KYOCERA Document Solutions Inc.

KYOCERA Fleet Services
Version 2.0
Security White Paper

For Customers

History of revisions

Data	Version	Description	Author
August 7, 2015	Beta	First version For Dealers and Customers	Koto Takasu
September 9, 2015	Gamma	For Customers	Koto Takasu
September 30, 2015	1.00	For Customers	Koto Takasu
November 11, 2015	1.01	Added: - Network Load Figure 3 KFS Components and Data Flows	Koto Takasu
December 18 , 2015	1.02	Corrected and Updated: - Figure 3 KFS Components and Data Flows Added Sections: - Security Technical Details - Law Compliance Appendix	Koto Takasu Takumi Nakamura
February 2, 2016	1.03	Updated: - Table 1 The Amount of Data - Explanation about the amount of data - Explanation about the remote services Added: - Communication of Remote HyPAS Management	Koto Takasu
June 17, 2016	1.04	Added: - More details about information used by KFS including identifiable information (see p12-15) Deleted:	Koto Takasu Takumi Nakamura

		One sentence to eliminate redundancy (see “Protection of Stored Data” on page 21)	
August 2, 2016	082016	Added: - On-demand USB Log - Delete captured data automatically after limited time - Single-point of outgoing connection - Figure 1 Comparison of Connection with and without Single-Point of Outgoing Connection - Audit Log upon downloading of captured data - TCP port 8443, 9090, 9091, 8442 and 8081 (see “On the Machine Hosting KFS Gateway for Windows”) Updated: Figure 4 KFS Components and Data Flows	Koto Takasu Takumi Nakamura
September 21, 2016	092016	Deleted: - Law Compliance Added: - Health Insurance Portable & Accountability Act (HIPAA) Corrected: Password Length	Koto Takasu
February 13, 2017	022017	Deleted: - Single-Point of Outgoing Connection (p7) - Description about customer’s personal information (p9) Corrected: - Password Settings (p19)	Koto Takasu

		- Hosting Environment (p33) Updated: - User Account Management (p19) - Data Access Control Policy (p19) - Registration into KFS (p20) - Communication with KFS via the Internet (p26) Added: - “and send file function” to the description about KFS Gateway (p8) - Description about personally identifiable information (p10) - Note (*2) (p10) - Backup Data to Table 1 (p10) - Description about Backup Data to Table 2 (p13-14) - Connection Mode (p21) - Single-Point of Outgoing Connection (p22) - Table 6 How the key length is generated and managed (p26) Note about firmware upgrade (p29)	
July 25, 2017	072017	Added: - Responsibility lies in terms of authentication information - Protection and management of audit logs - KYOCERA’s efforts ensuring KFS Security - Data that is deleted and not deleted - The method of deleting data	Koto Takasu

		- The base time used in the timestamp of audit logs - Vulnerability check method for the infrastructure and OSS Deleted: Auto-Logout Policy	
September 7, 2017	092017	Changed and Added: - Automatic Upgrade for KFS Gateway - Protection of Stored Data - Encryption - Data Backup Deleted: - A phrase (from “Communication of Remote Panel Capture”) A sentence (from “HIPAA)	Koto Takasu
October 16, 2017	102017	Changed: - Figure 5 KFS Components and Data Flows Deleted: Description about WinRM (TCP 5985) (from “On the Machine Hosting Local Agent”)	Koto Takasu
February 27, 2018	022018	Added: - Mobile Client (application UI) - BCC option - Transferring user’s report schedule, notification criteria and templates - ISMS certification Changed and Added: KFS Gateway (Java Gateway/NetGateway)	Koto Takasu

March 27, 2018	032018	Updated: - More accurate and precise data listed in Table 2 and Table 3 Descriptions about these tables	Koto Takasu
September 28, 2018	092018	Updated: - Added conditions to Table 2 - Added Application status to Snapshot - Deleted note from “Single-Point of Outgoing Connection” - Corrected “Audit Logs” - Corrected description of “Local area network communication between KFS Gateway and device” - Added relay server to Table 12 - Corrected description of KFS Mobile in Table 12 - Added “Communication of Remote Panel” - Corrected description about ISMS certification - Added description to “On the Internet Firewall” Added description to “On the Machine Hosting KFS Gateway (NetGateway)”	Jumpei Takagi
July 5, 2019	072019	Updated: - Deleted Gateway for IB description - Added description to “Password Policy” Added description to “On the Machine Hosting KFS Gateway (NetGateway)”	Jumpei Takagi
September 6, 2019	092019	Updated: Added Server Certificate description	Jumpei Takagi

January 10, 2020	012020	Added: - Add annotation in KFS Configuration - Add annotation in Audit Logs of KFS Manager - Add annotation in Encryption Updated: - Deleted description of Access Control	Jumpei Takagi
April 27, 2020	042020	Updated: - Delete description of JavaGW Added: Add Configuration list to snapshot	Jumpei Takagi
November 18, 2020	112020	Updated: - Update Key Length in Encryption - Update Outline of ISMS Cloud Security Certification Registration - Delete description of The vulnerability validation (dynamic and diagnostic tests) in Defense against Security Threats Added: - Add Data anonymization mode by KFS Gateway	Jumpei Takagi
May 19, 2021	052021	Added: description about Hashing and Table 10 Updated: description about ISMS Cloud Security certification	Koto Takasu
February 8, 2022	022022	Added/Changed description due to installation of MQTT server on cloud	Koto Takasu

Table of contents

Introduction

Purpose

The purpose of this document is to inform customers about the security measures 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 is customers of KYOCERA Document Solutions Inc. (KYOCERA).

Document Structure

This document is organized into the following sections:

- KFS Overview
- Protection of Information Assets
- Security
- Kyocera's effort for KFS Security
- Security Technical Details
- Health Insurance Portable & Accountability Act (HIPAA)
- Appendix

Edition Notice

The information contained in this document is subject to change without notice. This document could include minor errors. 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 information of devices distributed in a certain region.

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

Management Feature provides centralized management and monitoring of Kyocera devices and of competitors devices, 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. They can increase customer satisfaction by providing rapid remote customer support, such as:

- system setup
- detailed device information
- device diagnosis
- troubleshooting of devices
- remote firmware upgrades
- 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 upgrade, device restart and remote setting of maintenance mode. In addition, KFS Manager provides a web-based user interface and also a mobile application user interface to manage devices, components and users.
>
> In order to enable two-way communication, KFS Device and KFS Mobile must be registered in KFS Manager.

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

> KFS Device provides device log, counter, status page based on the requests and schedule of KFS Manager. KFS Device sends device information to KFS Mobile via Bluetooth™, USB™ or Wi-Fi Direct™.

KFS Mobile is an application installed on service personnel's mobile devices such as smartphones and tablets.

> KFS Device/KFS Gateway communicates with KFS Manager on a customers' network (i.e. LAN). KFS Mobile is used when KFS Device/KFS Gateway cannot connect to the customers' 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 Mobile can be used as a mobile application interface to KFS Manager.

KFS Gateway is a NetGateway for Windows on a PC, which manages KFS Device as legacy devices under KFS Gateway.

> KFS Gateway connects Kyocera devices and non-Kyocera devices to KFS Manager via the internet.

