as needed.
- Import maps from a variety of formats, e.g., JPG, TIFF, PNG, and BMP.
- Export maps in PDF format.
- Create up to 100 maps per group; choose one map as your default view.

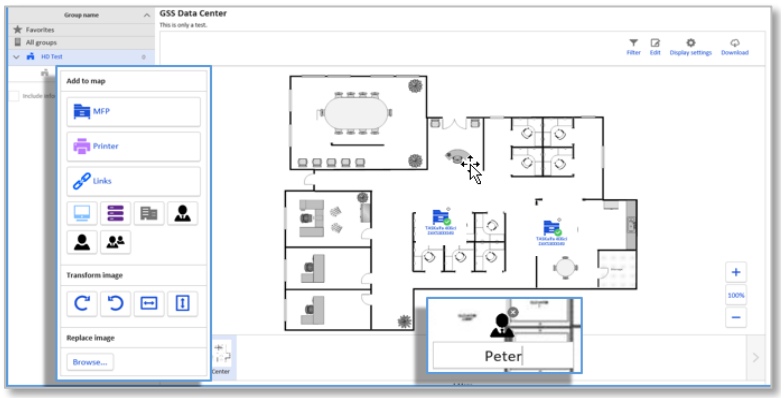



*Fig. 10: Device/User Map*

## Management Tools

Management Tools allow the service provider to control many facets of fleet operation, for instance, establish configuration settings, perform firmware upgrades, remotely restart machines and much more. These features are available for all KFS-ready Kyocera devices.

Click on any Management Tool listed below to go directly to that section.



### Device Settings

Device Settings automate configuration tasks, to meet customers' requests and approvals.

- Change device settings, e.g., default all units to duplex printing (print cost savings), 300 dpi scan resolution (smaller file size), etc.
- Saved settings can be applied to multiple devices (in same model series), immediately or on a scheduled basis.
- Upload and download settings, as needed, to keep fleet configuration consistent and current.

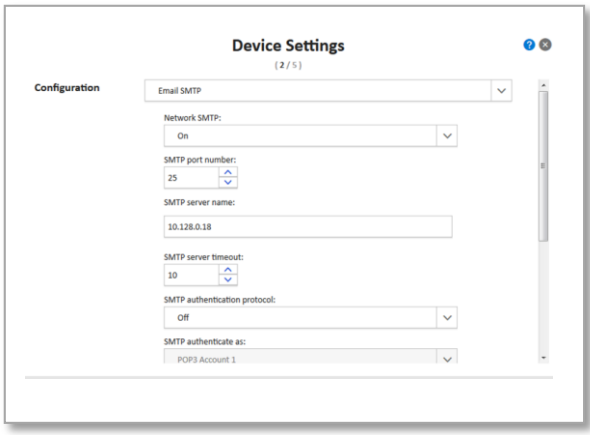



*Fig. 11: Device Configuration*

### Device Restart

A single device or group of devices can be restarted. For easier fleet management, the restart can set up on a scheduled basis. Should an error occur, for example, in a print queue this function reboots the device.

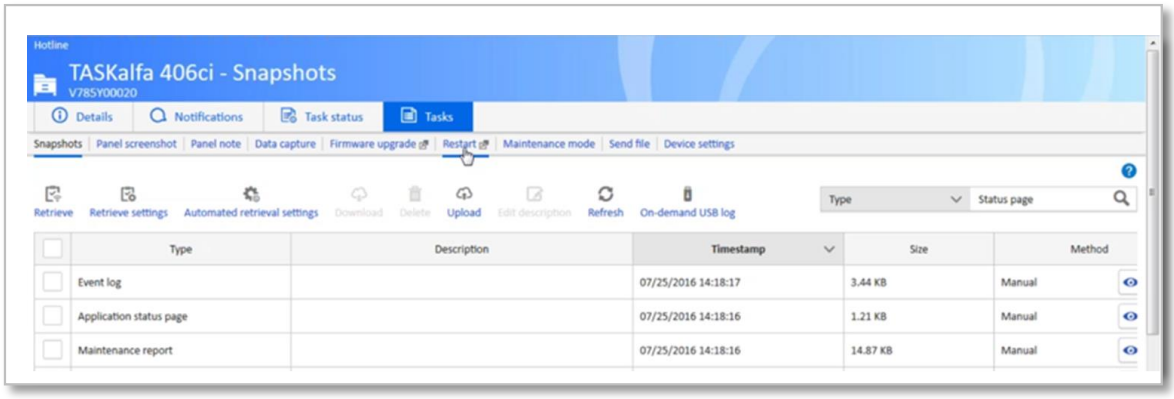
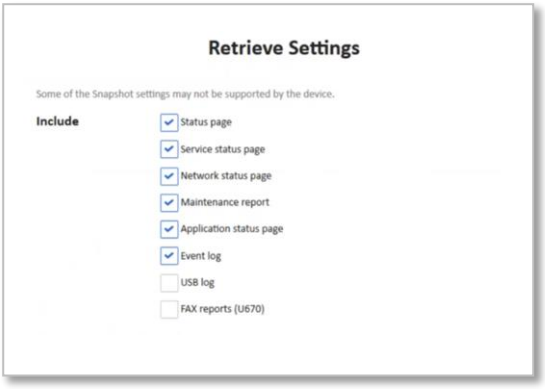



*Fig. 12: Device Restart*

## Snapshots

Snapshots show the current state of the device and can be retrieved automatically or manually.

