KYOCERA Fleet Services
Version 1.3
Security White Paper

For Customers

Document Version 082016
September 2016

Corporate Software Division
KYOCERA Document Solutions Inc.

TABLE OF CONTENTS

Introduction

Purpose

The purpose of this document is to inform customers about the security measures implemented in KYOCERA Fleet Services (KFS).

KYOCERA's first priority is to provide secure protection of information assets that are handled by KFS. The information assets are rigorously protected by the secure configuration and security features of KFS.

Target Audience

The target audience for this document are customers of KYOCERA Document Solutions Inc. (KYOCERA).

Document Structure

This document is organized into the following sections:

- KFS Overview
- Protection of Information Assets
- Security
- Security Technical Details
- Low Compliance
- Appendix

Edition Notice

The information contained in this document is subject to change without notice. Changes and improvements in KFS may be incorporated in later editions without prior notice.

KFS Overview

This section describes KFS overview and configuration .

What is KFS?

KFS is a cloud service developed for customers using MFP/Printer (devices) to reduce service costs and improve operational support. KFS can remotely collect and centrally manage device information.

KFS **Management Feature** and **Tasks**.

Management Feature provides centralized management and monitoring of KYOCERA devices and of competitors devices. Thus, improving utilization of assets and increasing productivity. Management Feature allows you to:

- Read counters
- Create reports
- Check the status of consumables
- Assist ordering system
- Monitor device operation status

Tasks are only available for KYOCERA devices. Increased customer satisfaction is achieved through quick remote customer support, such as:

- System setup
- Detailed device information
- Device diagnosis
- Troubleshooting of devices
- Remote firmware updates
- Remote maintenance

KFS Configuration

KFS consists of **KFS Manager, KFS Device, KFS Mobile** and **KFS Gateway.**

KFS Manager is the backbone of KFS using the cloud system of Microsoft Azure.

KFS Manager, communicates with KFS Device, KFS Mobile and KFS Gateway and manages devices via these components. KFS Manager also provides device information to these components.

KFS Manager, provides features such as remote firmware updates, device restarts and remote maintenance mode utilization. In addition, KFS Manager provides a web-based user interface to manage devices, components and users.

In order to enable two-way communication, KFS Device, KFS Mobile, and KFS Gateway must be registered in KFS Manager.

KFS Device is a module embedded in a device at a customer's site.

KFS Device provides device logs, counters and status pages, upon request, and is scheduled in KFS Manager. KFS Device sends device information to KFS Mobile via Bluetooth™, USB™ or Wi-Fi Direct™ .

KFS Mobile is an application installed on authorized service personnel's mobile devices, such as smart phones and tablets.

KFS Device/KFS Gateway communicates with KFS Manager on a customer's network (i.e. LAN), while KFS Mobile is used when KFS Device/KFS Gateway cannot connect to the customer's network (i.e. LAN). KFS Mobile uses peer-to-peer communication, such as Bluetooth, USB or Wi-Fi Direct to connect to devices and obtains various information from devices.

Similarly with KFS Device, KFS Mobile sends device data to KFS Manager. In addition, KFS Mobile provides features to display device information and event logs.

KFS Gateway is a Windows application that is installed on a PC.

KFS Gateway connects KYOCERA devices and non-KYOCERA devices to KFS Manager via the internet. Non-KYOCERA devices can be monitored, but only KYOCERA devices can be maintained with device restart, firmware updates, and snapshots functions.

KFS Gateway supports Single-Point of Outgoing Connection, providing the capability to consolidate the point of contact to the external internet into one point. Consequently, only one address needs to be added in the whitelist of outbound firewall.