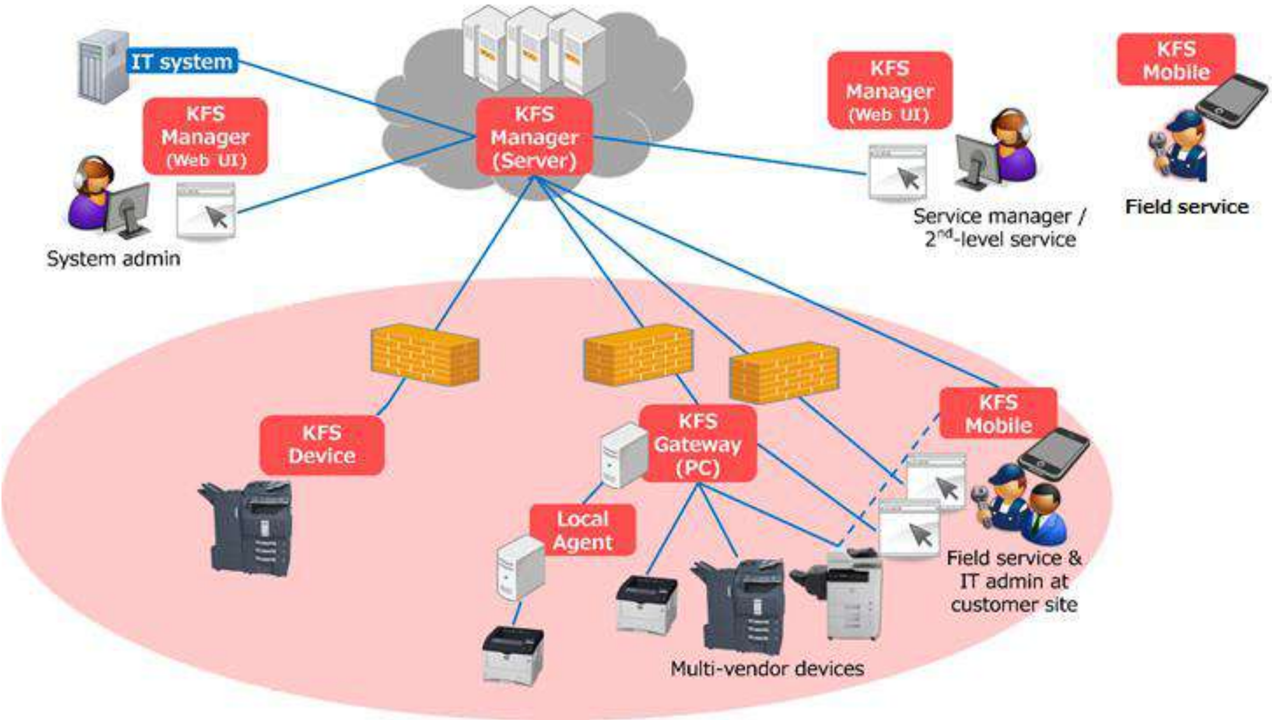

Figure 1 KFS Configuration

Protection of Information Assets

When using KFS, the following information assets handled through KFS are strictly protected(*2).

(*2) See Security section for protection measures

Device information obtained from the customer's environment

The device information obtained from customers only contains information necessary for management and maintenance of the devices. No personally identifiable information is transmitted without obtaining the customer's consent in advance.

Table 1 and Table 2 show the amount of data obtained from the devices using KFS Device, for example. The device information is sent to KFS Manager regularly once a day. To maintain an XMPP connection/MQTT connection between KFS Manager and KFS Device/KFS Gateway, the XMPP Keep-Alive connection/MQTT Keep-Alive connection is used every minute/every four minutes(*3). The total amount of connection: XMPP Keep-Alive/MQTT Keep-Alive per day is about 1,300 Kbytes/108 Kbytes but this depends on packet sizes. The total amount of data obtained from an MFP device per day is about 100 Kbytes. Thus to maintain an XMPP connection and an MQTT connection, the total amount of communication data is roughly 1,400 Kbytes and 208 Kbytes, respectively.

(*3) However in Monitor mode, neither an XMPP connection nor an MQTT connection is established between KFS Device and KFS Manager. Refer to Connection Mode for more details.

Table 1 The Amount of Data

To maintain an XMPP connection

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 minute	1,300 Kbytes	
• Device Setting • Snapshot • Device Status • Maintenance Mode Setting • Data Capture • On-Demand USB Logs • Backup Data	During remote maintenance operation	0 Kbytes - Not communicated without remote maintenance operation. - Data amount depends on device model and operation contents.	

Table 2 The Amount of Data

To maintain an MQTT connection

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	208Kbytes
• Device Notification	Per each alert event	20 Kbytes	
• Connection: Keep-Alive	Every four minutes	108 Kbytes	
• Device Setting • Snapshot • Device Status • Maintenance Mode Setting • Data Capture • On-Demand USB Logs • Backup Data	During remote maintenance operation	0 Kbytes -Not communicated without remote maintenance operation. - Data amount depends on device model and operation contents.	

Table 3 shows the amount of data transmitted from KFS Gateway to KFS Manager. The device information is sent to KFS Manager once a day. The total amount of data obtained from a MFP device per day is 7.3 Kbytes. As for the Gateway log, the audit log is 1 Kbyte, and the system log is 94 Kbytes when discovering and registering 10 devices. Additionally, discovery setting is 13 Kbytes when saving 10 discovering settings. However this amount of data can be different depending on the value of the discovery settings.

Table 3 The Amount of Data from KFS Gateway to KFS Manager

Communication Data	The frequency of data transmission	The amount of data communication per day
Counter	Once a day - Counter/Toner Level data can be transmitted up to four times a day but once a day as the default setting.	4 Kbytes (1 device)
Toner Level		2 Kbytes (1 device)
Device Notification	Per each alert event	1.3 Kbytes (1 alert)
Gateway Log	Once a day for each file (two zip files) - Audit Log - System Log	Audit Log: 1 Kbyte System Log: 94 Kbytes (Test performed after discovering and registering 10 devices)
Discovery Settings	Once a day for each discovery setting	13 Kbytes (10 discovery settings)

Table 4 shows the amount of data transmitted from KFS Gateway to the devices, which indicates the average usage of a KFS Gateway that have fewer than 25 registered devices. The amount of data transmitted depends on the number of registered devices. With regard to the frequency of data transmission, refer to Table 5. The amount of data communication per day for counter, toner level and device notification for each device is 1,776 Kbytes, 144 Kbytes and 21,600 Kbytes, respectively. Thus the total amount of data communication per day is 23,520 Kbytes.

Note that the more registered devices KFS Gateway has, the polling intervals automatically increase, which result in decreasing the total amount of data communication per day.

Table 4 The Amount of Data from KFS Gateway to the devices

Communication Data	The frequency of data transmission	The amount of data communication per day	The total amount of data communication per day
Counter	Every 60 minutes	74 Kbytes for each device x 24 hours = 1,776 Kbytes	23,520 Kbytes
Toner Level	Every 60 minutes	6 Kbytes for each device x 24 hours = 144 Kbytes	
Device Notification	Every 1 minute	15 Kbytes for each device x 24 hours x 60 minutes = 21,600 Kbytes	

Table 5 Polling Interval

	Alert					Counter/Consumables					
Number of Devices	2,000-1,001	1,000-301	300-101	100-26	25-1	2,000-1,001	1,000-601	600-201	200-101	100-26	25-1
High priority category	120 (min)	60 (min)	15 (min)	5 (min)	1 (min)	24 (hours)	12 (hours)	6 (hours)	2 (hours)	60 (min)	60 (min)
Middle priority category	x2				1 (min)	x2 [Note] Polling must be executed once a day					60 (min)
Low priority category	x4				1 (min)	x4 [Note] Polling must be executed once a day					60 (min)

Note that the MFPs/Printers users usually use are treated as high priority.

- **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)

  Service personnel remotely perform an optimal device setting at customers' site upon receipt of customers' requests and approvals.

  The service personnel save the device setting in KFS Manager, and send 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, Application status, Configuration list)

  Service personnel can obtain snapshot data to remotely diagnose device problems.

  The service personnel obtain the snapshot from the device by operating KFS Manager.

- **Device Status** (Panel message and Alert list)

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

  The service personnel obtain the panel messages and the alert list from the device by operating KFS Manager.

- **Maintenance Mode Setting**

  Service personnel remotely perform an optimal maintenance mode setting at customers' site.

  The service personnel obtain the device maintenance mode setting from KFS Manager.

  The service personnel change the maintenance mode setting and send it to the device from KFS Manager.

- **Data capture[(*4)]**

  Customers' print data is sent to KFS Manager.

(*4) Data capture is obtained only when the confirmation message is shown on the panel of the target device and the approval is gained from IT administrator in advance. Service Manager can specify the period of time up to 7days (default: 1day) 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[(*5)]**

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

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

  KFS Manager stores the USB logs received from KFS Device.

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

(*5) On-Demand USB Logs can be retrieved only when the confirmation of approval is gained from 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 automatically gets restarted. After device restarts, the USB logs are automatically downloaded to users' PC from KFS Manager.

- **Backup Data [(*6)]**

  The service personnel (System Administrator/Manager/Service) can import the backup data exported from a device to other devices at once.

(*6) Backup Data can be obtained only after the user has accepted the confirmation message on the panel of the target device. Any backup data containing personally identifiable information is not be stored in KFS Manager. Backup data obtained is encrypted. The use of the feature is restricted only for authorized access to group devices. Importing/Exporting the backup data will be recorded.

All KFS features are enabled by default. However, when creating a group, the Manager has the option to disable features. Disabled features will be grayed out on the user interface and will not be accessible by the users of the group.

When notifying and reporting to multiple users via an email, their email addresses shall not be disclosed to each other since the email address can be taken as personal data. BCC option is available for users to safeguard their personal information.

