KYOCERA FLEET SERVICES
SECURITY WHITE PAPER

V1.7 November 2018

BUSINESS SOLUTION

GLOBAL NETWORK

KYOCERA
Document Solutions

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 so important? Harnessing the continuous flow of usage data is a proven way to optimise 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 utilise 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 organisation? 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 organisation.

The intelligence gathered from device metrics enables a service provider to quickly respond to their customers' present and future technology needs.

KYOCERA Document Solutions

KFS is a cloud-based device monitoring and management 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

The 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 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.


In many cases, service issues can be resolved over the phone with minimal disruption and delay to customers' business operations.

By more efficiently utilising human resources, service providers can maximise device uptime, reduce workflow interruptions and reduce the frequency, duration and cost of on-site service calls; in many cases, service issues can be resolved over the phone with minimal disruption and delay to customers' business operations. The more devices and users that are connected, the more insights can be gathered and the more sophisticated the predictive capabilities become, helping to realise enterprise-wide efficiencies and meet service-level response objectives faster than ever before.

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 print fleet running smoothly. To that end, these components enable service providers to optimise the operation of KYOCERA and non-KYOCERA digital imaging systems.

With KFS it is possible to monitor a wide range of multivendor devices. To benefit from the additional remote maintenance functionalities, KYOCERA devices are required. This ensures that KYOCERA can provide you with the best possible end-to-end solution to meet your organisational needs.

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. KFS Gateway is installed for Windows application on a PC or on a server in the customers' environment. It is possible to support a single point of communication via the Gateway, as shown in Figure 1. KFS Mobile is an application installed on service personnel's mobile devices such as smart phones and tablets.
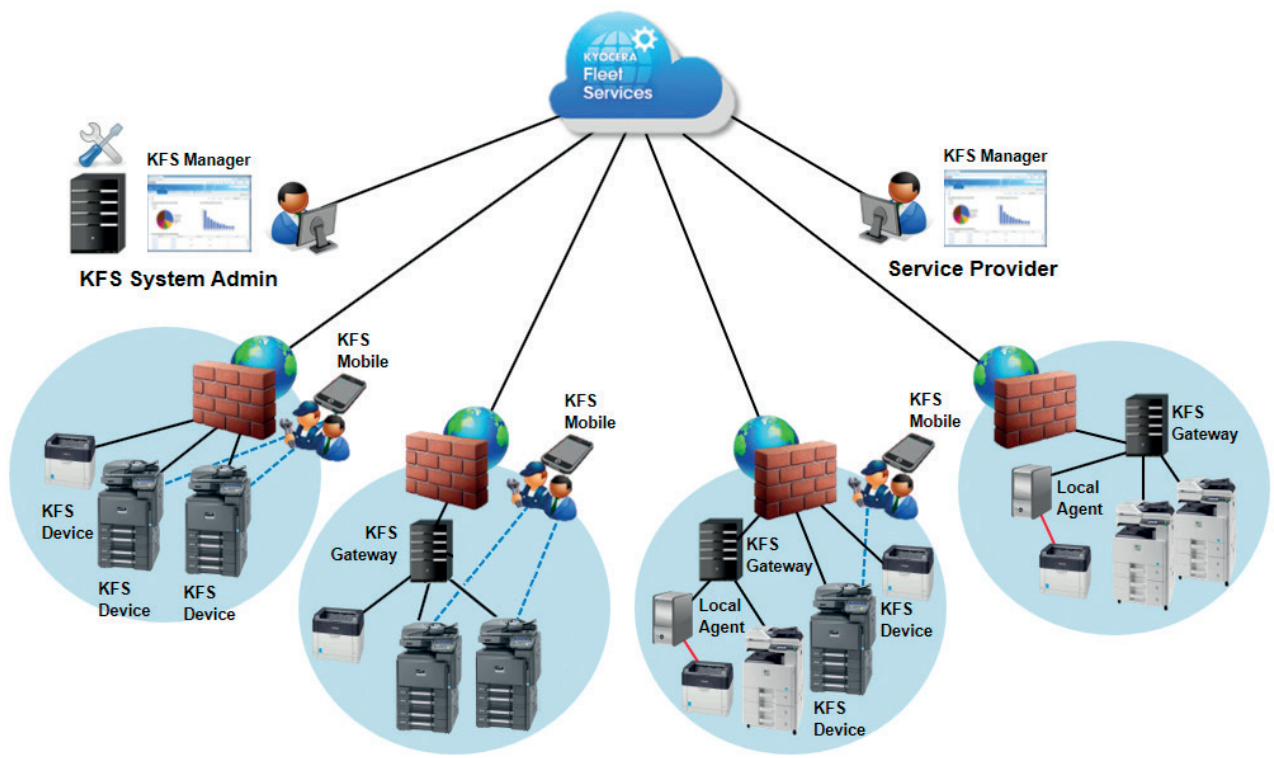
KYOCERA devices directly connected through KFS Devices