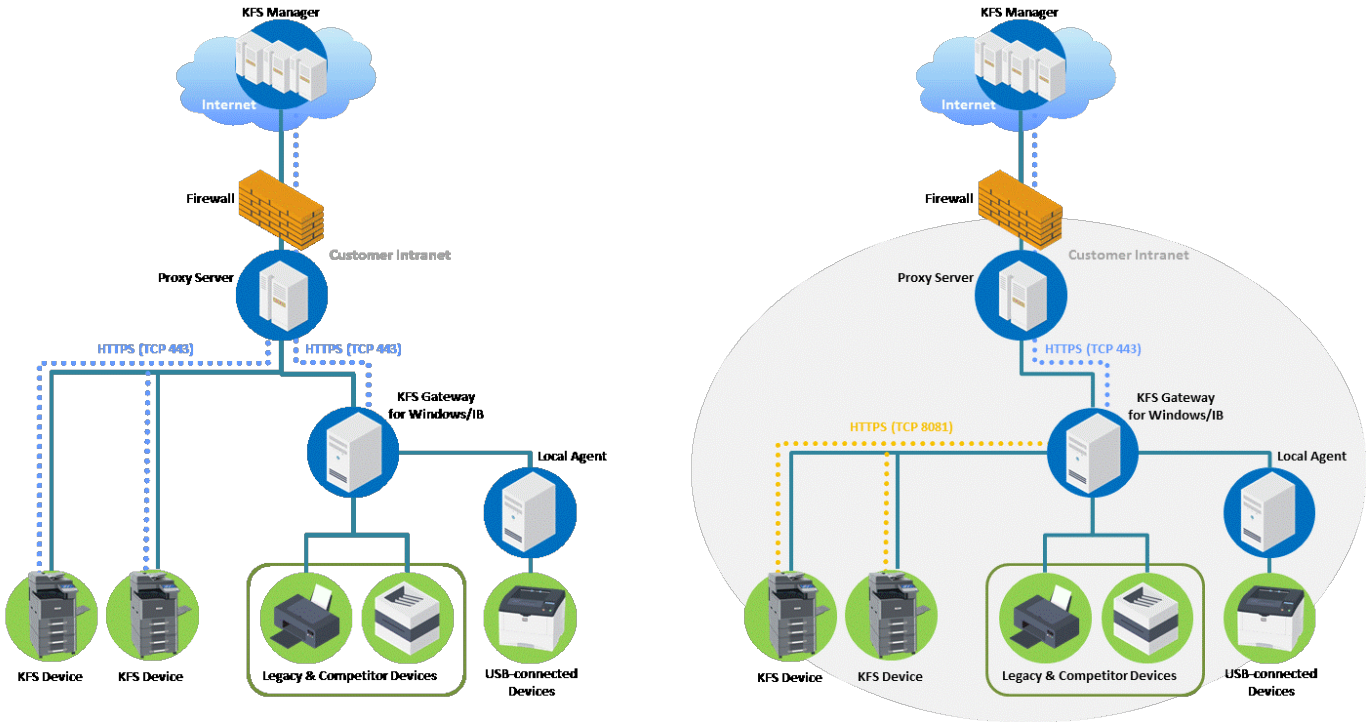

Figure 1 Comparison of Connection With (the Right Figure) and Without (the Left Figure)

Single-Point of Outgoing Connection

Note: KFS Gateway availability may vary by region.

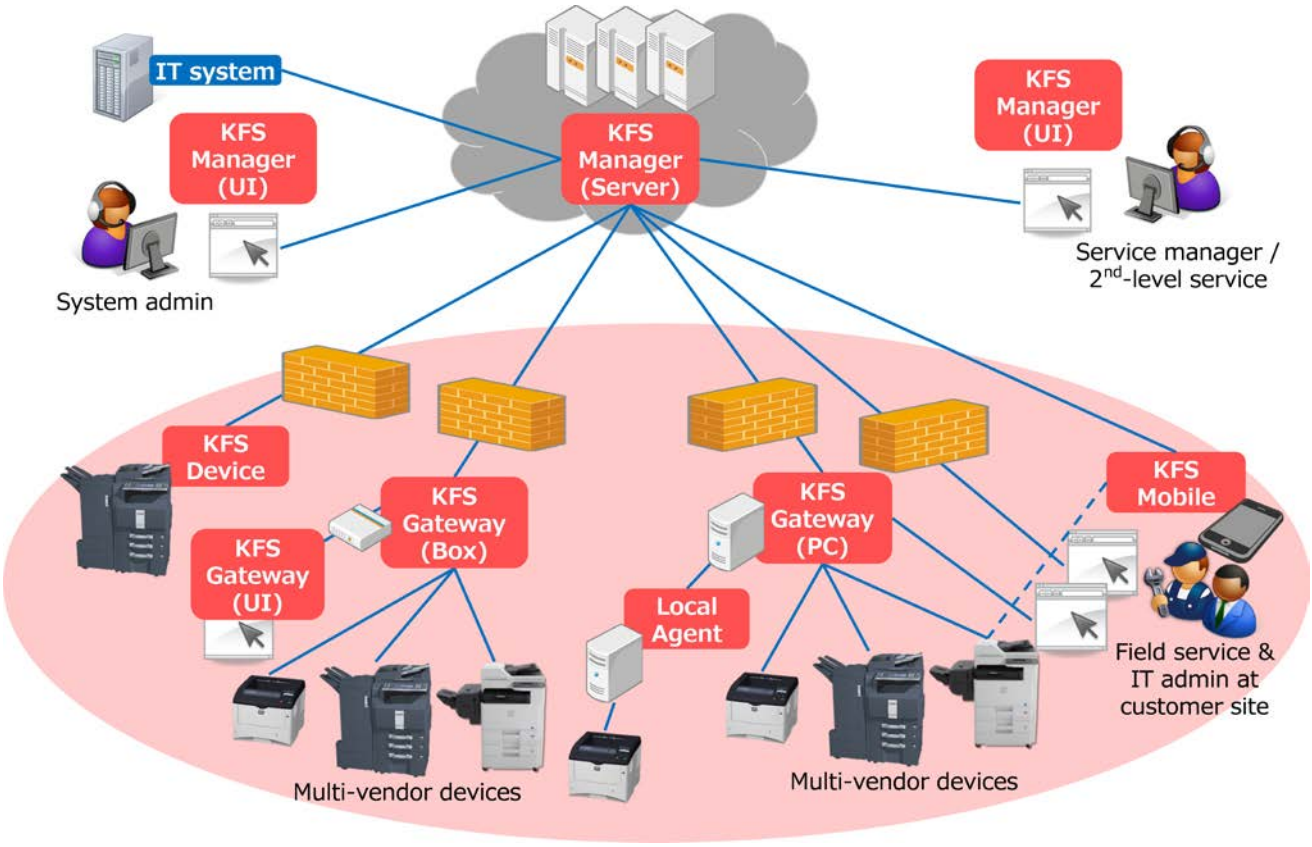

Figure 2 KFS Configuration

Protection of Information Assets

When using KFS, the following information assets handled through KFS are strictly protected.

See Security section for protection measures

Device information obtained from the customer's environment

The device information obtained from customers' devices only contains information necessary for management and maintenance of the devices. It does not contain a customer's personal information, such as the address book. The device information is sent to KFS Manager, regularly, once a day. Table 1 shows the amount of data obtained from the KFS Device and the KYOCERA MFP device. In order to maintain an XMPP connection between KFS Manager and KFS Device/KFS Gateway, Keep-Alive connection is used every one minute. The total amount per connection: Keep-Alive per day is about 1,300 Kbytes, but this depends on packet sizes. The total amount of data obtained from an MFP device per day is 100 Kbytes or so. Thus, the total amount of the communication data is roughly 1,400 Kbytes.

Table 1 The Amount of Data

Communication Data	The frequency of data transmission	The amount of data communications per day	The total amount of data communications per day
• Counter • Toner Level • Device Log	Once a day *Counter/Toner Level data can be transmitted up to four times a day but once a day as the default setting.	80 Kbytes	1,400Kbytes
• Device 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	During remote maintenance operation	0 Kbytes *Not communicated without remote maintenance operation. *Data amount depends on device model and operation contents.	