Table 6 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 • Application status • Configuration list
Device Status	• Panel Message • Alert List
Maintenance Mode Setting	• Device Adjustment
Data Capture	• Customers’ Print Data
On-Demand USB Logs	• USB Logs
Backup Data	• Address Book

	• Job Account • One Touch • User Administration • IC Card • Document Box • Program • Shortcut • Fax Forward • System Setting • Network Setting • Job Setting • Fax Setting • Printer Setting • Panel Setting

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 KFS Device • Server Certificate generated by KFS Device and registered to an MQTT server

KFS Gateway	• Authentication information used by an IT administrator to log in to KFS Gateway • MAC address of the machine 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

Security

This section explains in detail how the information assets mentioned in the previous section are securely protected by various security features implemented in KFS, and unless given permission by customers, customers' information cannot be accessed by any organization including sales companies and other tenants(*8).

(*8) 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 and giving access right to users and devices registered in the group.

Data Management

Users can access to devices located at the user site, and securely manage the devices. As shown in Figure 2, KFS Gateway and KFS Device are positioned under a group that is Customer 1. A user can access to KFS Gateway and KFS Device, and also can securely manage user data and device data.

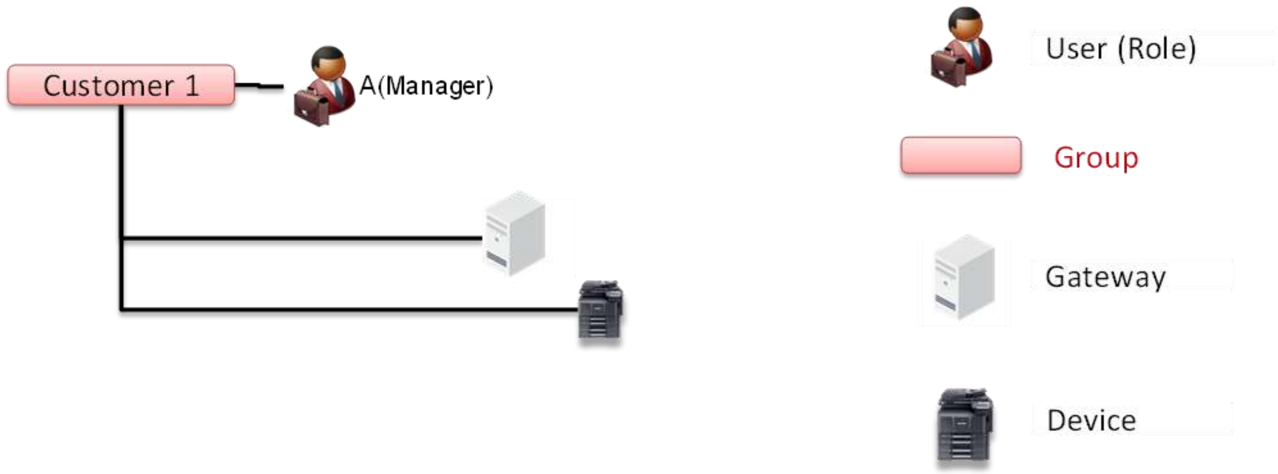

Figure 2 Data Management

User Account Management

User Account is created and managed within a group.

One of the following roles is assigned to every user.

In Manager to Customer order, privilege of Manager role includes one of Customer role.

- ✧ Manager
- ✧ Customer

✧ **Manager**

Manager manages and maintains child groups of the group where he/she belongs.

Manager can add new groups, edit or delete groups to the group which he/she manages. Manager can also add new user accounts, edit, delete, and change status. Further, when the user account is deleted, Manager can transfer the report schedule, notification criteria and templates which he/she manages to another user in the same delegated group.

✧ **Customer**

Customer manages devices at the customer site. Customer also can create and issue a report template that is used by the 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 a user ID, a temporary password and a link to the service URL. If the user account is created but is in an invalid state, unless this is valid, KFS Manager will not send an email notification to the user.

Data Access Control Policy

Access to data stored in KFS is controlled by the user role and access code linked to the user's group. Access to data is strictly restricted by the user roles.

Manager can access all the data of their group and all the data in child groups by defaults. However, access rights can be set or edited later by Manager of their group and parent groups.

Customer can access device property 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.

Users (**Manager and Customer**) can access the data in different groups only when external access is set by Manager of the different groups to be accessed by the users or their parent groups. This setting can be done upon entering the user's email address and unique external access codes that are issued by the above-mentioned Manager in the edit user wizard.

Registration into KFS

In order for KFS Manager to manage MFP device through KFS Device/KFS Gateway/KFS Mobile, Mutual registration between KFS manager and KFS Device/KFS Gateway/KFS Mobile must be done in advance.

When devices are registered in KFS they can have a status of "Pending" or "Managed". However, the status depends on the registered components. As one example, the following describes the behavior for one type of KFS Device registration.

- If registered with just the access code of the group, the status will be "Pending". In order to change to "Managed" an authorized user must change the status
- If registered with 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 like who, when and to where the access occurred can be used to help trace the unauthorized access.

Connection Mode

During KFS Device registration to KFS Manager, users can select a Connection Mode: Manage mode or Monitor mode. Users who use KFS Device can only select Monitor mode. For Manage mode, the user can set the expiration time period to automatically change from Manage mode to Monitor mode so that the time period for the network connection with KFS Manager can be restricted.

In Manage mode, KFS Device uses a bidirectional connection. An XMPP connection or an MQTT connection is established between KFS Device and KFS Manager.

Monitor mode establishes a unidirectional connection from KFS Device/KFS Gateway to KFS Manager only when the device information such as counters, toner level, device log and device notification is uploaded to KFS Manager. Neither an XMPP connection nor an MQTT connection is established between KFS Device/KFS Gateway and KFS Manager. Access by KFS Manager to KFS Device/KFS Gateway is blocked. This prevents intrusion to the customer's network by KFS Manager via the Internet, and can also decrease the network load. KFS Device/KFS Gateway can keep the KFS Manager information assets separate from the customer's environment. An IT administrator can enhance the security of the KFS environment. Monitor mode helps the IT administrator maintain efficient KFS security condition.

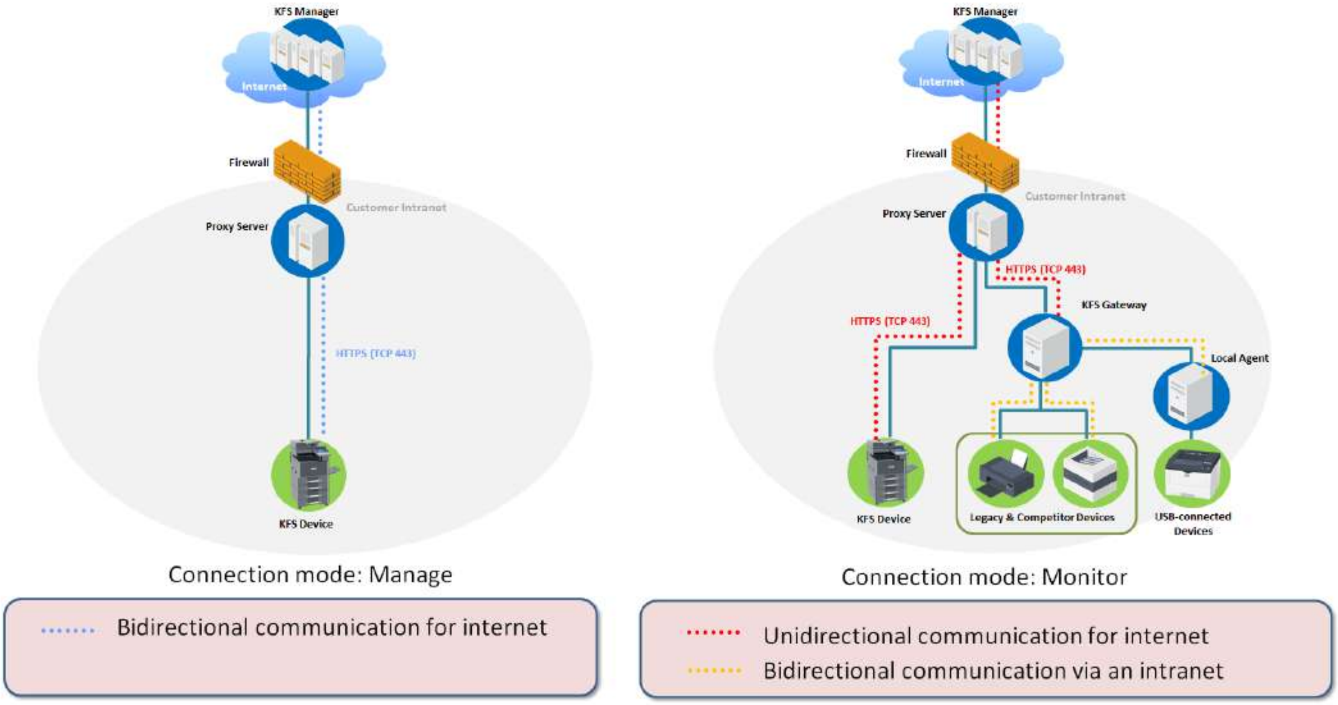

Figure 3 Connection Mode

Single-Point of Outgoing Connection

KFS Gateway supports Single-Point of Outgoing Connection with a capability of consolidating the point of contact to external Internet into one point. Consequently only one address needs to be added to the whitelist of the outbound firewall.