KYOCERA devices connected through the Gateway, **with a single line of communication. For more details on the Port Settings, please see page 15**

KYOCERA devices connected directly through KFS Device and Third Party/KYOCERA legacy Devices and USB printers connected through the Gateway

KYOCERA legacy devices, third party devices and USB printers connected through the Gateway

Figure 1: System Map – Options for connecting with KFS

☁ KFS MONITORING

Provides centralised control for key system features and enables improved utilisation of assets and increased productivity with an intuitive web interface, for both KYOCERA and third party devices.

> View device counters and properties

> Generate list and graphical reports

> Check consumable levels

> Monitor real-time device status

> Assist ordering systems

⚙ KFS MANAGEMENT

The below features are available only for KYOCERA devices, and can increase customer satisfaction by providing rapid remote customer support.

> Register and manage users and device groups

> Establish configuration settings

> Obtain detailed device information

> Perform maintenance / diagnostics / troubleshooting

> Restart (reboot) devices

> Remotely upgrade firmware

Table 1: Key benefits and functionalities

KYOCERA Document Solutions

3 HOW IS YOUR SECURITY GUARANTEED?

According to the latest predictions by IDC[1] it is estimated that by 2025, the global volume of data will expand tenfold to 163 zettabytes. Not only that, but the data held in the public cloud will double to 26% in 2025, with an increasingly bigger proportion of data being generated by enterprise. At the same time it is estimated that the average person will interact with connected devices nearly 4,800 times per day, the equivalent of one interaction every 18 seconds. In this increasingly data-intensive world, protection of your valuable information assets is therefore of paramount importance. For these reasons KFS employs a variety of robust security features that safeguard communication between KFS components and devices.

SECURE MICROSOFT® AZURE® HOSTING ENVIRONMENT AND REGULATORY COMPLIANCE

KFS Manager is hosted on Microsoft Azure[2], a cloud-based platform that provides a highly-secure server infrastructure to manage KFS applications and protect against malicious attempts, such as distributed denial-of-service (DDoS) and domain name system (DNS) attacks. Azure's defense 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. It provides an internal DNS to secure internal virtual machine (VM) names. VM names are resolved to private IP addresses within a cloud service while maintaining privacy across cloud services, even within the same subscription. In addition to offering multiple layers of security, Microsoft Azure provides complete isolation from all other networks; traffic only flows through customer-configured paths.

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. Microsoft meets a broad set of internationally recognised information security controls and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards including Australia CCSL (IRAP), UK G-Cloud, and Singapore MTCS.

Third-party auditors regularly certify Microsoft's adherence to these standards for both the physical and virtual aspects of Azure infrastructure. As a result, 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., and any serious issues unearthed in these tests or reports from other sources are promptly resolved to keep the application secure.

In May 2017, KYOCERA also completed the Cloud Security Alliance (CSA) STAR Self-Assessment - the industry's most powerful program for assurance in the cloud, encompassing key principles of transparency, rigorous auditing and harmonisation of standards. In November 2017, KYOCERA completed the certification of its Information Security Management System (ISMS). This is a follow-up to the self-assessment, in accordance with ISO27001 information security and ISO27017 cloud information security standards and includes third party validation.