Device Notification/Log (System Error, Event, Consumption, Counter)

When system errors or various events occur, such as a paper jam or low toner volume, the device sends event information to KFS Manager.

KFS Manager immediately notifies the designated users of events.

Device Setting

The following device setting information is obtained:

- Network Setting (e.g. Enhanced WSD)
- System Setting (e.g. Date/Time, Time Zone)
- E-mail Setting (e.g. SMTP, E-mail Send Settings)
- Print Setting (e.g. Eco Print)
- Copy Setting (e.g. Original Image, Prevent Bleed-through)
- FAX Setting (e.g. Continuous Scan, FAX TX Resolution)
- Default Setting (e.g. Scan Resolution)

Authorized service personnel can remotely perform optimal device settings upon receipt of customers' requests and approvals.

The authorized service personnel saves the device setting in KFS Manager and sends the device setting to the device when the device isn't being used.

Snapshot (Status, Service status, Event log, Maintenance report, USB log and FAX report)

Authorized service personnel can obtain snapshot data to remotely diagnose device problems utilizing KFS Manager.

Device Status (Panel message and Alert list)

Authorized service personnel can view panel messages and the alert list to remotely check the device status.

Maintenance Mode Setting

Authorized service personnel can remotely access maintenance modes and make adjustments for optimal performance.

Authorized service personnel can obtain device maintenance mode settings from KFS Manager.

The authorized service personnel adjusts the maintenance mode setting and sends it to the device from KFS Manager.

Data capture

Customers' print data is sent to KFS Manager.

Data capture is obtained only when the confirmation message is shown on the panel of the target device and the approval is gained from an IT administrator in advance. Authorized service managers can specify the period of time up to 7 days (default: 1 day) to remove the captured data. This setting can be done by each group. When reaching the specified period of time, the captured data will be removed automatically.

On-Demand USB Logs

The authorized service personnel select a device and retrieve on-demand USB Logs.

KFS Device generates USB Logs and sends it to the KFS Manager.

KFS Manager stores the USB logs received from KFS Device.

The authorized service personnel can download the USB logs to a PC from KFS Manager via a Snapshot list.

On-Demand USB Logs can be retrieved only when the confirmation of approval is gained from an IT administrator at customers' site. The device will be locked for several minutes (3 to 4 minutes) when retrieving. After the operation ends, the device will automatically be restarted. After device restarts, the USB logs are automatically downloaded to the user's PC from KFS Manager.

All of the remote services, like the above-mentioned features and HyPAS, are enabled as the default settings. The manager can then enable/disable the specific features as used by that group. Hence, only limited groups can use these particular features. The prohibited features are grayed out so a third party person cannot access these disabled features. This KFS secure configuration prevents information leaks, while maintaining user friendliness.

Table 2 Data and Attribute Data

Data	Attribute Data
Device Notification/Log	• System Error • Event（e.g. Paper Jam, Low Toner Volume） • Consumption • Counter
Data Setting	• 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 Bleed-through） • FAX Setting（e.g. Continuous Scan, FAX TX Resolution） • Default Setting（e.g. Scan Resolution）
Snapshot	• Status • Service Status • Event Log • Maintenance Report • USB Log • FAX Report
Device Status	• Panel Message • Alert List
Maintenance Mode Setting	• Device Adjustment
Data Capture	• Customers' Print Data
On-Demand USB Logs	• USB Logs

Information utilized in KFS

KFS Component	Information Assets (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 authorized service technician to log into 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 into KFS Manager • Proxy authentication information used by a KFS Mobile and paired KFS Device when connecting to KFS Manager through the proxy server

Security

This section explains in detail how the information assets mentioned in the previous section are protected by various security features that have been implemented in KFS. Unless given permission by customers, information cannot be accessed by any organization, including sales companies and other tenants(*4).

(*4) Tenant indicates users who use KFS.

Access Control

KFS strictly enforces user and device data access control in order to prevent leakage of information. Access to KFS is controlled by treating a group as one unit, thus, giving access right to users and devices registered only to that group.

Data Management

Users can access devices located at their user site and securely manage these devices. As shown in Figure 3, KFS Gateway and KFS Device are positioned under a group that is Customer 1. A user can access the KFS Gateway and KFS Device and also, securely manage their user data and device data.

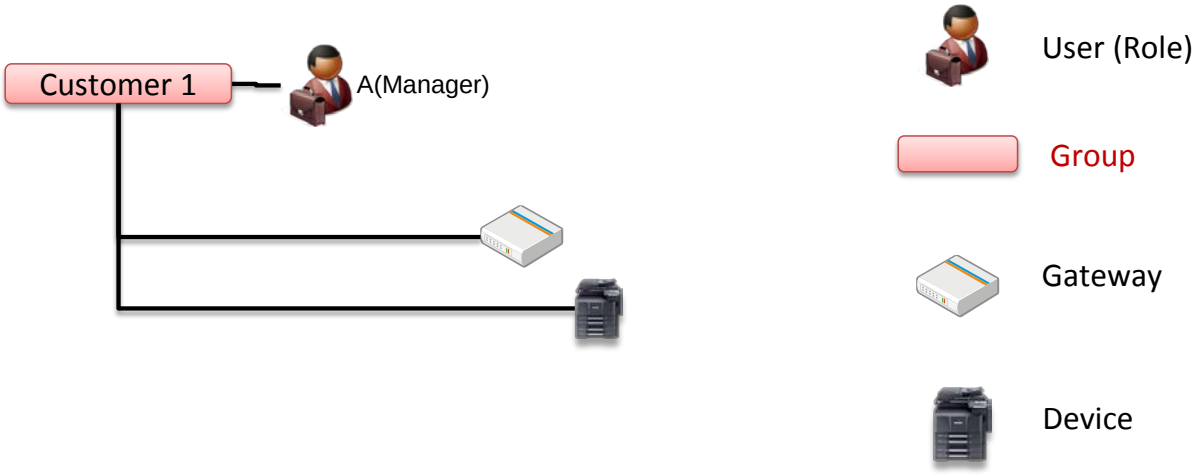

Figure 3 Data Management

User Account Management

User Account is created and managed within a group.