This is an ideal alternative for secure sites that are more concerned with security and their devices have direct access to the public network.

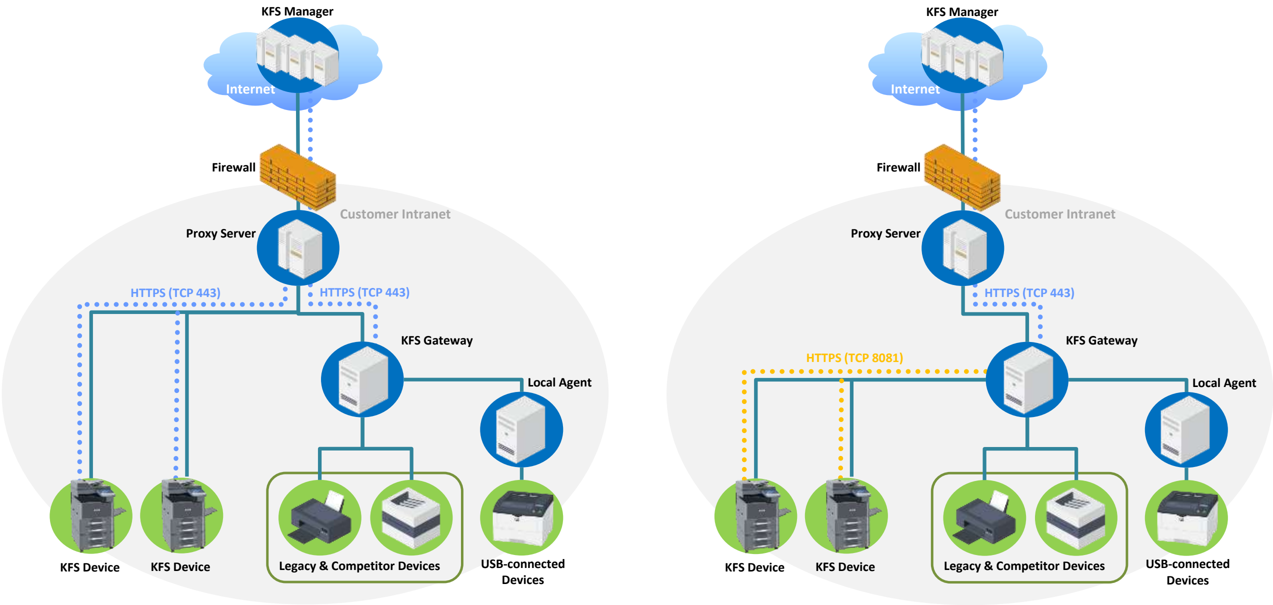

Figure 4 Comparison of Connection With (the Right Figure) and Without (the Left Figure)
Single-Point of Outgoing Connection

Note: KFS Gateway availability will vary by region.

Automatic Upgrade for KFS Gateway

The Automatic upgrade feature is a security improvement intended to maintain daily that the latest Gateway version is being used and to ensure secure and stable KFS Gateway operations. Once enabled, the automatic upgrade feature checks for software updates at a daily specified time or based upon the time of the initial Gateway registration. It removes any manual work. The setting is made in the Security settings section of the KFS Gateway Preferences tab. From both a security and convenience point of view, the automatic upgrade for KFS Gateway is recommended to be used.

Data anonymization mode by KFS Gateway

For customer's security, user can configure the mode on KFS Gateway not to send the following information to KFS Manager. This mode can only be enabled during KFS Gateway installation. When this mode is enabled, the Discovery settings are not synchronized with KFS Manager.

- IP address, Subnet mask, Default gateway IP address, DNS server addresses, Computer name, Host name and Site/location information

Identification and Authentication

When accessing to KFS, A user must log in with the registered User ID(*10). An unauthorized user cannot access KFS.

Access information is recorded when logging and is available for auditing.

The following features are supported as security features for login.

(*10) Please note that it is the responsibility of the users to ensure that the authentication information such as their password and user ID registered in KFS are managed and kept as confidential. The users should not let others use the authentication information, and should not provide or transfer the same to a third person. The users shall be, and KYOCERA shall not be liable for the damages caused by inappropriate management, misuse or use of the authentication information by a third person.

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 7, 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 7 Account Lockout Policy

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

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

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 8.

Table 8 Password Policy

Password Length	At least 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.

The password is valid for one year. The user cannot log in if his/her password has expired.

Audit Logs

KFS records audit logs of various events. The logs provide a record that can be checked to verify that KFS is secure. The users with access to the audit logs in their environment are restricted to required users.

Audit Logs of KFS Manager

An audit record is generated by KFS Manager for the following events(*14):

- Successful/unsuccessful user identification and authentication
- Add/Edit/Move/Delete group and user account
- Register/Terminate/Move/Delete KFS Device/KFS Gateway/KFS Mobile
- User password reset by e-mail.
- Delete/Archive task
- Export device logs
- Download data capture
- Import/Export backup data
- Import device information
- When requesting to use the remote panel
- When receiving permission from the remote panel from device
- When connecting to the remote panel
- When disconnecting to the remote panel

Audit Logs of KFS Gateway

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

- 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(*11) 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 unauthorized access. The operation logs are saved for the purpose of maintaining audit trails.

(*11) A timestamp for audit logs shows when the operation occurred. The timestamp is always synchronized with an accurate time in Azure. It uses the time zone set on the user's PC.

(*14) It will be deleted at the latest 67 days after the audit logs is generated (email logs as well).

Protection of Stored Data

The important KFS information assets must be protected and not leaked or lost. KYOCERA implements security protection measures for stored information assets and a data recovery support through the features described below.

Encryption/Hashing

The sensitive information assets stored in KFS components such as KFS Manager(*15), KFS Gateway, KFS Device and KFS Mobile, are encrypted with the following encryption algorithms. 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. These sensitive information assets are protected by encryption.

In addition, the sensitive information assets such as login passwords stored in KFS Manager and KFS Gateway, respectively, are protected using the hash algorithms indicated in Table 11.

The information assets are protected against information leaks by a malicious third party.

(*15) By Transparent Data Encryption (TDE), encrypt SQL Server and Azure SQL Database data files at rest.

Table 9 Encryption Strength

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

Table 10 Key Generation and Management Method

System Name	Key Length	Key generation and management method
KFS Manager	256 bit	Keys are generated for each environment and are setup for each deployed server. Keys are saved in configuration management software (Azure DevOps) where only the deployment Engineer can reference.
KFS Gateway (NetGateway)	256 bit	Keys are generated during registration to KFS Manager and stored in the local DB.
KFS Mobile (Android)	256 bit	Keys are automatically created during the first launch of the application after its installation. Keys are saved to DB specific to the application.
KFS Mobile (iOS)	256 bit	Keys are generated beforehand and embedded in application (same for all devices)
KFS Device	256 bit	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 the volatile memory of the device.

Table 11 Hashing – Hash Algorithm

System Name	Hash Algorithm
KFS Manager	Salted SHA-256
KFS Gateway (NetGateway)	Unsalted SHA-256

Data Backup

The important information assets are saved as backup data so that it can be restored, if necessary. The data protection plan relies on specific recovery times.

Table 12 Data Backup – System & Current Data

	Objective Type	Recovery Time
System & Current Data	RPO (Recovery Point Objective)	5 minutes
	RTO (Recovery Time Objective)	4 hours

	Backup Timing:	Frequency:	Retention Period
System & Current Data	- Transaction Log	- Every 5 minutes	35 days
	- Differential Backup	- Once a day	
	- Full Backup	- Once a day	

Every hour, all backups are copied to a secondary storage location in a different data center to support disaster recovery.

Table 13 Data Backup – Historical Data

	Objective Time	Recovery Time
Historical Data (Azure Storage Data)	RPO (Recovery Point Objective)	30 minutes
	RTO (Recovery Time Objective)	48 hours

Historical Data (Azure Storage Data)	Backups Timing:	Frequency:	Retention Period
	- Transaction Log	- Every 5 minutes	30 days

Transaction logs are saved in three different storage locations within the same data center. Three logs are copied to a different data center to support disaster recovery.

Protection of Communication Data

KFS realizes protection of communication data regarding user access to use KFS, data communication to transfer data between KFS and device, and tasks, respectively.

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 or mobile application, an authenticated communication channel is established.

Communication to access KFS via Web browser or mobile application

KFS user can access KFS Manager from the Web browser’s client UI or mobile application UI regardless of the user role. When a user accesses KFS Manager, the user is always identified and authenticated. If this identification and authentication are 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 located in a users' environment via the internet and local area network.