KYOCERA continuously monitors the newest security trends and vulnerability information. KYOCERA developed KFS following the "Open Web Application Security Project (OWASP)" as a guideline. We strictly check for potential vulnerabilities to ensure the best possible security. Prior to release, security diagnostic tests are conducted not only within KYOCERA but also by an independent service provider.

1- D. Reinsel, J. Gantz, J. Rydning, "Data Age 2025: The Evolution of Data to Life-Critical", IDC Whitepaper, April 2017
2- For more information, you can refer to the Microsoft Azure Network Security White Paper: https://docs.microsoft.com/en-us/azure/security/abstract-azure-network-security
or visit http://azure.microsoft.com

KYOCERA Document Solutions

Compliance with privacy legislation is very important to KYOCERA, even more so after applicability of the EU General Data Protection Regulation ("GDPR") as of May 2018. The GDPR has tightened the obligations of data controllers and processors and penalties for breaches have increased, affecting KYOCERA and its customers alike with the organisation of their work and data flows.

KYOCERA Document Solutions Inc. ("KDC") is the owner of the KFS software and is located in Japan. The KFS software is stored in the cloud and the server is located in the European Union, Amsterdam, The Netherlands. As the owner of the KFS software, KDC can log in to the KFS server and can access the KFS account holder's personal data (name, email ID, device IP address). KDC can only process the personal data to operate or support the KFS services or at the end user's request. KDC may also use a number of sub-processors to support the provision of KFS

services. A list of sub-processors is published on KYOCERA's website www.kyoceradocumentsolutions.eu.

For the KFS service, KYOCERA is acting as a data processor on behalf of the data controller, which is the customer. A data controller is the company that is responsible for determining the purposes and means of the processing of personal data and the data processor is a company which processes personal data on behalf of the data controller. To ensure full compliance for both the customer and KYOCERA, we require KFS customers to agree to our Data Processing Terms and Conditions. KYOCERA also processes some personal data as a data controller, i.e. for the purpose of improving our products and services. For this part of data processing, our KFS Privacy Statement applies. both documents can be viewed and downloaded from the KYOCERA website www.kyoceradocumentsolutions.eu.
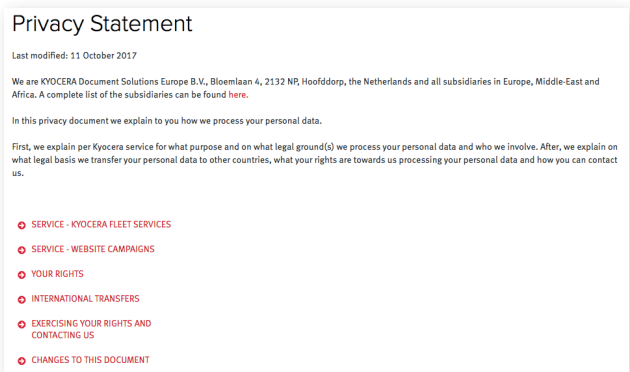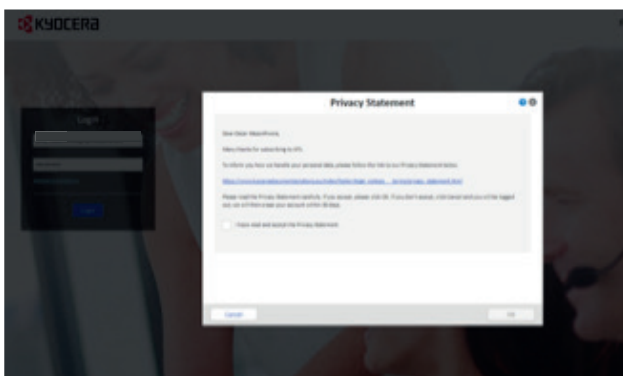