- Retrieve Snapshots from one or more devices.
- View, download and delete multiple Snapshots directly from KFS Manager.
  ***Note***: KFS Manager can store up to 100 Snapshots per device. Snapshots can be viewed in a variety of formats, e.g., JPG, PNG, GIF, TXT, XML and LOG.
- Capture Status page, Service status page, Network status page, Maintenance report, Application status page, Event log, USB log and FAX reports.
- Prepares technician with the necessary replacement parts/consumables.
- Snapshot data can be retrieved via KFS Device, KFS Gateway and/or KFS Mobile.




***Important***: After a device is installed, the technician will run a Snapshot of the Service status page. This information can assist in future troubleshooting, as initial settings can be referenced.

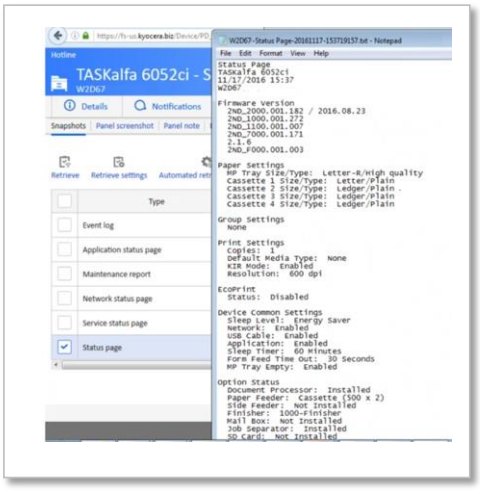



*Fig. 13: Snapshot Data in Notepad*

## Remote Operation Panel

KFS Remote Operation Panel allows your service provider to connect to your device through KFS and operate the Display Panel in real-time. You can be guided through custom job settings and specific device configurations, like media settings per paper drawers. All functions can be operated as if your servicing agent was standing with you in front of your device. Additionally, you can take advantage of personalized training while at the display and learn how to use all the device features available to you. All Remote Operation Panel sessions must have your permission in order to proceed, ensuring your device security.

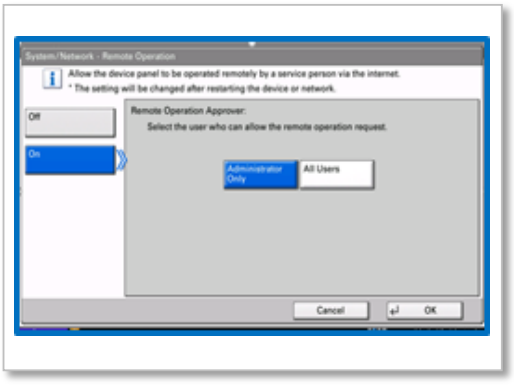



*Fig 14: Remote Operation Panel*

## Panel Screenshot

Panel screenshot is a troubleshooting tool that allows you to remotely capture an image of a target device's display panel.

- Determine device status in real time.
- Provide guidance to users over the phone, e.g., when changing settings on a machine.
- Maximize uptime by reducing the need for on-site service.

***Important***: A confirmation request displays on the device panel, which must be accepted in order for capture to take place. No other KFS functions are available for the device during a Panel screenshot.

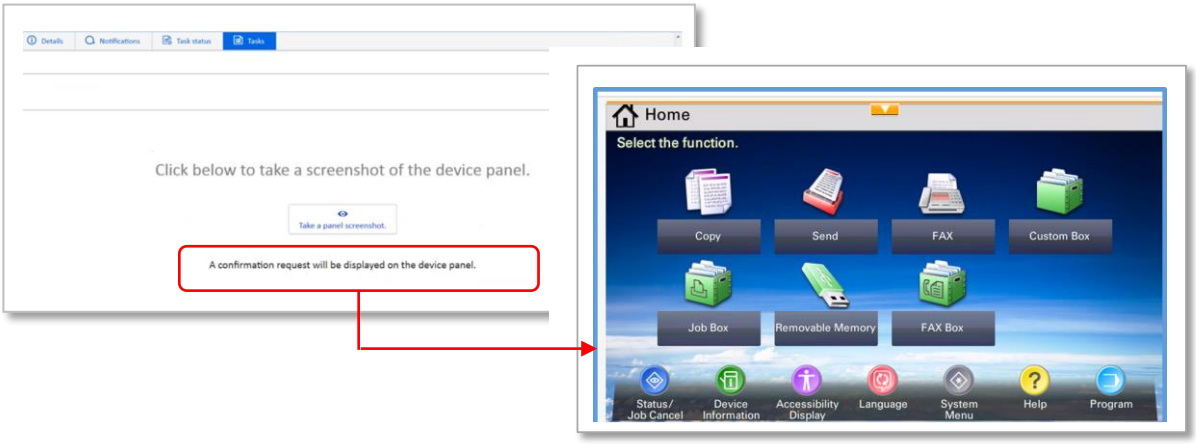



*Fig. 15: Panel Snapshot*

## Panel Note

This function enables your service provider to post messages on the display panel of the remote device.

- You can be notified of upcoming service activity, supply shipments and/or firmware updates.
- The panel note can be set to display on the device once or at regular intervals.
  ***Note***: A 30-minute or 1-hour interval is recommended, to ensure all users are informed of the upcoming activity.

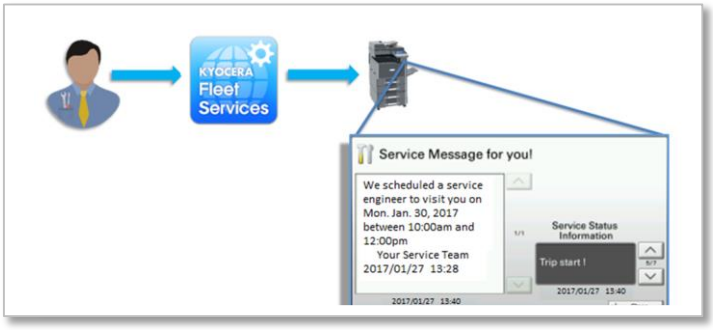



*Fig. 18: Panel Note*

### Send File

This troubleshooting feature enables your service provider to send a test file to one or more remote devices, immediately or on a scheduled basis.