One of the following roles is assigned to every user.

The Manager role also includes the Customer role.

- Manager
- Customer

- **Manager**

  Manager is assigned to one or more users in a group and in addition, also maintains the child groups to which he/she belongs.

  Manager can add or delete the groups managed by him/her. Manager can also add new user accounts, as well as edit, delete, and change status.

- **Customer**

  Customer manages the onsite customer devices. Additionally, the customer can create and issue a report template used by that customer.

Password Settings

When a user account is initially created in KFS Manager, KFS Manager sends a notification to user via an email. This email contains an automatically generated user ID, a temporary password and a link to the service URL. If the user account is created but is in an invalid state, the KFS Manager will not send an email notification to the user.

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 sent to the user will no longer be valid.

This stringent security setting prevents password from being stolen by malicious persons.

Data Access Control Policy

Access to data stored in KFS is controlled by the user role, as well as the access code that is linked to the user's group. Access to data is strictly restricted according to the user roles.

Manager can access all the data in their group and all the data in child groups.

Customer can access device properties in their group and in child groups. However, access rights need to be set by Manager.

Manager can access device log data, but Customer cannot access the device log data.

Registration into KFS

In order for KFS Manager to manage MFP devices through KFS Device/KFS Gateway/KFS Mobile, mutual registration between KFS manager and KFS Device/KFS Gateway/KFS Mobile must be performed in advance.

When devices are registered in KFS, they can have a status of “Pending” or “Managed”. The status depends on the method of registration. This is also true when registering a device from a device panel or performed remotely.

- If registered with just the access code of the group, status will be “Pending”. In order to change to “Managed,” an authorized user must change the status
- If registered with a user name, password and access code, the status will be “Managed”

Since users must identify themselves in order to register a device as “Managed”, unauthorized access is prevented.

The access logs indicate who, when and to where the access occurred and can be used to help trace the unauthorized access.

Identification and Authentication

When accessing KFS, a user must log in with the registered User ID. An unauthorized user cannot access KFS.

Accessed information is recorded, even when logging in and will be available for auditing.

The following features are supported as security features for login:

Account Lockout Policy

When a user fails to login a pre-determined number of times, the user account will be locked for a certain period of time.

As shown in Table 3, when reaching the account lock-out threshold for failed login attempts of three times, the account will be locked. The setting will unlock the account after 30 minutes.

Table 3 Account Lockout Policy

Number of continuous failed login attempts	3 times
Auto Unlock Time	30 minutes later

The Account Lockout Policy setting protects KFS against password cracking attacks.

Auto-Logout Policy

The user will be automatically logged out if their account has been idle for a certain period of time after being logged in. The auto-logout time is 30 minutes.

This feature prevents unauthorized operation of KFS by a malicious attacker. This is especially true if a user has left their desk without logging out.

Password Policy

A user needs to employ a strong password that is difficult to be analyzed and must be applicable to the KFS Password Policy. The password length and complexity of password are as defined in Table 4.

Table 4 Password Policy

Password Length	8 characters
Password Complexity	Include at least one or more numbers between 0 and 9, upper case letters, lower case letters and special symbols

A password that does not meet the password policy is prohibited. This policy prevents simple passwords from being set by users and guards against unauthorized access by a third person.

Audit Logs

KFS records audit logs of various events. The logs provide a record that can be checked to verify that KFS is secure.

Audit Logs of KFS Manager

An audit record is generated by KFS Manager for the following event:

- 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

Audit Logs of KFS Gateway

An audit record is generated by KFS Gateway for the following event:

- Successful/unsuccessful user identification and authentication
- KFS Gateway local administrator password reset
- Configure device recovery settings
- Configure security settings
- Terminate inactive sessions

The history above shows the time/date and result (Success/Failure). In the event of alteration or leak of information, the audit logs can be used to investigate and help trace the unauthorized access.

Protection of Stored Data

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

The information assets are protected against information leaks.

Table 5 Encryption Strength

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

Protection of Communication Data

KFS protects the communication of data when a user accesses KFS. In order to protect KFS communication data from masquerading, tapping or modifying the data, the communication data is encrypted, and KFS components are mutually authenticated.

User Access

When a KFS user accesses KFS via a web browser, an authenticated communication channel is established.

Communication to access KFS via Web browser

KFS users can access KFS Manager from the Web browser's client UI, regardless of the user role. 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. KFS Manager protects the communication data through HTTPS.

Data Communication

KFS sends and receives encrypted data to and from devices via the internet and local area network.