Figure 2: Personal data handling – process for obtaining consent from the end user. The full privacy statement is publicly available from the KDE EU website via the following link: https://www.kyoceradocumentsolutions.eu/index/footer/legal_notices___terms/privacy_statement.html

5 HOW DOES KFS RESPECT YOUR RIGHT TO PRIVACY?

KFS does not collect, store or transmit information contained in print jobs. KFS sends device information in a secure manner for the purpose of device management or maintenance only and does not transmit or identify any individual or group, unless given permission to do so by and on behalf of dealers and their customers. Due to the multi-tenancy system architecture, dealer and their customers' information cannot be accessed by any other dealer or customer.

PROTECTION OF STORED DATA

The sensitive information assets stored in KFS components such as KFS Manager, KFS Device, KFS Gateway and KFS Mobile, are encrypted with the following encryption algorithms. The sensitive information assets stored in KFS Mobile includes the user password of KFS Manager, refresh token for setting up a secure communication channel with KFS Manager and the password for proxy server authentication. These sensitive information assets are protected by encryption and are protected against information leaks by a malicious third party, etc.

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

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 unless it is authorised and provided by the customer at the printer panel.

KFS Manager	256-bit	Keys are generated for each environment and are setup for each deployed server. Keys are saved in configuration management software (CMS) where only the deployment engineer can reference.
KFS Gateway (PC/Box Common)	128-bit	Keys are automatically created during first launch of KFS Gateway. Keys are saved in local Database of application. Furthermore, access key to local DB (Apache Derby) are managed inside the program.
KFS Mobile (Android)	256-bit	Keys are automatically created during first launch of application after installation. Keys are saved to DB specific to application.
KFS Mobile (iOS)	128-bit/256-bit	Keys are generated beforehand and embedded in application (same for all devices).
KFS Device	128-bit/256-bit (depends on model)	Keys are generated to be a unique number on the device basis during launch for each device following KYOCERA Document Solution's own algorithm and are saved to volatile memory of the device.

Table 2: How the key length is generated and managed

KYOCERA Document Solutions

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 sends 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.

> Extensible Messaging and Presence Protocol > Extensible Messaging and Presence Protocol (XMPP)	> Between KFS Manager and XMPP Server > Between XMPP Server and KFS Gateway/KFS Device
> Hyper Text Transport Protocol Secure (HTTPS)	> Between Web browser's client UI and KFS Manager > Between Web browser's client UI and KFS Gateway > Between KFS Manager and XMPP Server > Between XMPP Server and KFS Gateway/KFS Device
> Simple Network Management Protocol (SNMPv1/v2)	> Between KFS Gateway and device
> Bluetooth > Wi-Fi Direct > USB	> Between KFS Mobile (USB currently only available for Android) and KFS Devicee

Table 3: Summary of data protocols and communication

DATA ACCESS CONTROL

Like many other SaaS solutions today, KFS is based on a multi-tenant system to accommodate multiple dealers and sales companies, and uses the concept of "Group Management" in order to enforce appropriate user and device data access control, and prevent leakage of information to other tenants. 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. Thus a dealer cannot view the data of another dealer, and their customers.

CONNECTION MODE

The Connection mode feature in KFS allows users to determine the type of connection a device has with the KFS server. There are two settings for connection mode: Manage and Monitor. The setting is available for Gateway and KFS Device Agent. Users can access it on: Gateway UI, Device panel, CCRX, Device Registration and Diagnostic Tool (DRD Tool), and Mobile.

> **Monitor:** Communication between KFS Device or Gateway with KFS is limited. (Customer A in below diagram).

> **Manage:** Constant communication between the Device or Gateway with KFS using XMPP (Customer B in below diagram).