### Data Capture

Data capture provides printable data from a registered device to be retrieved for troubleshooting purposes. In the past, diagnosis of print-related issues was done manually, via USB drive carried to and from your account, a time-consuming and costly process.
***Note***: If the 15 MB Data capture is exceeded, the excess data is discarded. A maximum of 10 printable files can be saved per device, for 1 to 7 days after capture. When the specified time period is reached, the captured data is automatically removed.

***Important***: Data capture is only possible with IT administrator approval, in advance, and after the confirmation message displayed on the device panel is accepted; no data is retrieved without multiple levels of on-site authorization.

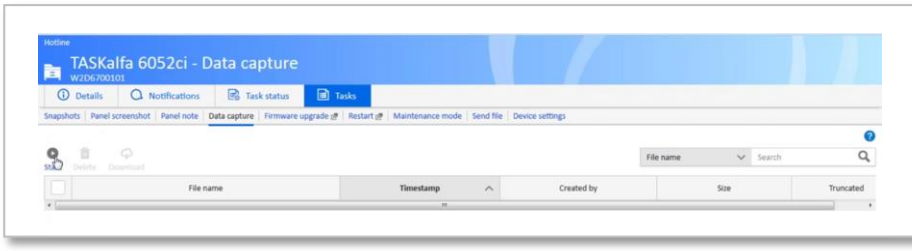



*Fig. 16: Data Capture*

### Firmware Upgrade

Periodic firmware updates are necessary to optimize device performance. Firmware packages are stored in KFS Manager, thus available for remote upload to connected devices. Remote updates save a significant amount of time and money, over a technician manually updating devices on-site (via USB drive).

- Supports batch firmware upgrades (of devices in same model series).
- There are no workflow interruptions; upgrades can be scheduled for a later date/time, e.g., during off-peak hours.

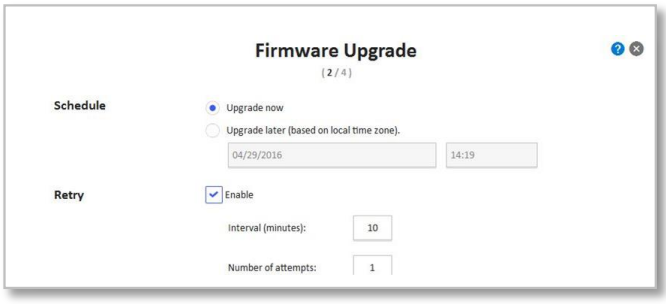



*Fig. 17: Firmware Upgrade*

### USB Logs

KFS Device generates USB logs and sends them to KFS Manager, where they are stored. You can download the USB logs to a PC from KFS Manager via a Snapshot list.

***Note***: On-Demand USB logs can only be retrieved on-site with your approval. While retrieving logs, the device will be locked for 3 to 4 minutes. After retrieval ends, the device will automatically be restarted. After device restart, the USB logs are automatically downloaded to the user's PC from KFS Manager.

### Enable/Disable Device Features

Specific device features can be enabled/disabled by user group. Prohibited features, e.g., color copying/printing, are grayed out so the function cannot be accessed.

- Controls costs and prevents information leaks, without impacting ease of use.

### Toner Order

Criteria can be set for an alert to display in the Toner Order View, when preset thresholds are met, e.g., toner level or number of days. A key operator can then email their service provider for replacement toner. This enables toner to be on hand *before* it is depleted, maximizing device uptime.

Service providers have the ability to…

- Set thresholds per group.
- Set thresholds per device (overrides settings per group).
- Set criteria for individual toner cartridges, if applicable.
- View current toner levels.
- View toner history in graphical form.
- Check if toner ordering is Recommended, Optional or Not Applicable.

### Address Book Import/Export

Corporate address book data can be retrieved by the KFS system. For instance, if an MFP is being replaced, the address book data from the old device can be imported to the service provider's computer. It is then exported to the newly-installed device, saving a significant amount of time over manual entry. Note that system security measures require that a key operator (at the customer site) accept a confirmation message on the device control panel prior to import.

The KFS system does not store address book data; KFS is just the conduit between the device and service provider. The data is retained by the service provider, who can also perform on-going address book updates, if requested. This is helpful when employee changes occur, as the updated address book can be remotely pushed to any location or department.

***Note***: Also see KFS Feature Summary by Component.

## Other Tools

Other tools integrate with KFS, providing you with added system flexibility.

### E-Automate

KFS integrates with E-Automate, a service management tool that enables service providers to migrate meter counts from KFS directly into their billing system. Counts can be collected at a scheduled interval, time or on demand, ensuring accurate billing cycles. And since there's no customer intervention required, either by phone or mail, employees can focus on more important tasks at hand.

### CRM Integration

You can import Customer Relationship Management (CRM) data into the KFS Manager database from a CSV file. KFS Manager matches registered devices in the CRM data according to the device Serial number (in the KFS database) and updates the Asset number in KFS Manager.

### Data Collection Tool (DCT)

DCT allows KFS sales professionals and service providers to perform a quick fleet assessment by capturing device IP addresses, serial numbers, brand name, MAC address, etc., without the need to install software.

The DCT application is installed on a USB drive and can discover Kyocera and third-party network devices. Once collected, device data are presented in a summary view. With this information, sales teams can demonstrate the breadth of KFS functionality to current and prospective customers.