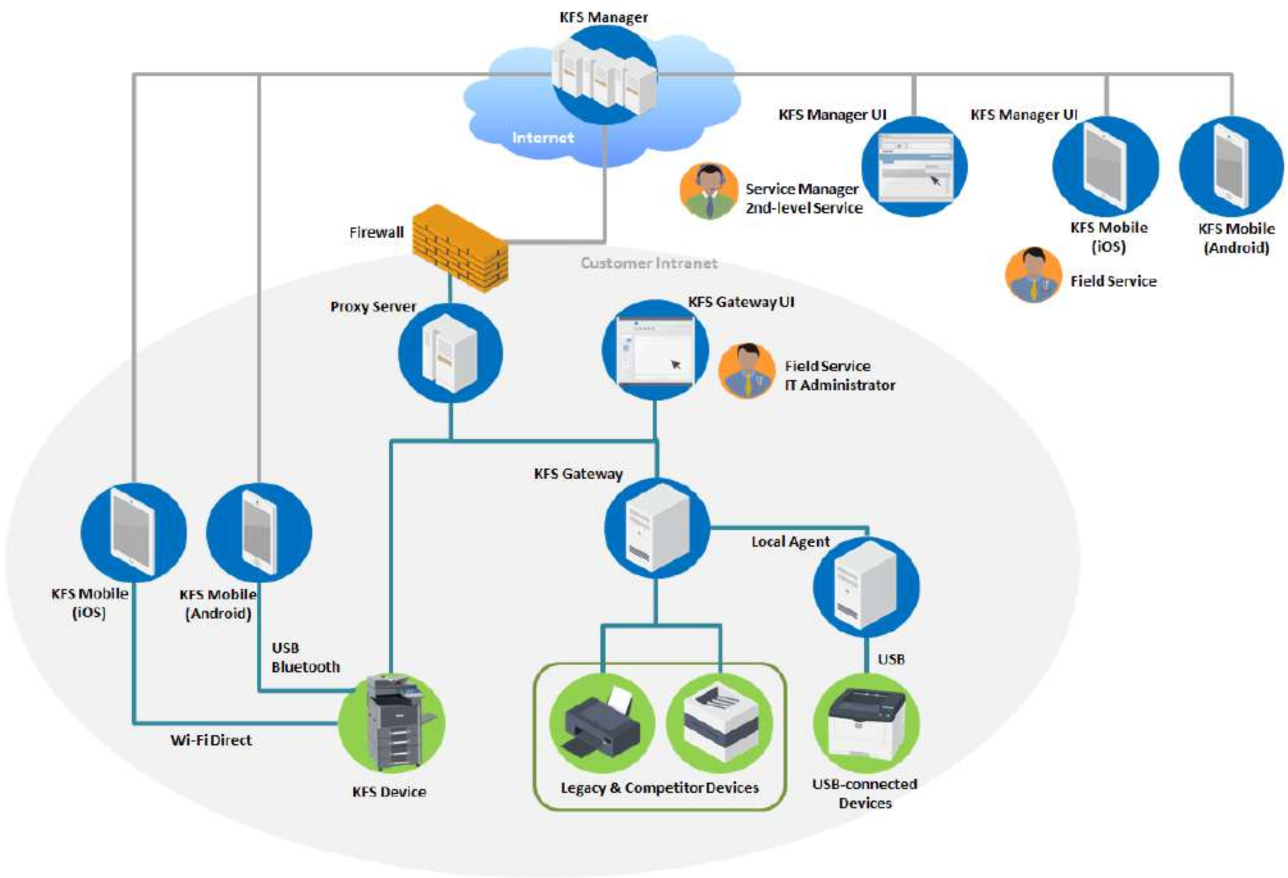

Figure 5 KFS Components and Data Flows

Communication with KFS via the Internet

KFS network communication is set up by XMPP server/MQTT server and KFS Manager in the cloud. XMPP/MQTT protocol uses HTTPS protocol for transporting. XMPP/MQTT protocol is used for the communication between KFS Manager and XMPP server/MQTT server in the cloud, or for the communication between KFS Device and XMPP server/MQTT server over the firewall. HTTPS protocol protects the data on the communication channel and therefore information data will not leak to an external source through the normal data communication path.

Communication with KFS via Local Area Network

The web service between KFS Gateway and device uses SOAP (WSDL) on HTTPS. SNMPv3 with a capability of authenticating and encrypting SNMP packet flowing on the network is used between KFS Gateway and device. Above encryption ensures secure communication.

The communication via local area network is controlled by setting a range of 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 devices can be set up via encrypted Bluetooth/Wi-Fi Direct, USB, and without passing through the local area network.

Table 14 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 Device
• Message Queuing Telemetry Transport (MQTT)	➢ Communication between KFS Manager and MQTT server
• Hyper Text Transport Protocol Secure (HTTPS)/TLS1.2	➢ Communication between Web browser's client UI and KFS Manager ➢ Communication between KFS Mobile 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 ➢ Communication between Web browser and Relay Server
• Simple Network Management Protocol (SNMPv3)	➢ Communication between KFS Gateway and device
• Simple Object Access Protocol (SOAP WSDL)	➢ Communication between KFS Gateway and device
• Bluetooth • Wi-Fi Direct	➢ Communication between KFS Mobile and KFS Device
• USB	➢ Communication between KFS Mobile (Android) and KFS Device

Tasks

Maintenance and management tasks are performed by KFS users through KFS Manager, or by service personnel when visiting the customers' office environment. These tasks cannot be performed without the customers' agreement. Users who can perform these tasks on KFS are restricted by identification and authentication. Data handled through respective tasks is protected by encryption of communication channels and mutual authentications.

Communication of Remote Firmware Upgrade

Please Note:

When firmware is uploaded to KFS Manager, software validation is made on the firmware, using the original algorithm. The algorithm of the package is validated to verify data integrity, so during firmware upgrade, the main controller in the device validates the algorithm after download.

Firmware upgrade communication from KFS Device

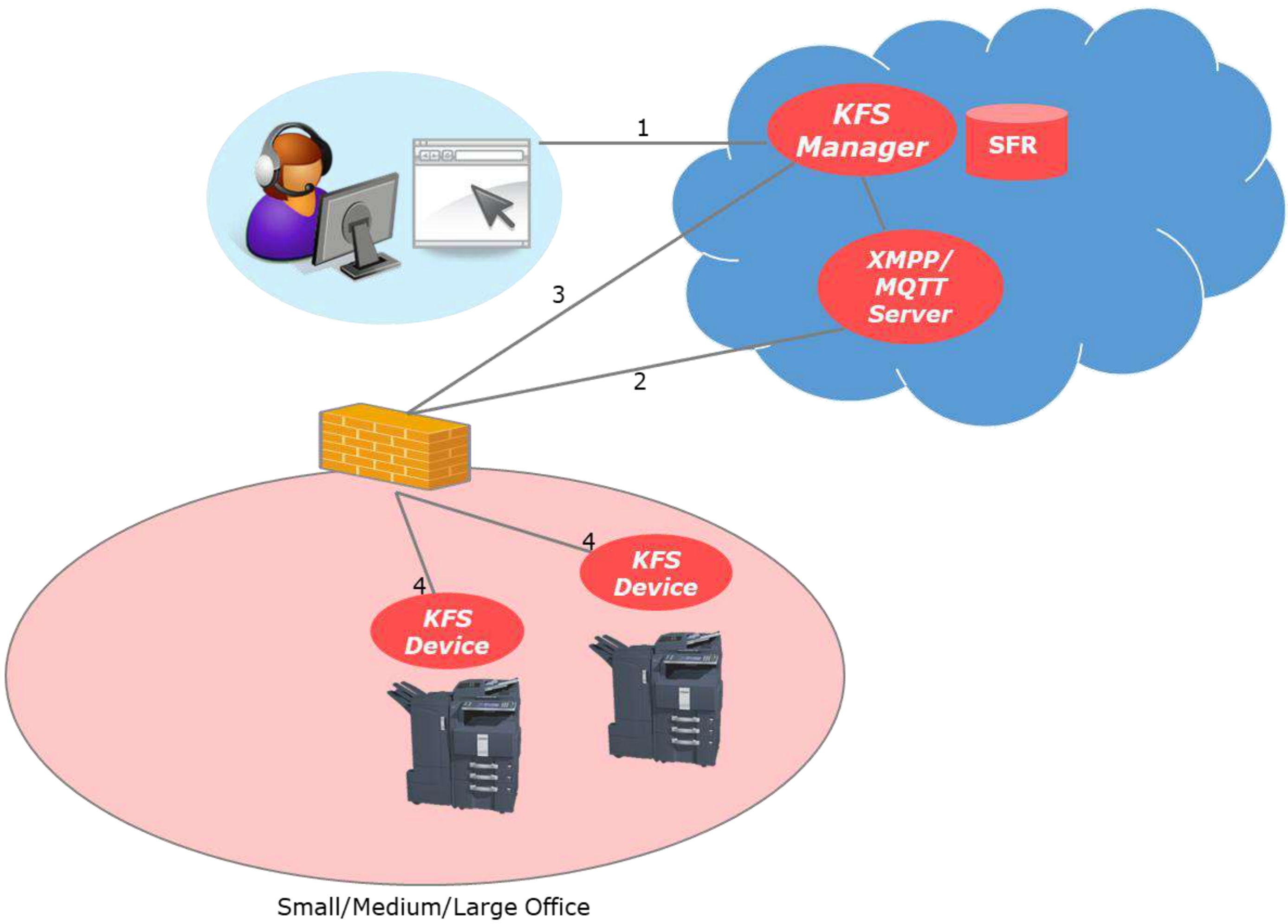

Figure 6 Communication flow of firmware upgrade from KFS Device

As shown in Figure 6, a secure firmware upgrade to KFS Device is achieved with the above-mentioned secure communication through the following steps:

1. User selects a firmware package for device through KFS Manager Web browser's client UI or mobile application UI. The communication between Web browser's client UI and KFS Manager is protected through HTTPS.
2. KFS Manager initiates secure communication with KFS Device through the XMPP/MQTT protocol, and sends firmware upgrade command to KFS Device.
3. KFS Device securely downloads firmware package from KFS Manager through HTTPS.
4. KFS Device updates the firmware on the machine.

<u>Firmware upgrade communication from KFS Mobile</u>

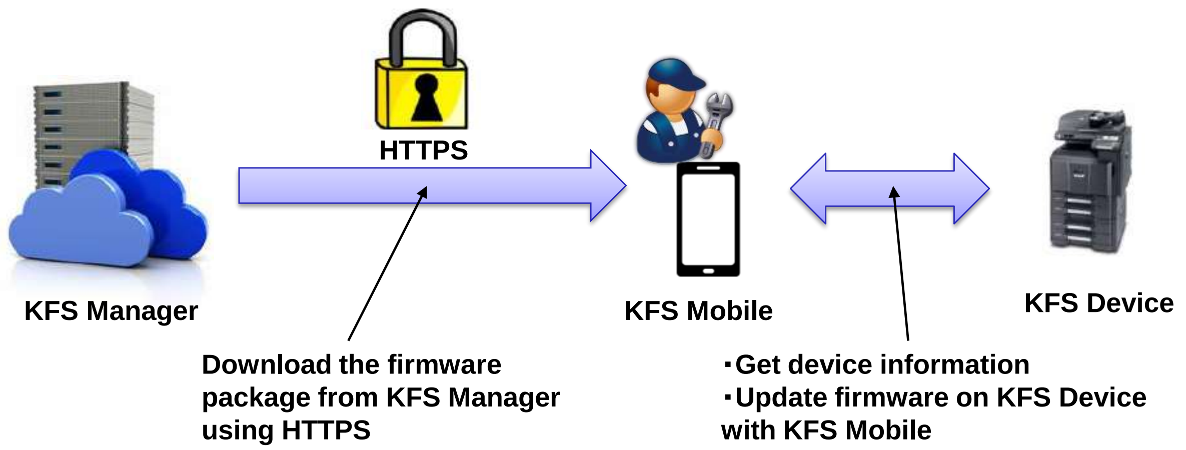

Figure 7 Communication flow of firmware upgrade from KFS Mobile

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

1. The 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 upgrade 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 only when the confirmation message is shown on the panel of the target device and the users' approval is given in advance.

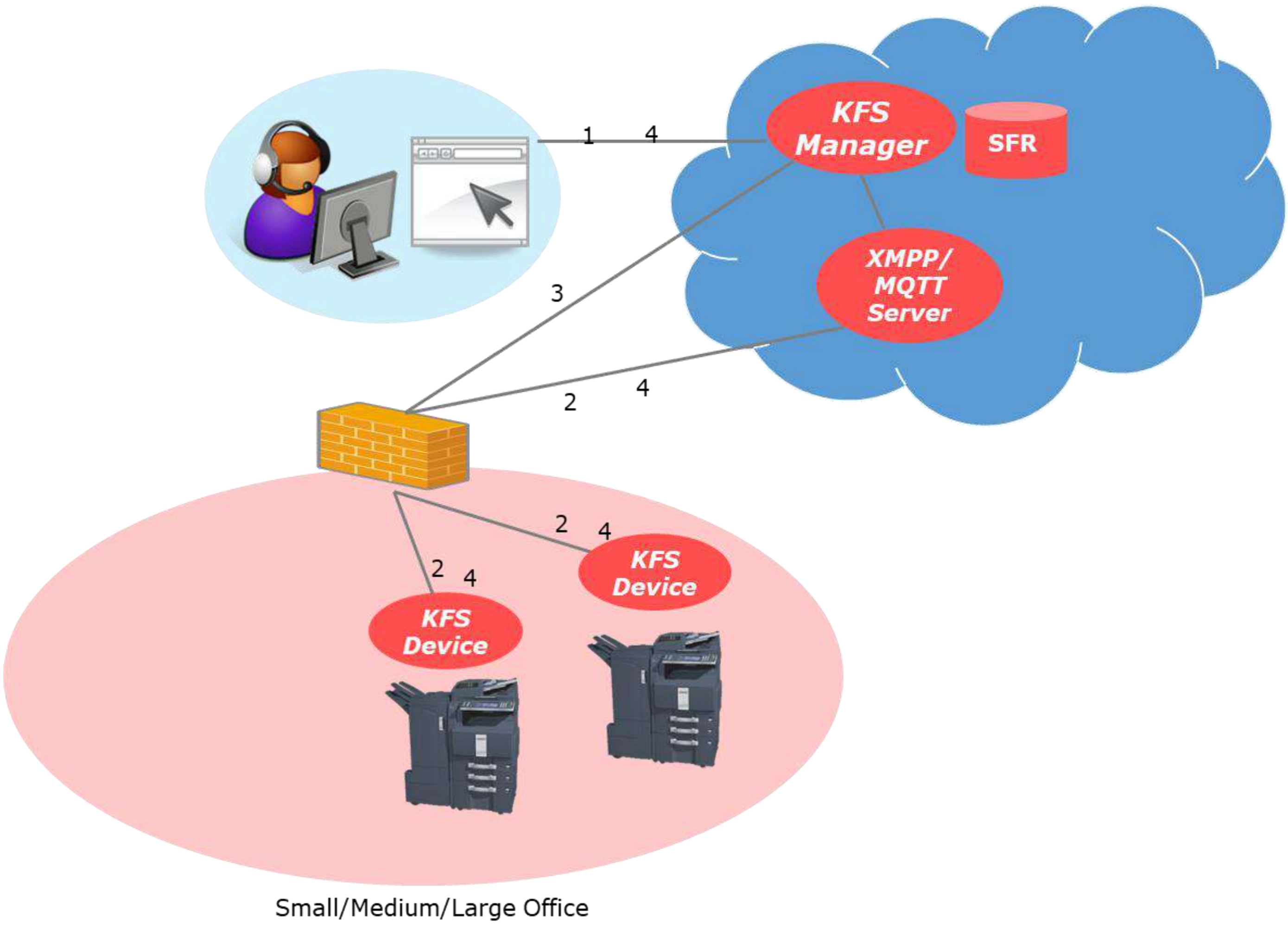

Figure 8 Communication flow of remote device panel capture

As shown in Figure 8, 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/MQTT 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/MQTT communication channel.

Communication for obtaining Remote Device Snapshot Data

To support a KFS user in performing device diagnostics, the following device snapshot data can be obtained from KFS Manager Web UI or mobile application UI.