This means that remote maintenance tasks cannot be performed on the devices set with "Monitor" until the Customer with the role of Manager can provide the permission for the service provider by using the connection mode feature to switch to "Manage" however, the device status will automatically switch over to Monitor mode from Manage mode after a certain time period. That time period is adjustable in one hour increments.
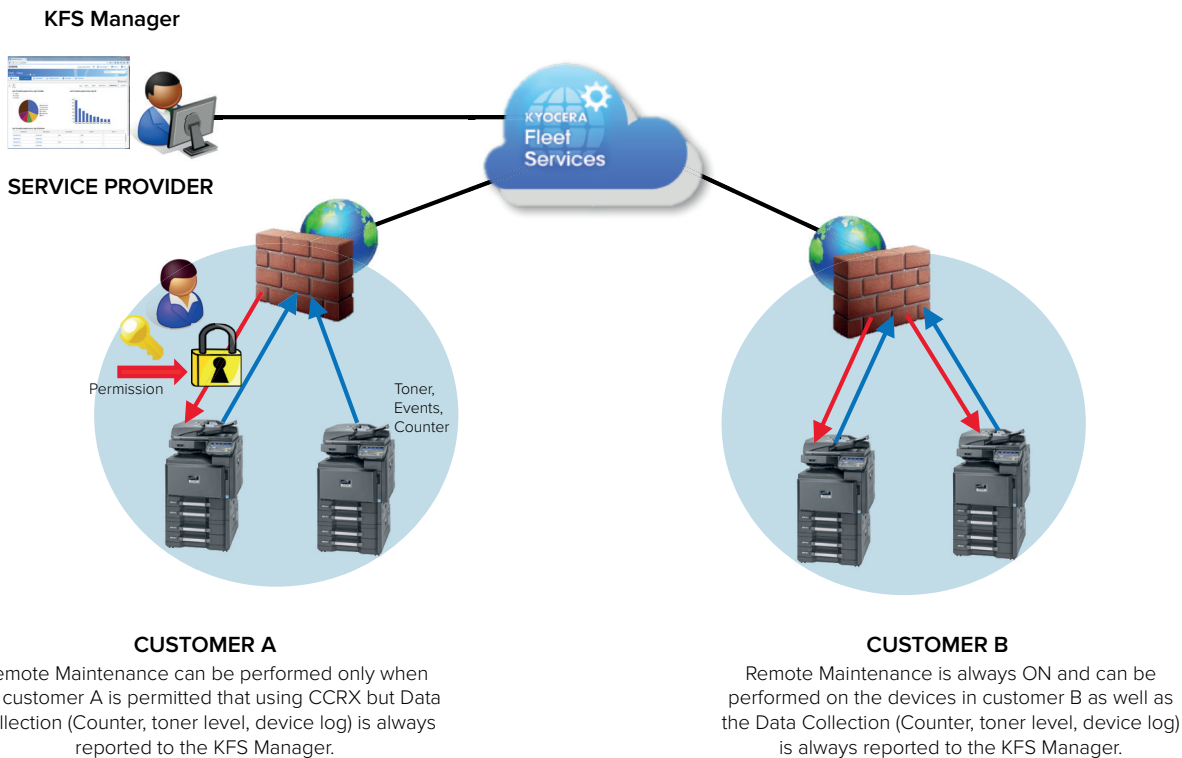

CUSTOMER A
Remote Maintenance can be performed only when the customer A is permitted that using CCRX but Data Collection (Counter, toner level, device log) is always reported to the KFS Manager.

CUSTOMER B
Remote Maintenance is always ON and can be performed on the devices in customer B as well as the Data Collection (Counter, toner level, device log) is always reported to the KFS Manager.

Figure 3: Example of group setup and device connection mode setting
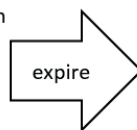
Figure 4: Command Centre (CCRX) example of screen settings

KYOCERA Document Solutions

DATA TRANSFER

Table 4 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 size. 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.

> Counter > Toner Level > Device Log	Once a day 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 > Snapshot > Device Status > Maintenance Mode Setting > Data Capture > On-demand USB Logs > Back-up data	During remote maintenance operation	0 Kbytes > Note: Not communicated without maintenance operation > Data amount depends on device model and operation contents.	