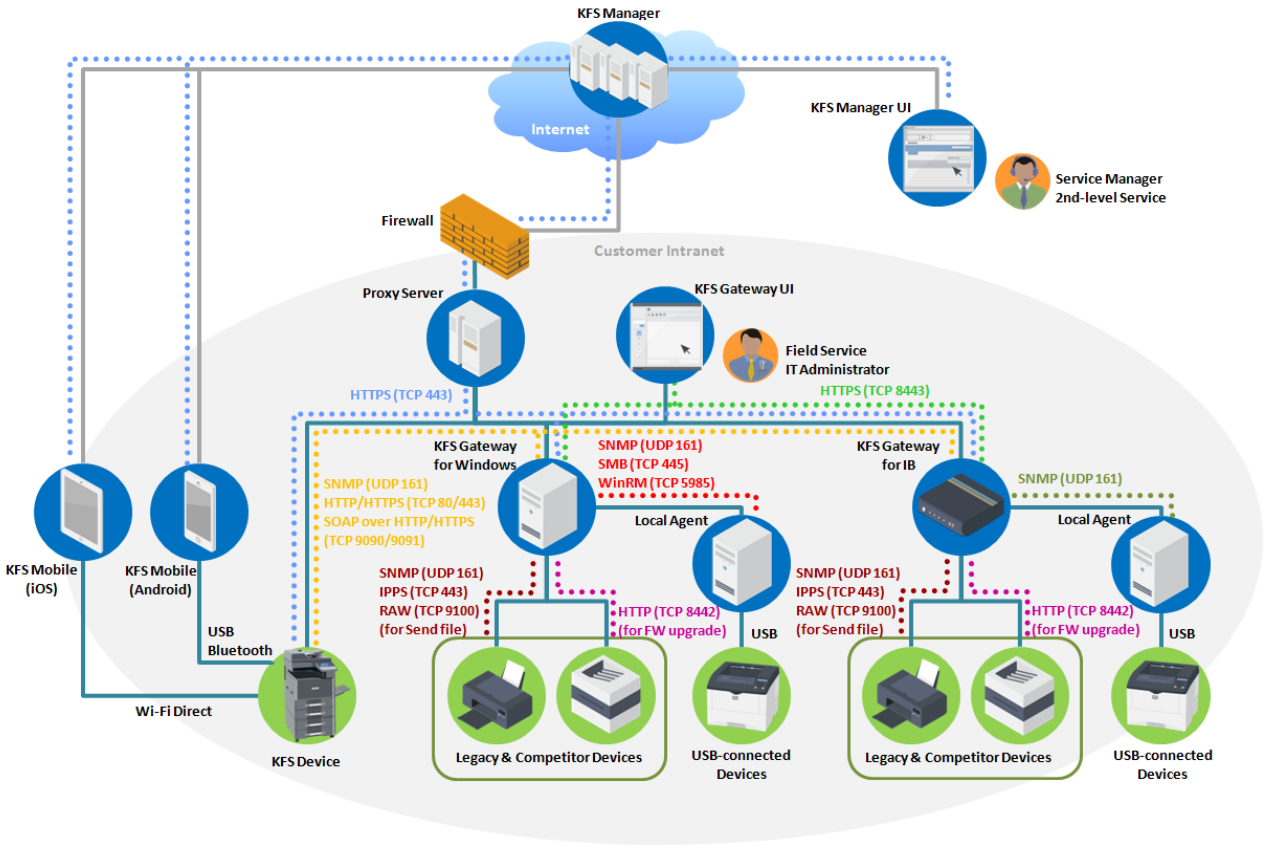

Figure 4 KFS Components and Data Flows

Communication with KFS via Internet

KFS network communication is set up by XMPP server and KFS Manager in the cloud. XMPP protocol uses HTTPS protocol for transporting. 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 firewall. HTTPS protocol protects the data on the communication channel.

Communication with KFS via Local Area Network

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 packet flowing on the network.

The communication via local area network is controlled by setting a range of the subnet mask, IP address and host name. There is no unintended transmission to the network.

Communication with other KFS Components

One-to-one secure communication between KFS Mobile and device can be set up via encrypted Bluetooth/Wi-Fi Direct and USB. Data will not be passed through the local area network.

Table 6 Protocol/Interface and Data Communication

Protocol/Interface	Data Communication
• Extensible Messaging and Presence Protocol (XMPP)	➢ Communication between KFS Manager and XMPP Server ➢ Communication between XMPP Server and KFS Gateway/KFS Device
• Hyper Text Transport Protocol Secure (HTTPS)	➢ Communication between Web browser's client UI and KFS Manager ➢ Communication between Web browser's client UI and KFS Gateway ➢ Communication between KFS Manager and XMPP Server ➢ Communication between XMPP Server and KFS Gateway/KFS Device
• Simple Network Management Protocol (SNMPv3)	➢ Communication between KFS Gateway and device
• Bluetooth • USB • Wi-Fi Direct	➢ Communication between KFS Mobile and KFS Device

Tasks

Tasks are performed by an operator through KFS Manager or by authorized service personnel when visiting the customer's office environment. These tasks cannot be performed without the customer's agreement. Users who can perform these tasks on KFS are restricted by identification and authentication. Data handled through respective tasks are protected by encryption of communication channels and mutual authentications.