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

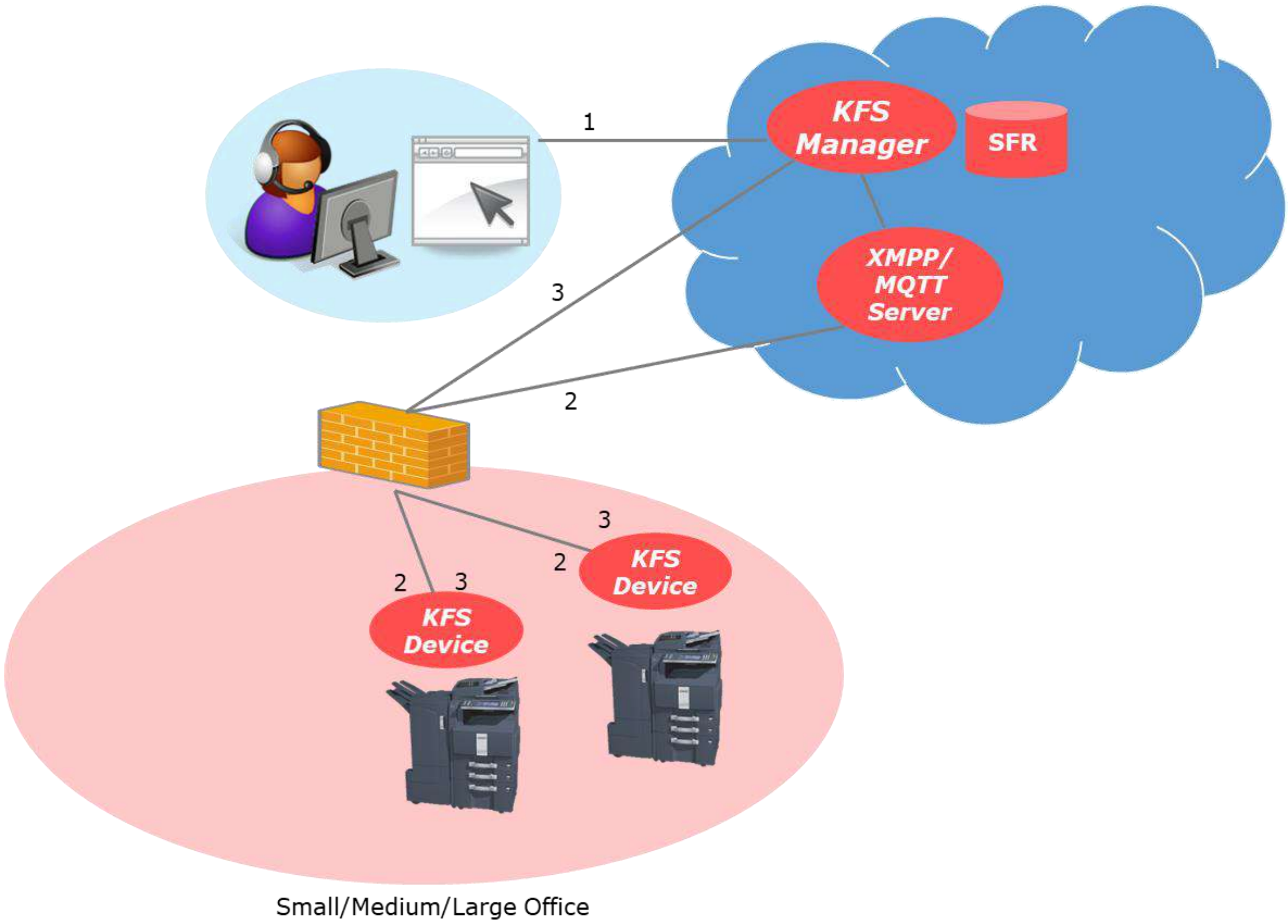

Figure 9 The flow of obtaining remote snapshot data

As shown in Figure 9, the KFS remote device snapshot feature uses secure communication :

1. KFS Manager user requests device snapshot information from either KFS Manager Web UI or mobile application UI through HTTPS.
2. KFS Manager initiates communication with KFS Device through a secure XMPP/MQTT protocol, and sends the snapshot command.
3. 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 application on KFS Device.

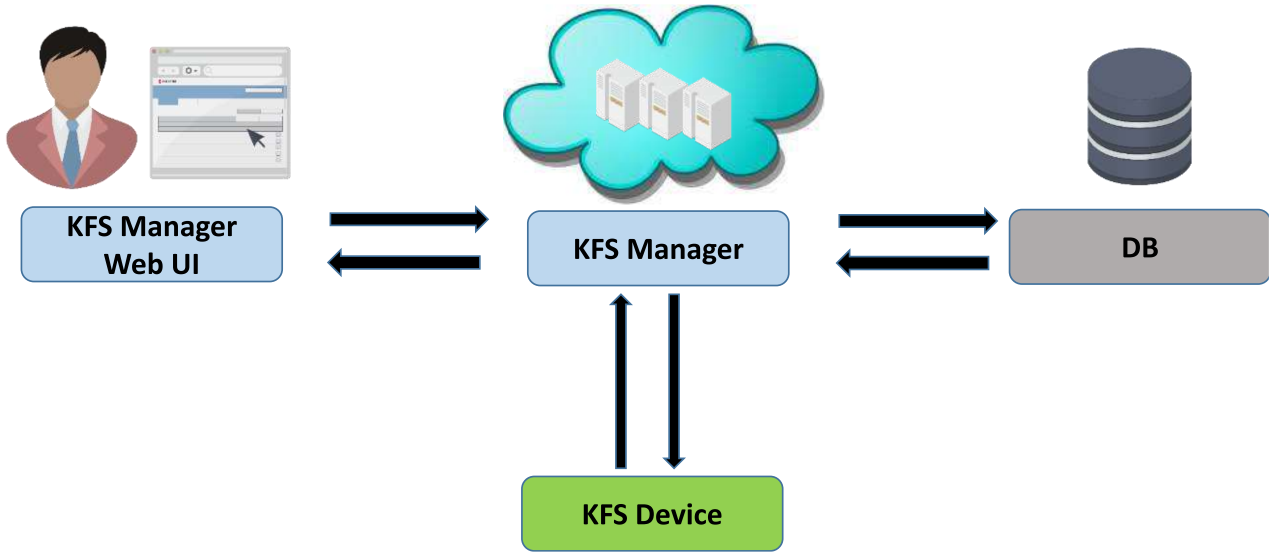

Figure 10 The flow of remote HyPAS management

As shown in Figure 10, 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/MQTT 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/MQTT 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 the case of installing the application).
4. KFS Manager can terminate this process upon receipt of notification directly from KFS Device when action is complete.

Communication of remote panel

KFS provides a remote panel feature that can operate panel from KFS Manager in addition to displaying the current panel image of a managed device on KFS Manager. This feature operates device panel when the confirmation message is shown on the panel of the target device and the users' approval is given in advance. It is possible to restrict the user who gives approval to the administrator.