Table 4: Type of communication and data flows

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 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 helps to prevent user accounts being compromised.

IDENTIFICATION AND AUTHENTICATION

When accessing KFS, a user must log in with their registered User ID and password; an unauthorised 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.

> **Password Policy**
   To prevent simple passwords from being set by users, and guard against unauthorised access, a user must employ a strong password. Specifically, the password length must be a least eight (8) characters, as well as include one (1) or more numbers (0-9), upper case letters, lower case letters and symbols.

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.

Data	Description and attribute data collected to perform functions
Device Notification/ Log	When a system error or event occurs, the device sends event information to KFS manager, which immediately notifies the user. > System Error > Event (e.g. Paper Jam, Low Toner Volume) > Consumption > Counter
Data Setting	Personnel can remotely set up the device upon receipt of a request and approval. The personnel save the settings in KFS manager and send it to the device when it is not being used. The following information is obtained: > Network Setting e.g. Enhanced WSD > System Setting e.g. Date/Time, Time Zone > E-mail Setting e.g. SMTP, Email Send Settings > Print Setting e.g. Eco Print > Copy Setting e.g. Original Image, Prevent Bleedthrough > FAX Setting e.g. Continuous Scan, FAX TX Resolution > Default Setting e.g. Scan Resolution
Snapshot	Obtained to remotely diagnose device problems, done by operating KFS Manager. > Status > Service Status > Event Log > Maintenance Report > USB Log > FAX Report
Device Status	To remotely check device status. > Panel Message > Alert List
Maintenance Mode Setting	To perform optimal maintenance at the customer site. Obtained from KFS Manager, can be changed and sent to the device. > Device Adjustment
Data Capture	Obtained when the confirmation message is shown on the panel of the target device and approval is received from the IT administrator in advance. Service managers can specify the time period up to 7 days (default – 1 day) to remove the captured data. > Customer Print Data
On-Demand USB Logs	On-Demand USB Logs can be retrieved only when the confirmation of approval is gained from IT administrator at the customer site. The device will be locked for several minutes (3 to 4 minutes) when retrieving. After the operation ends, the device automatically gets restarted. After the device restarts, the USB logs are automatically downloaded to users' PC from KFS Manager. > USB Logs
Back-up Data	The service personnel can import the back-up data exported from one device to other devices. Back-up data can be obtained only after the user has accepted the confirmation message on the panel of the target device. Any back-up data containing personally identifiable information is not stored in KFS Manager. Back-up data obtained is encrypted. The use of the feature is restricted only for authorised access to group devices. Importing / Exporting the backup data will be recorded. > Address Book > Job Account

Table 5. Type of data collected for performing key functions and related attribute data

KFS Component	Information (Used for the purpose of identification and communication within KFS)
KFS Manager	> Authentication information of each KFS user > Access codes used by KFS Devices (KFS Gateway and KFS Mobile) > Server certificates used for secure communications between KFS Manager and various agents or clients, such as Web browsers, KFS Devices, KFS Gateways and KFS Mobile, as well as between internal components of KFS Manager > MAC addresses of each KFS Device or KFS Gateway > Network information, such as the host name and IP address of each registered device, intended to be used for the purpose of remote device management or maintenance > SNMP credentials (e.g. SNMPv1/v2 community name, SNMPv3 username and password, etc.), entered from either KFS Manager or KFS Gateway as part of device discovery settings and used to connect to the devices by SNMP > Serial numbers of each mobile device (smartphone or tablet) on which KFS Mobile is installed [In case the serial number cannot be obtained from the mobile device, its IMEI may be used for the same purpose.]
KFS Device	> MAC address of the device in which KFS Device is embedded > Proxy authentication information entered from the device panel, or by other means, and used by KFS > Gateway itself or KFS Device to connect to KFS Manager through the proxy server > Authentication token generated by KFS Manager and downloaded to a KFS Device
KFS Gateway	> Authentication information used by an IT administrator to log in to KFS Gateway > Authentication information used by a visiting service technician to log in to KFS Gateway > MAC address of the machine (either a PC in the case of KFS Gateway for Windows or a Linux box in the case of KFS Gateway for IB) on which KFS Gateway is installed > Access code used by KFS Gateway to register itself to KFS Manager [The same code may be used by KFS Gateway to register devices in the case of automatic discovery and registration.] > Proxy authentication information used by a KFS > Gateway or KFS Device when connecting to KFS Manager through the proxy server > Authentication token generated by KFS Manager and downloaded to KFS Gateway > SNMP credentials (e.g. SNMPv1/v2 community name, SNMPv3 username and password, etc.), entered from either KFS Manager or KFS Gateway as part of device discovery settings and used to connect to the devices by SNMP > Authentication information used by KFS Gateway to communicate with devices by proprietary protocols
KFS Mobile	> Serial numbers of each mobile device (smartphone or tablet) on which KFS Mobile is installed [in case the serial number cannot be obtained from the mobile device, its IMEI may be used for the same purpose]. > Authentication token generated by KFS Manager and downloaded to KFS Mobile > Authentication information entered by the user of KFS Mobile to log in to KFS Manager > Proxy authentication information used by a KFS Mobile and paired KFS Device when connecting to KFS Manager through the proxy server