Communication of Remote Firmware Update

Firmware update communication from KFS Gateway/KFS Device

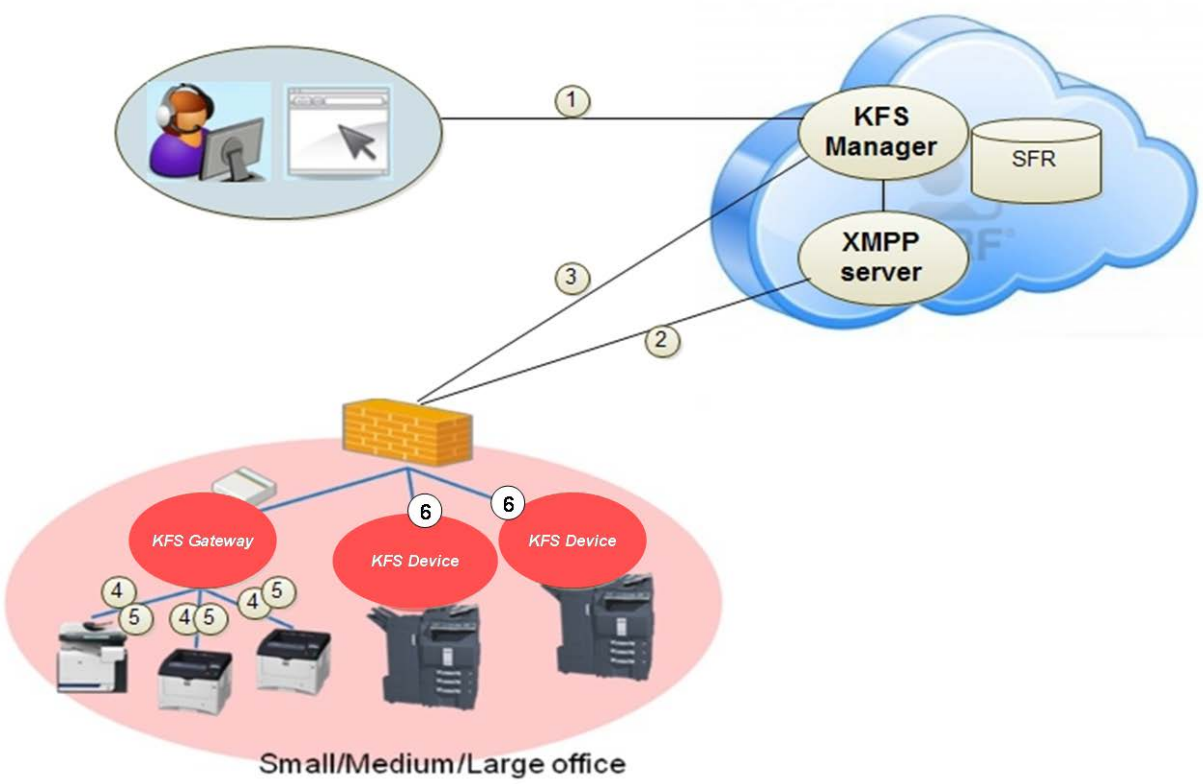

Figure 5 Communication flow of firmware update from KFS Gateway/KFS Device

As shown in Figure 5, a secure firmware update to KFS Gateway/KFS Device is achieved with the above-mentioned secure communication through the following steps:

1. User selects a firmware package for a device through KFS Manager Web browser's client UI. The communication between Web browser's client UI and KFS Manager is protected through HTTPS.
2. KFS Manager initiates secure communication with KFS Gateway/KFS Device through XMPP protocol and sends firmware update commands to KFS Gateway/KFS Device.
3. KFS Gateway/KFS Device securely downloads firmware packages from KFS Manager through HTTPS.
4. KFS Gateway sends firmware update command to devices.

5. Device downloads firmware package from KFS Gateway and updates the firmware.
6. KFS Device updates the firmware on the machine.

Firmware update communication from KFS Mobile

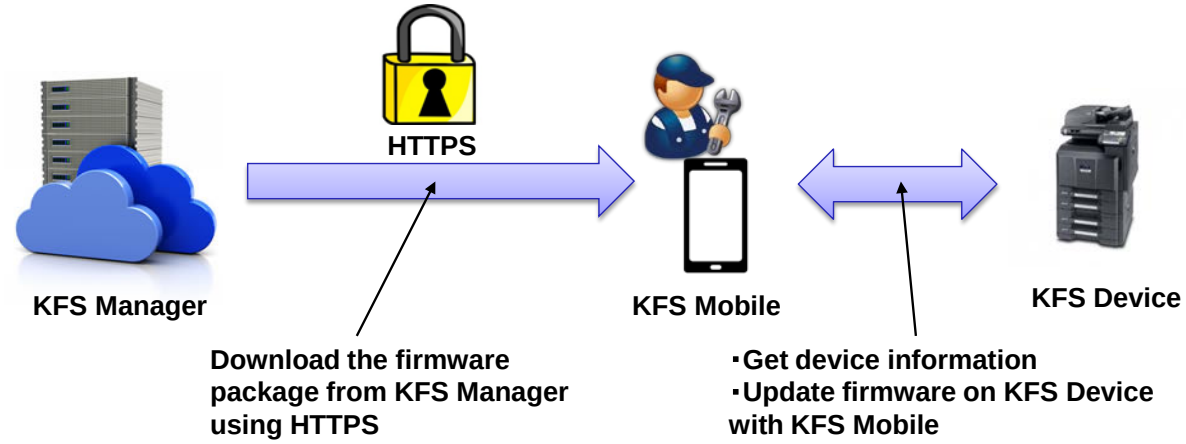

Figure 6 Communication flow of firmware update from KFS Mobile

When the network at a customer site cannot be accessed from KFS Manager, firmware updates can be performed on a device with KFS Mobile. This is achieved with the above-mentioned secure communication through the following steps:

1. The authorized service personnel use KFS Mobile to check the latest firmware package from KFS Manager.

   KFS Mobile uses HTTPS to securely download the firmware package from KFS Manager.
2. KFS Mobile initiates communication with KFS Device, sends firmware update command to KFS Device when only USB or Wi-Fi Direct is used, and then updates the firmware.

Communication of Remote Device Panel Capture

KFS provides a remote device panel capture feature that can display the current panel image of a managed device on KFS Manager UI. This feature obtains device panel information (such as the most recent device snapshot or the device log) only when the confirmation message is shown on the panel of the target device and the users' approval is given in advance.