*Fig. 18: Data Capture Tool Summary*

### Device Registration Diagnostic (DRD) Tool

The DRD tool provides one-click registration of up to 100 network printers/MFPs* to KFS Manager. Device registration is typically performed by an on-site technician who runs the DRD Tool from a USB drive inserted into a Windows PC or laptop. Features of the DRD tool include:

- Discovery of network printers/MFPs over SNMP
- Registration to KFS Manager (KFS-ready, legacy and non-legacy devices)

- Configuration of registration settings
- Firmware upgrade
- Device authentication
- Registration status check

**If more than 100 devices are in the fleet, the network can be searched by IP address range.*

- Diagnosis of issues with XMPP and Proxy settings, KFS authentication, as well as communication with the HTTP and XMPP servers

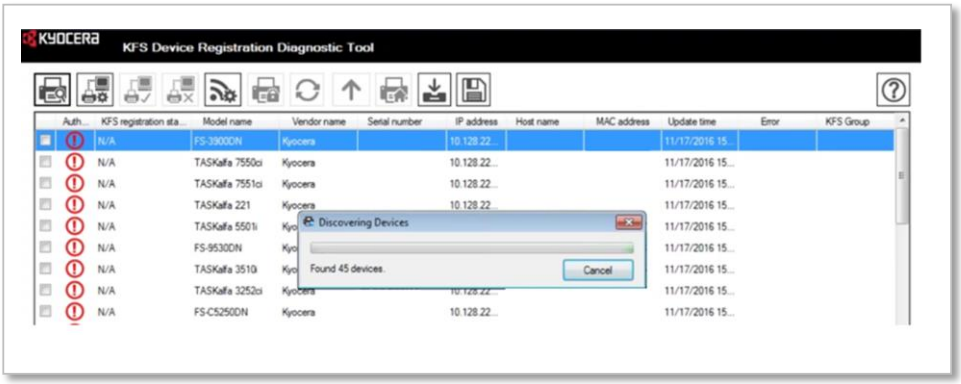



*Fig. 22: DRD Tool / Device Discover*

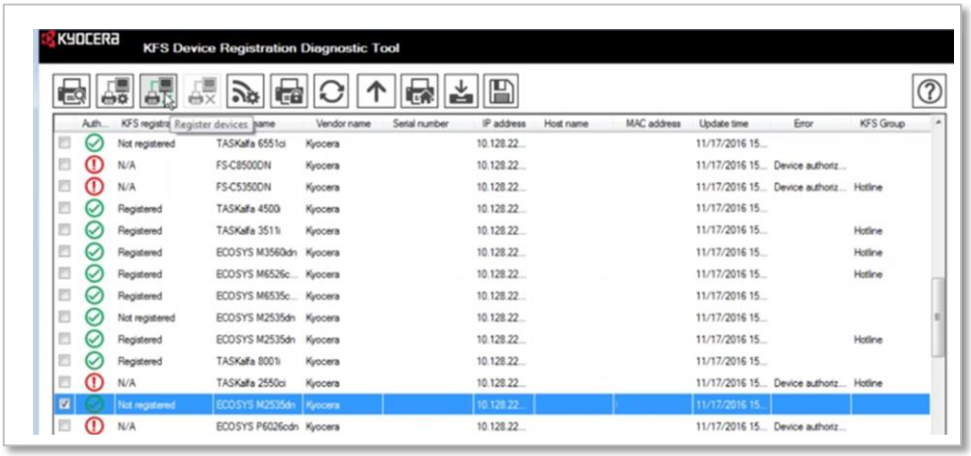



*Fig. 19: DRD Tool / Device List*

## HyPAS Application Management

KFS Manager enables your service provider to manage (Install, Uninstall, Activate & Deactivate) Kyocera's Hybrid Platform for Advanced Solutions (HyPAS) business applications. HyPAS is an open software development platform that supports custom application integration on Kyocera printers/MFPs. This enables the service provider to address your unique workflow requirements. For more information on Kyocera business applications, please visit Kyocera's website at: http://usa.kyoceradocumentsolutions.com.

## Security and Safeguards

In today's data-intensive workplace, protection of your valuable information assets is of paramount importance. To safeguard these assets, KFS employs a variety of robust security features that safeguard communication between KFS components and devices.



### Data Storage

Sensitive information assets stored in KFS components–KFS Manager, KFS Gateway, KFS Device and KFS Mobile–are encrypted with the following algorithms and bit strength.

| | |
|---|---|
| Encryption Algorithm: | Advanced Encryption Standard (AES) |
| Key Length: | 128-bit, 256-bit |

The sensitive information assets stored in KFS Mobile indicates, for example, user password of KFS Manager, refresh token for setting up a secure communication channel with KFS Manager, and password for proxy server authentication.

***Important***: Device data only contains information necessary for management and maintenance of the devices. It does not contain the customer's image data or personal information, such as address book.

### Data Communication

KFS encrypts communication data using HTTPS protocol, whether a user is accessing data via KFS Manager or data is being transferred between a device and other KFS components. HTTPS protects KFS communication data streams from masquerading, tapping or modification, as all KFS components are mutually authenticated.

KFS send and receives encrypted data to and from devices via the internet or local area network (LAN).

- **KFS Communication via Internet**
  KFS network communication is set up by XMPP server and KFS Manager in the cloud. XMPP protocol uses HTTPS protocol for data transport. XMPP protocol is used for the communication between KFS Manager and XMPP server in the cloud or for the communication between KFS Gateway/KFS Device and XMPP server over the firewall.