Table 6. Information utilised by KFS components

AUDIT LOGS

One of the key advantages of implementing a fleet management system, as recommended by Quocirca[3], is that it provides continuous monitoring essential to establish ongoing governance of print infrastructure. KFS records audit logs of various events, accessible by restricted users. An audit record is generated for the following events:

Audit Logs - KFS Manager
> Successful/unsuccessful user identification and authentication

> KFS Manager version up

> Database backup

> Database restore

> Add/Edit/Delete group and user account

> Register/Terminate/Delete KFS Device/KFS Gateway/KFS Mobile

> Configure Security settings

> Terminate inactive user sessions

> User password reset by e-mail.

> Import/Export user list

> Delete/Archive task

> Delete/Archive system event

> Export device logs

> Delete/Archive audit records

> Download data capture

> Import/Export backup data

Audit Logs - KFS Gateway
> Successful/unsuccessful user identification and authentication

> KFS Gateway local administrator password reset

> Configuration of device recovery settings

> Configuration of security settings

> Termination of inactive sessions

The history for these events shows the time/date and the result (success/failure). In the event of alteration or leak of information, the audit logs can be used to investigate and help trace the unauthorised access. The operation logs are saved for the purpose of maintaining audit trails.

3- For more information, you can refer to the Quocirca market prespective on Print Security: An Imperative in the IoT Era: http://quocirca.com/wp-content/uploads/2018/06/Quocirca-Print-Security-Jan-2017-Report-Excerpt.pdf

KYOCERA Document Solutions

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 to it.

> The names of the web servers can be found below in Table 7.

Server type	Host name	IP address	Effective from
User Web	fs-eu.kyocera.biz	191.233.91.217	
Device Rest	rfs-eu.kyocera.biz	104.46.60.117	
XMPP Servers	fs-eucs01.kyods.com	52.233.166.114 52.233.152.139 (back-up)	10-jan-18 10-jan-18
Remote Panel	fs-eurs001.kyocera.biz fs-eurs002.kyocera.biz	40.115.1.211 40.113.113.42	10-nov-18 10-nov-18

Table 7: KFS Web servers in EU 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 Devices that don't support the KYOCERA extension of WSDL (KM-WSDL). The same port is also used for the Send File feature over IPPS.

> TCP port 8443 (HTTPS) should be opened to allow inbound traffic. This is necessary if you wish to use the Web UI for 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 Devices as a single point of communication. The inbound rule thus created will be deleted when KFS Gateway for Windows is uninstalled.

> Setting up a single point of communication on the Gateway is simple. Once it is installed on the host PC and registered to the KFS server, configure the proxy settings if the customer is using a proxy. If not, activating the check box will complete the setup. Devices that are already registered to KFS can have the proxy settings changed to the host name of the Gateway with access to port 8081.