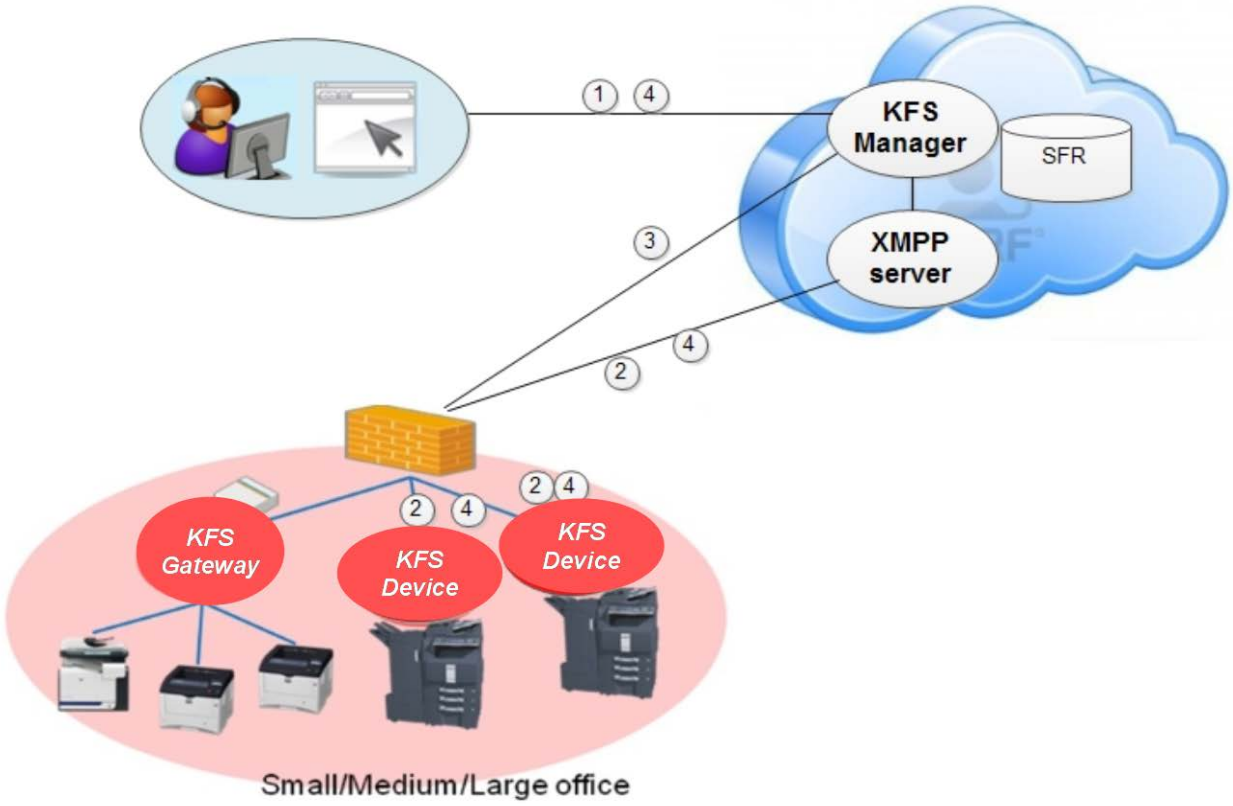

Figure 7 Communication flow of remote device panel capture

As shown in Figure 7, the remote device panel capture is achieved with a secure communication through the following steps:

1. KFS Manager user requests device panel information from KFS Manager Web UI through HTTPS.
2. KFS Manager initiates communication with KFS Device through a secure XMPP protocol communication, and sends captured device panel information to KFS Device.
3. KFS Device sends the image of the device's current panel information to KFS Manager through HTTPS. KFS Device updates the captured image every time the panel screen of the device is updated.
4. KFS Manager can terminate this process by sending a stop command to KFS Device through a secure XMPP communication channel.

Communication for obtaining Remote Device Snapshot Data

In order for KFS user to perform diagnosis of device problems, the following device snapshot data can be obtained from KFS Manager Web UI.

- Status page
- Service status page
- Network status page
- Maintenance report
- Application status page
- Event log
- USB log
- FAX report

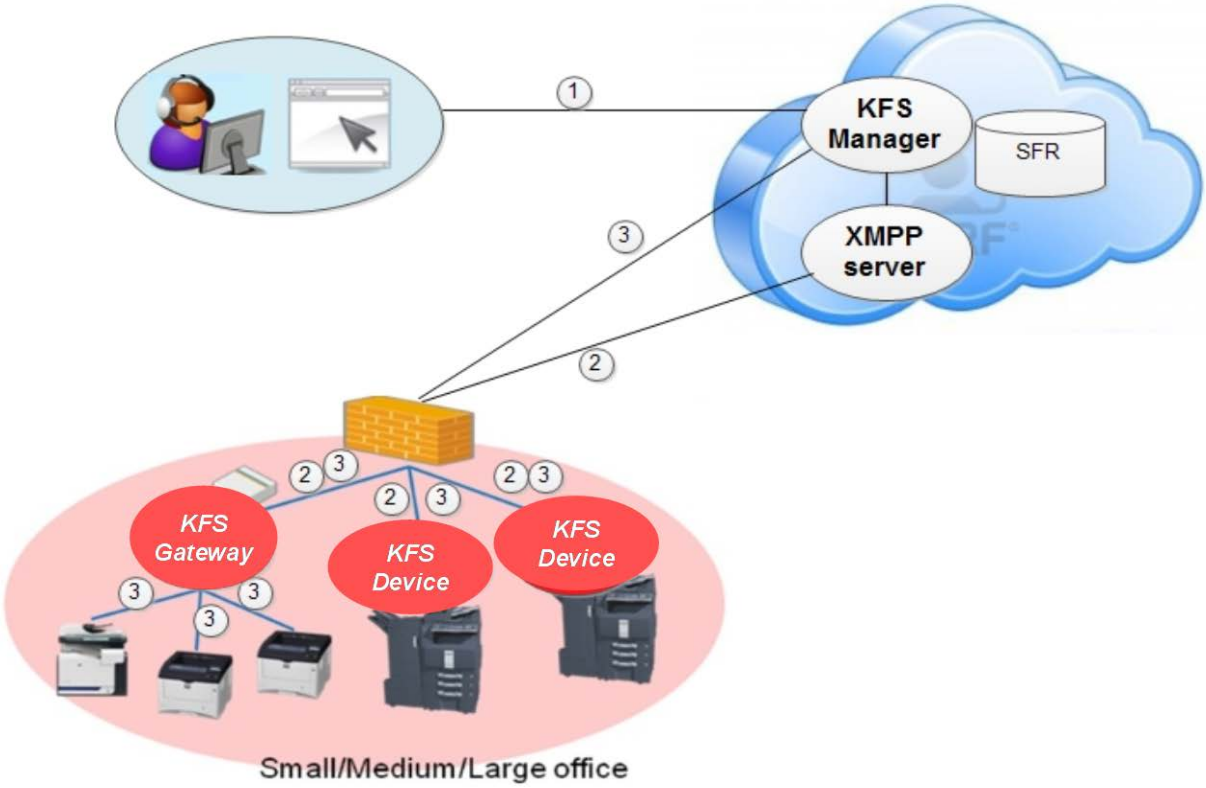

Figure 8 The flow of obtaining remote snapshot data

As shown in Figure 8, the KFS remote device snapshot feature uses secure communication:

1. KFS Manager user requests device snapshot information from KFS Manager Web UI through HTTPS.
2. KFS Manager initiates communication with KFS Gateway/KFS Device through a secure XMPP protocol and sends the snapshot command.