- **KFS Communication via LAN**
  Web service through HTTPS is used between KFS Gateway and devices. Between KFS Gateway and the device, a secure communication is set up using SNMPv3 which authenticates and encrypts SNMP packets flowing on the network. The communication via LAN is controlled by setting a range of subnet mask, IP address and host name. There is no unintended transmission via the network.

- **Communication Between KFS Components**
  One-to-one secure communication between KFS Mobile and devices can be set up via encrypted Bluetooth, Wi-Fi Direct or USB, without passing through the LAN.

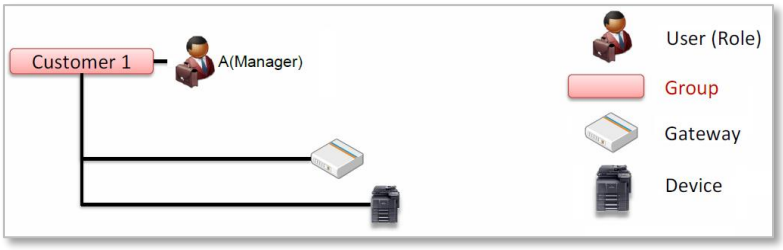
| Protocol/Interface | Data Communication |
|---|---|
| • Extensible Messaging and Presence Protocol<br>• (XMPP) | • Between KFS Manager and XMPP Server<br>• Between XMPP Server and KFS Gateway/KFS Device |
| • Hyper Text Transport Protocol Secure (HTTPS) | • Between Web browser's client UI and KFS Manager<br>• Between Web browser's client UI and KFS Gateway<br>• Between KFS Manager and XMPP Server<br>• Between XMPP Server and KFS Gateway/KFS Device |
| • Simple Network Management Protocol<br>• (SNMPv1/v2) | • Between KFS Gateway and device |
| • Bluetooth<br>• Wi-Fi Direct<br>• USB | • Between KFS Mobile and KFS Device |

## Data Access Control

Access to KFS is controlled by treating your group as one unit and giving access rights to users and devices registered in that group. Information assets are protected by strictly enforcing these access rights.

### Data Management

Authorized service providers can access devices located at the customer site, and securely manage those devices. In the example below, the group named Customer 1, with the role of Manager, can access KFS Gateway and KFS Device in order to securely manage user and device data.



## Data Transfer

Table 1 shows the amount of data obtained from the devices and frequency of communication. For instance, Device information (counters, toner levels and logs) is sent to KFS Manager once a day.
***Note***: Keep-alive connection is used every one minute, in order to maintain a XMPP connection between KFS Manager and KFS Device/KFS Gateway, The total amount of connection keep-alive per day is about 1,300 Kbytes, but this depends on packet sizes. The total amount of data obtained from a device per day is 100 Kbytes or so. Thus, the total amount of communication data is approximately 1,400 Kbytes.

***Table 1***

| Type of Communication Data | Frequency of Data Transmission | Amount of Data Communication/Day | Total Amount of Data Communication/Day |
|---|---|---|---|
| • Counter<br>• Toner Level<br>• Device Log | Once a day<br>***Note***: Counter/Toner Level data can be transmitted up to four times per day; once a day is the default setting. | 80 Kbytes | 1,400 Kbytes |
| • Notification | Per each alert event | 20 Kbytes | |
| • Connection Keep-alive | Every one minute | 1,300 Kbytes | |
| • Device Setting<br>• Snapshot<br>• Device Status<br>• Maintenance Mode Setting<br>• Data Capture<br>• On-demand<br>• USB Logs | During remote maintenance operation | 0 Kbytes<br>***Note***:<br>- Not communicated without maintenance operation<br>- Data amount depends on device model and operation contents. | |

## User Account Management

Within KFS Manager, users are created and assigned one of five roles, depending on the tasks they need to perform.

1. **System Administrator**: Manages the entire KFS system. Has access authority to all groups and users. May perform all monitoring, maintenance, and troubleshooting tasks.
2. **Manager**: Manages users under the delegated group to which the Manager belongs. Has access authority to all child groups. Manages users, service tasks, and reporting. Managers with RHQ permissions can upload and publish firmware.
3. **Service**: Registers and maintains devices for customers. Service users perform all maintenance tasks.
4. **Analyst**: Analyst has access rights to run reports but may not perform maintenance tasks. Tasks are not available for Analysts.
5. **Customer**: Customer can schedule and generate reports and notifications. Customers can also access device properties. However, they cannot access Log Data. Tasks, e.g., Device Configuration, are also not available to Customers.

***Note***: When a user accesses KFS Manager, the user is always identified and authenticated. If this identification and authentication is successful, the user can access KFS Manager based on his/her role.

### Password Settings

When a user account is initially created in KFS Manager, KFS Manager sends a notification to that user via an email. The email contains an automatically-generated user ID, a temporary password and a link to the service URL. The temporary password is valid for 7 days. When a user initially logs in with the User ID, he/she will be prompted to change the password. When the user changes the password, the URL (previously sent to the user) will no longer be valid. This stringent security setting prevents password from being stolen.

## Identification and Authentication

When accessing KFS, a user must log in with their registered User ID and password; an unauthorized user cannot access KFS. Access information is recorded and logged, thus available for auditing.

The following login security features are supported:

- **Account Lockout Policy**
  To protect KFS against password cracking attacks, if a user fails to login after three continuous attempts, the account is locked. The account will automatically unlock after 30 minutes.
- **Auto-Logout Policy**
  To prevent unauthorized operation of KFS, or a user fails to log out (account is idle), that user is automatically logged out after 30 minutes.
- **Password Policy**
  To prevent simple passwords from being set by users, and guard against unauthorized access by a third party, a user must employ a strong password. Specifically, the password length must be a least eight (8) characters, as well as include one or more numbers (0-9), upper case letters, lower case letters and special symbols. A password that does not meet the KFS Password Policy is prohibited.