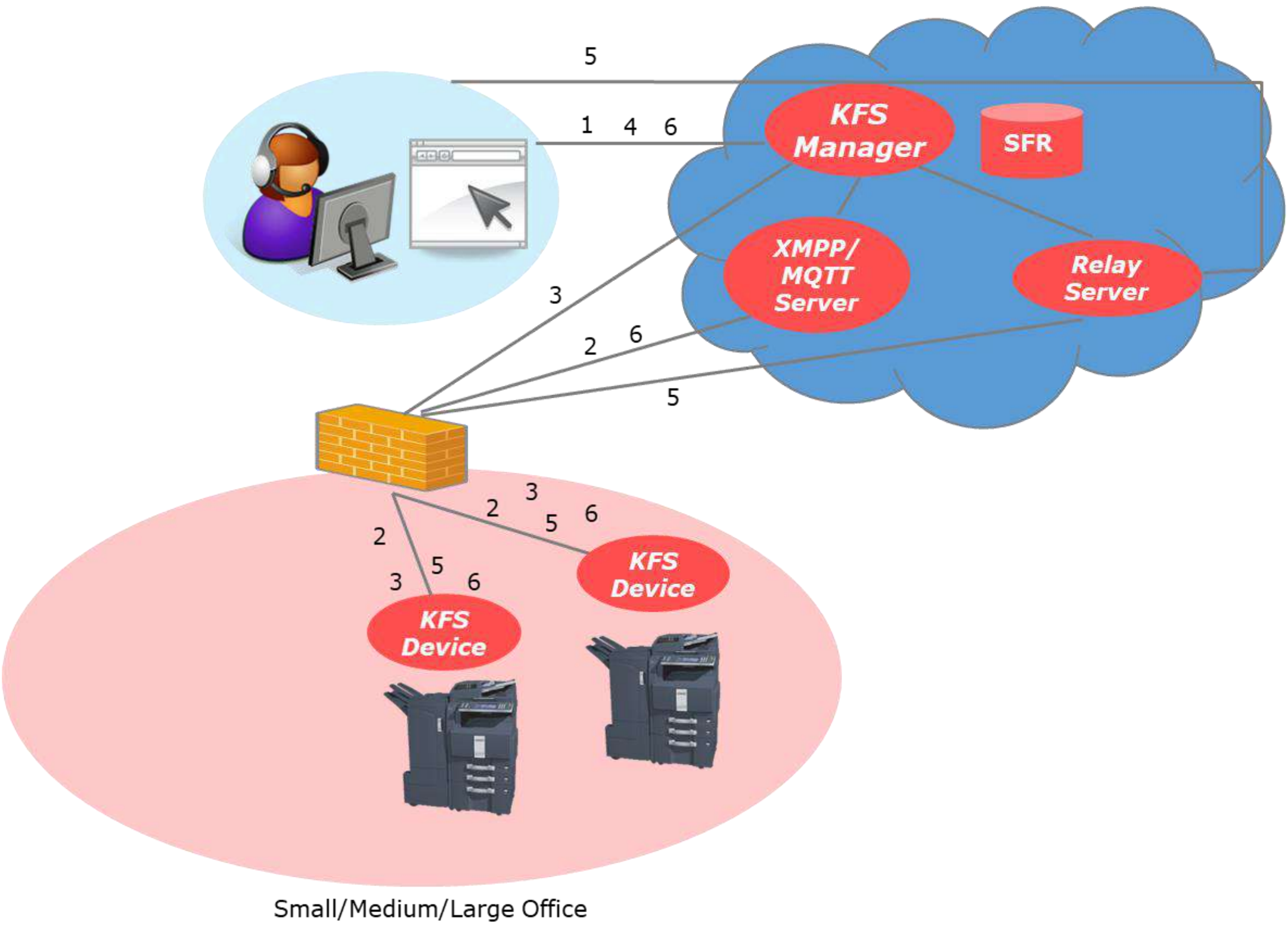

Figure 11 Communication flow of remote panel

As shown in Figure 11, the remote panel is achieved with a secure communication through the following steps:

1. KFS Manager user requests remote panel from KFS Manager Web UI through HTTPS.
2. KFS Manager initiates communication with KFS Device through a secure XMPP/MQTT protocol communication and sends remote panel request to KFS Device.
3. KFS Device obtains the information of relay server for KFS Manager through HTTPS and connects with KFS Manager in order to achieve remote panel.
4. The user's web browser obtains the information of relay server for KFS Manager through HTTPS and connects with KFS Manager in order to achieve remote panel.

5. Image information and operation commands are communicated mutually between the device and web browser and achieve the pseudo-panel operation remotely.
6. KFS Manager can terminate this process by sending a stop command to KFS Device through a secure XMPPMQTT communication channel.

Kyocera’s effort for KFS Security

Kyocera obtained ISMS Cloud Security certification (*12) ahead of all other MFP and printer manufactures on November 17, 2017. The certification was renewed on December 19, 2021, after an audit process to confirm compliance with audit standards. Nowadays, as cloud services are increasingly being used in a variety of industries, tighter security control and management is required in accordance with the latest international standards regarding data security and the handling of personal information. In certain sectors, when cloud services are introduced -- particularly at medical and educational institutions, and at companies and public offices where important information is handled -- compliance with security standards is necessary and thus the need for objective standards that certify the control system of each cloud service operator is growing.

Kyocera is working to achieve comprehensive control of security for data created in customers' document workflows. Kyocera has obtained ISMS Cloud Security Certification ahead of other companies in the industry as part of its efforts to provide safe, secure and flexible cloud services to customers. The company will continue to enhance the quality of its document solution services, thereby contributing to the growth of its customers' businesses.

Further, Kyocera continuously monitors the newest security trends and vulnerability information. Kyocera extracts and analyzes security requirements based on customer’s security requests and uses them in the updated version of KFS. Kyocera develops KFS following the “Open Web Application Security Project (OWASP)” as a guideline for our development. Kyocera strictly checks for potential vulnerabilities to ensure the best possible security for KFS. Prior to releasing KFS product, security diagnostic tests are conducted not only within Kyocera but also by an independent service provider.

Table 15 Outline of ISMS Cloud Security Certification Registration

Entity	KYOCERA Document Solutions Inc.
Date	November 17, 2017
Renewal Date	December 19, 2021
Range	ISO/IEC27001 (JIS Q 27001) Certificate Number: IS 735190 The ISMS cloud security management system for provision of "KYOCERA Fleet Services", development, operation and maintenance as a cloud service provider, and for the use of Microsoft Azure as a cloud service customer
No.	CLOUD 735193
Examining organization	BSI Group Japan K.K.

(*12) ISMS Cloud Security Certification is a third-party certification for cloud security, which is defined as an add-on specification to complement preparations against risks specific to cloud services. The prerequisite to this certification is to obtain ISO/IEC 27001 certification, requirements for a holistic information security management system (ISMS) that protects important data from various threats and mitigates risks.

Security Technical Details

This section describes defense against security threats and hosting environment.

Defense against Security Threats

KFS relies on Microsoft Azure for the protection, at the infrastructure level, of its cloud services and virtual machines 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. 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 Azure Network Security.pdf (microsoft.com)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.

The vulnerability validation (including external) are conducted on Kyocera's original modules, the infrastructure (Azure) and all operating systems. With respect to the infrastructure (Azure), Kyocera reviews the vulnerability information provided by Microsoft on a monthly basis. For operating system vulnerabilities, we check the revision histories once a half year.

Hosting Environment

KFS Manager is hosted on the Microsoft Azure platform. Microsoft meets a broad set of internationally recognized 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 and Japan ISMAP. 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).

Health Insurance Portable & Accountability Act (HIPAA)

HIPAA regulations include security standards for the protection of electronic health information. KFS is compliant with the HIPAA standards as KFS does not perform the critical operation of collecting, storing and transmitting patient information that identifies an individual or a group of patients. Access to KFS is strictly controlled by the user role and access code linked to the user's group. Users must log in with a registered User ID. A strong password policy is also applied. There is no way for unauthorized users to access KFS. Access to the system is recorded and available for auditing. These audit logs are checked to verify that KFS is secure. KFS communication data is encrypted and KFS components are mutually authenticated. KFS sends device information in a secure manner for the purpose of device management or maintenance only, and does not transmit any patient information. Prior to using the remote services of KFS, Kyocera will request your authorization.

Server Certificate

One of the big reasons why general web servers use the server certificate issued by CA is to prevent "spoofing" that includes the domain of the server within the subject of certificate. On the client side, spoofing is detected by certifying the domain set for the subject and the connection destination domain after verifying the validity of the certificate. On the other hand, KFS Device and KFS Manager use the server certificate only to encrypt the communication path. This is because the certification between KFS Device and KFS Manager adopts the unique method implemented on XMPP/MQTT. Even if the attacker spoofs the server in some way, KFS Device will not connect to that server because specific algorithm of the certification method is not disclosed. In addition, remote operation scenario including KFS Device periodically performs manned evaluation using vulnerability diagnosis service in order to ensure the safety.

Appendix

Please refer to Figure 5 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 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 vary depending on which Azure data center KFS Manager is hosted. This information is provided by the KYOCERA headquarters in your region.
- In order to simplify the whitelist management of customers' firewall, XMPP server/MQTT server end points are unified. This allows extracting the IP address from the existing XMPP server/MQTT server and providing it as the end point of the XMPP server/MQTT server. So the XMPP/MQTT servers are not required and can be removed from whitelist.
    - If the customer defines XMPP server/MQTT server with host name for the whitelist, new host name needs to be added due to the XMPP server/MQTT server end point unification.

To use remote panel, the IP address of remote panel relay server needs to be newly added to customers' firewall whitelist.

On the Machine Hosting KFS Gateway (NetGateway)

- TCP port 443 (HTTPS) must be opened to allow outbound traffic. This port is used for NetGateway to connect to KFS Manager. The port 443 is used to securely connect to device home page via HTTPS
- TCP port 9797 (HTTPS) should be opened to allow inbound traffic. This is necessary if you wish to connect to NetGateway webpage. If this port was already used when installing the NetGateway, the user can specify another port.
- TCP port 80 (HTTP) should be opened to allow outbound traffic. This port is used for NetGateway to connect to device home page.
- TCP port 9090 (HTTP) and/or 9091 (HTTPS) should be opened to allow outbound traffic. This port is used for NetGateway to request data from device.
- UDP port 161 must be opened to allow outbound traffic to devices. This port is used to collect device status and properties over SNMP.

- When NetGateway is installed, TCP port 8081 (HTTPS) is automatically opened in Windows Firewall to allow inbound traffic from devices. If this port was already used when installing the NetGateway, the user can specify another port. This is necessary if you wish to use the feature of NetGateway to consolidate outgoing network traffic from KFS Device as a single point of communication. The inbound rule thus created will be deleted when NetGateway is uninstalled.
- TCP port 9696 (HTTPS) is used. This port is used for communication between services internal the NetGateway, but it's not necessary to open. If this port was already used when installing the NetGateway, the user can specify another port.

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 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 to install or upgrade Local Agent.
  - ➢ If enabling WMI 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.

KYOCERA Document Solutions Inc.

1-2-28 Tamatsukuri, Chuo-ku, Osaka 540-8585, Japan
Phone: +81-6-6764-3555