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 for Local Agent over SMB.

> Windows Management Instrumentation (WMI) should be enabled if you wish to use the feature for 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.

Source	Destination	Protocol	Port	Service
MFP / Printer	KFS Manager	TCP	443	HTTPS : Send fleet data to KFS
Gateway for Windows	KFS Manager	TCP	443	HTTPS : Send fleet data to KFS
Client PC	KFS Manager	TCP	443	HTTPS : Access to the UI
Client PC	Gateway for Windows	TCP	443	HTTPS : Access to the UI
Gateway for Windows	MFP / Printer	UDP	161	SNMP
		TCP	443	IPPS
		TCP	9100	RAW (for Send File function)
		TCP	8442	HTTP (for Firmware upgrade function)
		TCP	80	HTTP
		TCP	443	HTTP
		TCP	9091	SOAP over HTTPS : Configuration for the device settings
		TCP	8081	Single point of communication
Gateway for Windows	Local Agent	UDP	161	SNMP
		TCP	445	SMB
		TCP	5985	WinRM

Table 8: Summary of port settings

KYOCERA Document Solutions

SYSTEM RECOMMENDATIONS

System components	Operation systems	Browsers	.NET Framework	Java runtime
Manager	-	Internet Explorer 11 Edge Firefox 40 or later (*1) Chrome 47 or later (*1) Safari 8 or later (*1)	-	-
Gateway for Windows	Windows 7 [32-bit/64-bit] Windows 8/8.1 [32-bit/64-bit] Windows 10 [32-bit/64-bit] Windows Server 2008 R2 [64-bit] Windows Server 2012 R2 [64-bit] Windows Server 2016 [64-bit]	Internet Explorer 11 Edge Firefox 40 or later (*1) Chrome 47 or later (*1)	-	JRE 7 [32-bit] JRE 8 [32-bit] JRE 7 [64-bit] JRE 8 [64-bit]
Local Agent	Windows 7 [32-bit/64-bit] Windows 8/8.1 [32-bit/64-bit] Windows 10 [32-bit/64-bit] (*3)	-	.NET Framework 3.5 (*2)	-

SYSTEM RECOMMENDATIONS

Mobile for Android	Android 4.1 or later	-	-	-
Mobile for iOS	iOS 8.0 or later	-	-	-
DRD (Device Registration and Diagnostics)	Windows 7 [32-bit/64-bit] Windows 8/8.1 [32-bit/64-bit] Windows 10 [32-bit/64-bit] Windows Server 2008 R2 [64-bit] Windows Server 2012 R2 [64-bit]	-	.NET Framework 4	-
DCT (Data Collection Tool)	Windows 7 [32-bit/64-bit] Windows 8/8.1 [32-bit/64-bit] Windows 10 [32-bit/64-bit] Windows Server 2008 R2 [64-bit] Windows Server 2012 R2 [64-bit]	-	.NET Framework 4	-

(*1) It is recommended to use the latest official version available.

(*2) Windows 8/8.1 requires ".NET Framework 3.5 (includes .NET 2.0 and 3.0)" to be enabled in Windows features.

(*3) In a non-domain environment, remote installation of the Local Agent from KFS Gateway for Windows may require alteration of a registry key on the target PC, as instructed in the following link, in order to enable administrative shares of the file system. This is documented in the Gateway User Guide.

https://support.microsoft.com/en-us/kb/942817

Table 9: Summary of system recommendations

ABOUT KYOCERA

KYOCERA Document Solutions Inc. is a wholly owned subsidiary of KYOCERA Corporation, which marked its 50th anniversary in 2009. KYOCERA Document Solutions is one of the world's leading office document solutions companies. Its range of products and services includes Ecosys printers, reliable multifunctional systems, high-quality consumables, a comprehensive portfolio of software solutions and Managed Document Services (MDS).

KYOCERA Document Solutions

KYOCERA
Document Solutions