## Task Restriction

Tasks are performed by a service provider through KFS Manager, some of which require prior customer approval. Specifically, Panel Screenshot and Data Capture cannot take place without customer approval. A confirmation request displays on the device panel, which must be accepted in order to execute the operation.
***Note***: Tasks and related data are encrypted using HTTPS protocol. KFS Manager can also terminate a task by sending a stop command to KFS Device through a secure XMPP communication channel.

## Regulatory Compliance

HIPAA regulations include security standards for the protection of electronic health information. KFS is compliant with these standards, as KFS does not collect, store or transmit patient information. In addition…

- Access to KFS is strictly controlled by the User ID and Access Code linked to the user's group
- Users must log in with a registered User ID
- A strong Password Policy is in place, so unauthorized users cannot access KFS
- Access to the KFS system is recorded and available for auditing
- KFS communication data is encrypted
- KFS components are mutually authenticated

In short, KFS sends device information in a secure manner for the purpose of device management or maintenance only and, again, does not transmit or identify any individual or group.

***Important***: KYOCERA Document Solutions Inc., does not believe that KFS will impact other federal laws related to privacy and confidential information, because KFS does not collect, store or transmit information

contained in print jobs. However, users must determine if special precautions should be implemented to comply with private, personal or confidential information regulations.

## Microsoft® Azure® Security

KFS relies on the Microsoft Azure platform for the protection, at the infrastructure level, of its cloud services and virtual machines (VM) against malicious attempts, such as distributed denial-of-service (DDoS) and DNS attacks. Azure's defense against DDoS is part of its continuous monitoring process and is continually improved through penetration-testing. It is designed to not only withstand attacks from the outside, but also from other Azure tenants.

Furthermore, Microsoft's Azure datacenter operations implement comprehensive information security policies and processes using standardized industry control frameworks, such as ISO 27001, SOC 1, and SOC 2. Third-party auditors regularly certify Microsoft's adherence to these standards for both the physical and virtual aspects of Azure infrastructure. Thus, KFS is continually diagnosed for the detection of such typical vulnerabilities of a web application as privilege escalation, directory traversal, code injection, cross-site scripting, etc.

***Note***: For general information and links about Azure, please visit http://azure.microsoft.com.

## Information Security Management System (ISMS) Certified

KFS is ISO/IEC 27001/27017 certified, meeting cloud services based security control standards. A top-down, risk-based approach that is technology-neutral and includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action.

## Appendix A: KFS Feature Summary by Component

| Feature | KFS Manager | KFS Device | KFS Gateway | KFS Mobile |
|---|---|---|---|---|
| 1. Register/unregister devices and users | ● | | | ● |
| 2. Access code required for device registration | ● | ● | ● | ● |
| 3. Manage device and user groups | ● | | | |
| 4. User authentication | ● | ● | ● | ● |
| 5. Establish device configuration settings | ● | | | ● |
| 6. Check toner levels | ● | | | ● |
| 7. Monitor device status | ● | | | ● |
| 8. Perform maintenance/diagnostics/troubleshooting | ● | | | |
| 9. Upgrade firmware | ● | | | ● |
| 10. Email logs | ● | | | |
| 11. Audit logs | ● | | ● | |
| 12. Data collection time stamp | ● | | | |
| 13. Page counter collection | ● | | | |
| 14. Manage firmware packages | ● | | | ● |
| 15. Generate list and graphical reports | ● | | | |
| 16. Restart one device or group of devices | ● | | | ● |
| 17. Email notification/log | ● | | | ● |
| 18. Toner order | ● | | | |
| 19. Set user account access | ● | | | |
| 20. View device properties | ● | | | ● |
| 21. Capture snapshots (status pages) | ● | | ● | ● |
| 22. Send panel note | ● | | | |
| 23. View panel status | ● | | | |
| 24. Capture panel screenshot* | ● | | | |
| 25. Send test files | ● | | ● | |
| 26. Data capture* | ● | | | |
| 27. Import/export floor maps | ● | | | |
| 28. Address book import/export | ● | | | |
| 29. View page counters | ● | | | ● |
| 30. Firmware upgrades | ● | | | ● |
| 31. Obtain device info via Bluetooth, USB or Wi-Fi Direct | | | | ● |
| 32. Manage mobile devices in a delegate group | ● | | | ● |
| 33. View toner replacement forecasts | ● | | | ● |
| 34. Track toner order status | ● | | | |
| 35. On-demand USB logs | ● | ● | | |
| 36. Enable/disable features by user group | ● | | | |
| 37. iOS, Android and Win mobile support | | | | ● |

**Only possible with advance IT administrator approval and confirmation of operation directly from device panel, i.e., the function is not possible without multiple levels of on-site authorization.*