3. KFS Gateway/KFS Device retrieves snapshot information from a specified managed device and sends the snapshot information to KFS Manager through HTTPS.

Communication of Remote HyPAS Management

KFS provides remote HyPAS management, such as remote installation, uninstallation, activation and deactivation of HyPAS applications on KFS Devices.

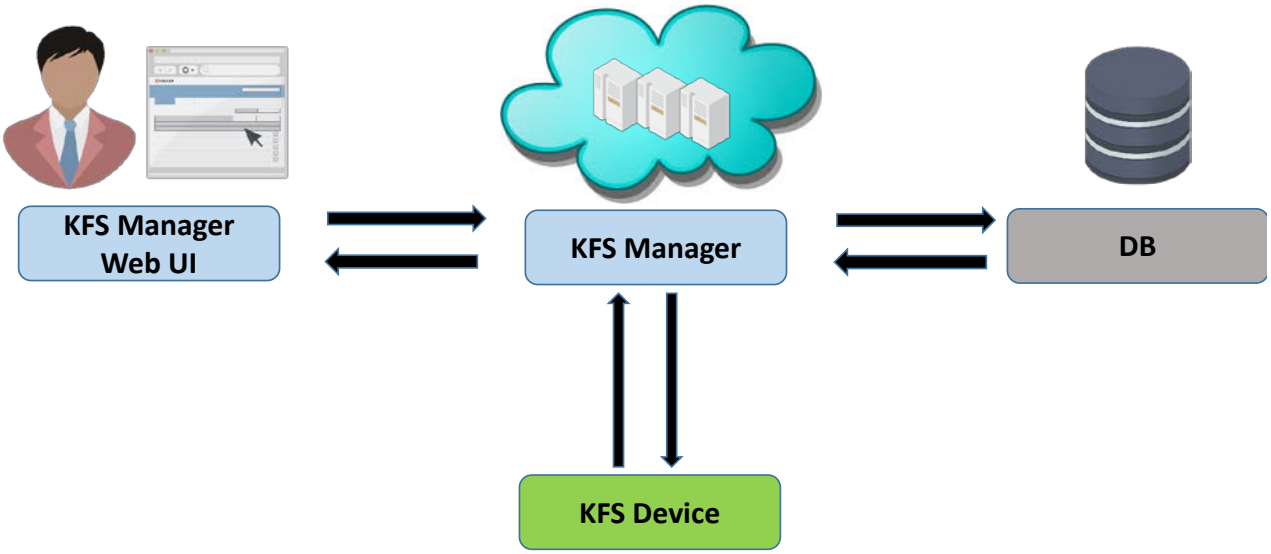

Figure 9 The flow of remote HyPAS management

As shown in Figure 9, the remote HyPAS management is achieved with a secure communication through the following steps:

1. KFS Manager user requests a list of HyPAS applications from KFS Manager Web UI through HTTPS.
2. KFS Manager initiates communication with KFS Device through a secure XMPP protocol communication, and sends KFS Device a list of HyPAS applications to install/uninstall/activate/deactivate the HyPAS application. The license key involved in the HyPAS activation process is also securely transmitted over XMPP and encrypted by AES before securely storing in Azure DB.
3. KFS Device downloads the encrypted HyPAS application package file from KFS Manager through HTTPS (in case of installing the application).
4. KFS Manager can terminate this process upon receipt of notification directly from KFS Device when action is complete.

Security Technical Details

This section describes defense against security threats and hosting environment.

Defense against Security Threats

KFS relies on Microsoft Azure for protection at the infrastructure level of its cloud services and virtual machines against malicious attempts. Such protections are distributed as 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. Azure also provides an internal DNS to secure internal 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. Refer to the Microsoft Azure Network Security White Paper http://download.microsoft.com/download/C/A/3/CA3FC5C0-ECE0-4F87-BF4B-D74064A00846/AzureNetworkSecurity_v3_Feb2015.pdf for more technical details.

At the application level, KFS is continually diagnosed by a third party 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 reported from other sources are promptly resolved to keep the application secure.

Specifically, against password cracking, KFS responds to a failed authentication request with a delay.

Hosting Environment

KFS Manager is hosted on the Microsoft Azure platform. Microsoft meets a broad set of international and industry-specific compliance standards, such as ISO 270001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia CCSL, UK G-Cloud, and Singapore MTCS. Microsoft was also the first to adopt the uniform international code of practice for cloud privacy, ISO/IEC 27018. Microsoft also offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the European Economic Area (EEA).

The Azure platform provides multiple layers of security. Inbound from the Internet, there is Azure DDoS protection watching for large scale attacks against Azure. Passing this would reach the service endpoints specifically configured for customer deployments (such as KFS). The endpoints translate publicly-exposed IP addresses and ports to internal addresses and ports on the Azure Virtual Network. The Azure Virtual Network ensures complete isolation from all other networks and that traffic only flows through customer configured paths and methods. These paths and methods are the next layer of protection, where traffic is controlled with the help of access control lists (ACLs).

Information Regulations

KYOCERA Document Solutions Inc., does not believe that KFS will impact certain federal laws related to privacy and confidential information because KFS does not collect, house, 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.

Appendix

Please refer to Figure 4 KFS Components and Data Flows.

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 both Windows and IB) 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 KM-WSDL 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. Thus, the inbound rule created will be deleted when KFS Gateway for Windows is uninstalled.
  - The above settings are preconfigured in KFS Gateway for IB when it is shipped.

On the Machine Hosting Local Agent

- 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.
  - Refer to the KYOCERA Fleet Services Gateway User Guide for detailed instructions about how to enable WMI and WinRM.
  - 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.