## Appendix B: KFS Supported Kyocera Models (as of November, 2018)

| | | |
|---|---|---|
| • TASKalfa 13600* | • TASKalfa/CS 3252ci | • ECOSYS M2635dw |
| • TASKalfa 11100* | • TASKalfa/CS 3212i | • ECOSYS M2635dn |
| • TASKalfa 9600* | • TASKalfa/CS 306ci | • ECOSYS M2540dw |
| • TASKalfa/CS 9002i | • ECOSYS M6635cidn | • ECOSYS M2535dn |
| • TASKalfa/CS 8052ci | • ECOSYS M6630cidn | • ECOSYS M2530dn |
| • TASKalfa/CS 8002i | • ECOSYS M6235cidn | • ECOSYS M2135dn |
| • TASKalfa/CS 8001i | • ECOSYS M6026cidn | • ECOSYS M2040dn |
| • TASKalfa/CS 8000i | • ECOSYS M6026cdn Type B | • ECOSYS M2035dn |
| • TASKalfa/CS 7551ci | • ECOSYS M6035cidn | • FS-4300DN |
| • TASKalfa/CS 7550ci | • ECOSYS M6030cdn | • FS-4200DN |
| • TASKalfa/CS 7052ci | • ECOSYS M6026cidn Type B | • FS-4100DN |
| • TASKalfa/CS 7002i | • ECOSYS M6026cdn | • FS-2100DN |
| • TASKalfa/CS 6551ci | • ECOSYS M5526cdw | • FS-2100D |
| • TASKalfa/CS 6550ci | • ECOSYS M5526cdn | • ECOSYS P8060cdn |
| • TASKalfa/CS 6501i | • ECOSYS M5521cdw | • ECOSYS P7240cdn |
| • TASKalfa/CS 6500i | • TASKalfa/CS 3051ci | • ECOSYS P7040cdn |
| • TASKalfa/CS 6052ci | • TASKalfa/CS 3050ci | • ECOSYS P7035cdn |
| • TASKalfa/CS 6002i | • TASKalfa/CS 3011i | • ECOSYS P6235cdn |
| • TASKalfa/CS 5551ci | • TASKalfa/CS 3010i | • ECOSYS P6230cdn |
| • TASKalfa/CS 5550ci | • TASKalfa/CS 300ci | • ECOSYS P6130cdn |
| • TASKalfa/CS 5501i | • TASKalfa/CS 266ci | • ECOSYS P6035cdn |
| • TASKalfa/CS 5500i | • TASKalfa/CS 2552ci | • ECOSYS P6030cdn |
| • TASKalfa/CS 5052ci | • TASKalfa/CS 2551ci | • ECOSYS P6026cdn Type B |
| • TASKalfa/CS 500ci | • TASKalfa/CS 2550ci | • ECOSYS P6026cdn |
| • TASKalfa/CS 5002i | • TASKalfa/CS 250ci | • ECOSYS P6021cdn |
| • TASKalfa/CS 4551ci | • ECOSYS M8130cidn | • ECOSYS P5026cdw |
| • TASKalfa/CS 4550ci | • ECOSYS M8124cidn | • ECOSYS P5026cdn |
| • TASKalfa/CS 4501i | • ECOSYS M5521cdn | • ECOSYS P5021cdw |
| • TASKalfa/CS 4500i | • ECOSYS M4132idn | • ECOSYS P5021cdn |
| • TASKalfa/CS 406ci | • ECOSYS M4125idn | • ECOSYS P4040dn |
| • TASKalfa/CS 4052ci | • ECOSYS M3660idn | • ECOSYS P4035dn |
| • TASKalfa/CS 4012i | • ECOSYS M3655idn | • ECOSYS P3060dn |
| • TASKalfa/CS 400ci | • ECOSYS M3645idn | • ECOSYS P3055dn |
| • TASKalfa/CS 4002i | • ECOSYS M3560idn | • ECOSYS P3050dn |
| • TASKalfa/CS 356ci | • ECOSYS M3550idn | • ECOSYS P3045dn |
| • TASKalfa/CS 3552ci | • ECOSYS M3540idn | • ECOSYS P2235dw |
| • TASKalfa/CS 3551ci | • ECOSYS M3540dn | • ECOSYS P2235dn |
| • TASKalfa/CS 3550ci | • ECOSYS M3145idn | • ECOSYS P2235d |
| • TASKalfa/CS 3511i | • ECOSYS M3040idn | • ECOSYS P2135dn |
| • TASKalfa/CS 3510i | • ECOSYS M3040dn | • ECOSYS P2040dw |
| • TASKalfa/CS 3501i | • ECOSYS M2735dw | • ECOSYS P2040dn |
| • TASKalfa/CS 3500i | • ECOSYS M2640idw | |
| * Limited reporting capability | | |
| Note: If a specific model does not appear in this list, please contact our Authorized Kyocera dealer regarding KFS compatibility. Specifications of KFS compatible models subject to change without notice. | | |

## Appendix C: Use Case Scenarios

### Case 1: Counter Collection / Process Improvement

Workflow associated with the collection of meter reads is an excellent use case scenario, one that any company with a leased print fleet can associate with. Prior to the availability of remote management tools, like KFS, the monthly reporting of device counters to a service provider was time-consuming and error-prone. Typically, the scenario goes as follows:

1. Service provider calls key contact (at customer site) and requests device counters.
2. The key contact physically accesses the counter display on each device and makes a notation. Depending on fleet size and geographic location, this can be a major undertaking.
3. Counters are reported back to the service provider by telephone, fax or email.
4. Service provider bills the customer, based on customer-reported page counts.

Manual meter reading is clearly an unproductive, costly method of communicating counter data. KFS eliminates these inherent drawbacks, and the obvious potential for errors, by automatically polling counter MIB data from each connected device. The resulting information is made available through KFS Manager and KFS Mobile, allowing for timely, accurate billing cycles. By simply automating counter collection, process improvement is immediate and measurable.

KFS also integrates with E-Automate, a service management tool that enables authorized Kyocera dealers to migrate meter counts from KFS directly into their billing system. Counts can be collected at a scheduled interval, time, or on demand, ensuring accurate billing cycles. And since there's no customer intervention required, either by phone or mail, employees can focus on more important tasks at hand.

### Case 2: Fleet Optimization / Cost Reduction

In today's busy office environments, it may go unnoticed that printers and MFPs are over- or under-utilized. This is particularly true for under-utilized devices, which may sit idle while over-utilized systems are just down the hall. With KFS remote monitoring, the exact Copy, Print, Scan and Fax volumes for each device are accessible at any time.

If over-utilized devices come with a higher cost-per-page, shift volumes to another device or swap the machine out for more efficient equipment. Redeployment, replacement and future procurement decisions can be made based on verifiable KFS usage data. That data can be presented in list or graphical form, to clearly present patterns and trends that will help determine "right-sizing" strategies. Taking the time to make these critical assessments ensures optimum fleet utilization and reduced total cost of ownership.

### Case 3: Fleet Uptime / Elevated Customer Support

Service dispatch is another area where KFS creates a new paradigm. With notifications set, the KFS system alerts the service provider (via email) of a potential event – low toner, waste toner box full, jam frequency, preventative maintenance due, etc. These device-specific alerts prepare a technician with the necessary information, parts and/or consumables to resolve the issue, frequently before the customer is aware; no user intervention is required. With the problem resolved, on-site service calls are reduced, taking customer support and satisfaction to the next level.

## Appendix D: Port Settings

### On the Intranet Firewall

- TCP port 443 (HTTPS) must be opened to allow outbound traffic. This port is used for KFS Device and KFS Gateway for Windows to connect to KFS Manager.
- If your firewall restricts outbound traffic by a destination whitelist, the host names of Web servers in KFS Manager should be added in it.
  - The names of the Web servers vary depending on which Azure data center KFS Manager is hosted. This information is provided by the Kyocera headquarters in your region.

### On the Machine Hosting KFS Gateway for Windows

- TCP port 443 (HTTPS) must be opened to allow outbound traffic. This port is used for KFS Gateway for Windows to connect to KFS Manager. The port is also used to send control commands by HTTPS when registering older models of KFS Device that don't support the KYOCERA extension of WSDL (KM-WSDL). The same port is used for the Send File feature over IPPS, too.
- TCP port 8443 (HTTPS) should be opened to allow inbound traffic. This is necessary if you wish to use the Web UI of KFS Gateway for Windows from a browser running on another PC in the LAN.
- UDP port 161 must be opened to allow outbound traffic to devices. This port is used to collect device status and properties over SNMP.
- TCP port 80 (HTTP) should be opened to allow outbound traffic. This port is used for KFS Gateway for Windows to send control commands when registering older models of KFS Device that don't support either KM-WSDL or HTTPS.
- TCP port 9090 (HTTP) and/or 9091 (HTTPS) should be opened to allow outbound traffic. This port is used for KFS Gateway for Windows to send control commands to KFS Device over KMWSDL at the time of device registration.
- When KFS Gateway for Windows is installed. TCP port 8442 (or an alternative port specified at the time of installation) is automatically opened in Windows Firewall to allow inbound traffic from devices. This is necessary if you wish to use the Firmware Upgrade feature via KFS Gateway for Windows. The inbound rule thus created will be deleted when KFS Gateway for Windows is uninstalled.
- TCP port 9100 (or an alternative port to be specified as a parameter of a Send File task) should be opened for outbound traffic, if you wish to use the Send File feature over raw port printing (RAW) via KFS Gateway for Windows.
- When KFS Gateway for Windows is installed, TCP port 8081 (HTTPS) is automatically opened in Windows Firewall to allow inbound traffic from devices. This is necessary if you wish to use the feature of KFS Gateway for Windows to consolidate outgoing network traffic from KFS Device as a single point of communication. The inbound rule thus created will be deleted when KFS Gateway for Windows is uninstalled.

### On the Machine Hosting Local Agent

Local Agent is a tool installed on a PC that has a USB connected printer so the Gateway can find that particular device.

- TCP port 445 should be opened for inbound traffic if you wish to use the feature of KFS Gateway for Windows to install or upgrade Local Agent. This port is used to transfer files necessary for the installation or upgrading of Local Agent over SMB.
- Windows Management Instrumentation (WMI) should be enabled if you wish to use the feature of KFS Gateway for Windows to install or upgrade Local Agent.
- TCP port 5985 gets opened for inbound traffic if you enable Windows Remote Management (WinRM). This is necessary if you wish to use the feature of KFS Gateway for Windows to install or upgrade Local Agent.
  - If enabling WMI or WinRM is against your site's security policy, you should keep them disabled. In that case, you need to install Local Agent manually, rather than from KFS Gateway for Windows.

## About KYOCERA

KYOCERA Document Solutions America, Inc. (usa.kyoceradocumentsolutions.com), headquartered in Fairfield, N.J., is a leading provider of computer-connectable document imaging and document management systems, including network-ready digital MFPs/printers, laser printers, color MFPs/printers, digital laser facsimiles, and multifunctional and wide format imaging solutions.

KYOCERA Document Solutions America is a group company of KYOCERA Document Solutions Inc., a core company of the KYOCERA Corporation, the world's leading developer and manufacturer of advanced ceramics and associated products, including telecommunications equipment, semi-conductor packages and electronic components.

KYOCERA Document Solutions America, the first document solutions company with third-party certified sales data, has received numerous honors for its products' high performance, reliability and cost efficiency. KYOCERA Corporation's consolidated net revenues exceeded $13 billion for the fiscal year ending on March 31, 2017.

Specifications and design are subject to change without notice.
For the latest on connectivity, please visit usa.kyoceradocumentsolutions.com.
HyPAS, TASKalfa and ECOSYS are trademarks of the KYOCERA Companies.
All other trademarks are the property of their respective owners.

KYOCERA Document Solutions America, Inc.
Headquarters: 225 Sand Road, Fairfield, NJ 07004-0008, USA

v062218

KYOCERA
Document Solutions