TA/UTAX Fleetmanager:

Security White Paper

Version 2.2

Document Version: 01/2024

January 11, 2024

1. Introduction

1.1. Purpose

The purpose of this document is to inform customers about the security measures in TA/UTAX Fleetmanager.

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

1.2. Target Audience

The target audience for this document is customers of TA Triumph-Adler/UTAX.

1.3. Document Structure

This document is organized into the following sections:

- ✧ TA/UTAX Fleetmanager Overview
- ✧ Protection of Information Assets
- ✧ Security
- ✧ TA/UTAX effort for TA/UTAX Fleetmanager Security
- ✧ Security Technical Details
- ✧ Health Insurance Portable & Accountability Act (HIPAA)
- ✧ Appendix

1.4. Edition Notice

The information contained in this document is subject to change without notice. This document could include minor errors. Changes and improvements in TA/UTAX Fleetmanager may be incorporated in later editions without prior notice.

2. TA/UTAX Fleetmanager Overview

This section describes TA/UTAX Fleetmanager overview and configuration .

2.1. What is TA/UTAX Fleetmanager?

TA/UTAX Fleetmanager is a cloud service developed for customers using MFP/Printer (devices) to reduce service costs and improve operational support. TA/UTAX Fleetmanager can remotely collect and centrally manage information of devices distributed in a certain region.

TA/UTAX Fleetmanager has **Management Feature** and **Tasks**.

Management Feature provides centralized management and monitoring of TA/UTAX 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 TA/UTAX 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

2.2. TA/UTAX Fleetmanager Configuration

TA/UTAX Fleetmanager consists of **TA/UTAX Fleetmanager Manager, TA/UTAX Fleetmanager Device, TA/UTAX Fleetmanager Mobile** and **TA/UTAX Fleetmanager Gateway.**

TA/UTAX Fleetmanager Manager is the backbone of TA/UTAX Fleetmanager using the cloud system of Microsoft Azure.

TA/UTAX Fleetmanager Manager communicates with TA/UTAX Fleetmanager Device, TA/UTAX Fleetmanager Mobile, and TA/UTAX Fleetmanager Gateway and manages devices via these components. TA/UTAX Fleetmanager Manager also provides device information to these components.

TA/UTAX Fleetmanager Manager provides features such as remote firmware upgrade, device restart and remote setting of maintenance mode. In addition, TA/UTAX Fleetmanager 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, TA/UTAX Fleetmanager Device, TA/UTAX Fleetmanager Mobile, and TA/UTAX Fleetmanager Gateway must be registered in TA/UTAX Fleetmanager Manager.

TA/UTAX Fleetmanager Device is a module embedded in a device at the customer's site.

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

TA/UTAX Fleetmanager Mobile is an application installed on service personnel's mobile devices such as smartphones and tablets.

TA/UTAX Fleetmanager Device/ TA/UTAX Fleetmanager Gateway communicates with TA/UTAX Fleetmanager Manager on a customers' network (i.e. LAN). TA/UTAX Fleetmanager Mobile is used when TA/UTAX Fleetmanager Device/ TA/UTAX Fleetmanager Gateway cannot connect to the customers' network (i.e. LAN). TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager Device, TA/UTAX Fleetmanager Mobile sends device data to TA/UTAX Fleetmanager Manager. In addition, TA/UTAX Fleetmanager Mobile provides features to display device information and event logs.

TA/UTAX Fleetmanager Mobile can be used as a mobile application interface to TA/UTAX Fleetmanager Manager.

TA/UTAX Fleetmanager Gateway is a TA/UTAX Fleetmanager Gateway for Windows on a PC, which manages TA/UTAX Fleetmanager Device as legacy devices under TA/UTAX Fleetmanager Gateway.

TA/UTAX Fleetmanager Gateway connects TA/UTAX devices and non-TA/UTAX devices to TA/UTAX Fleetmanager Manager via the internet.

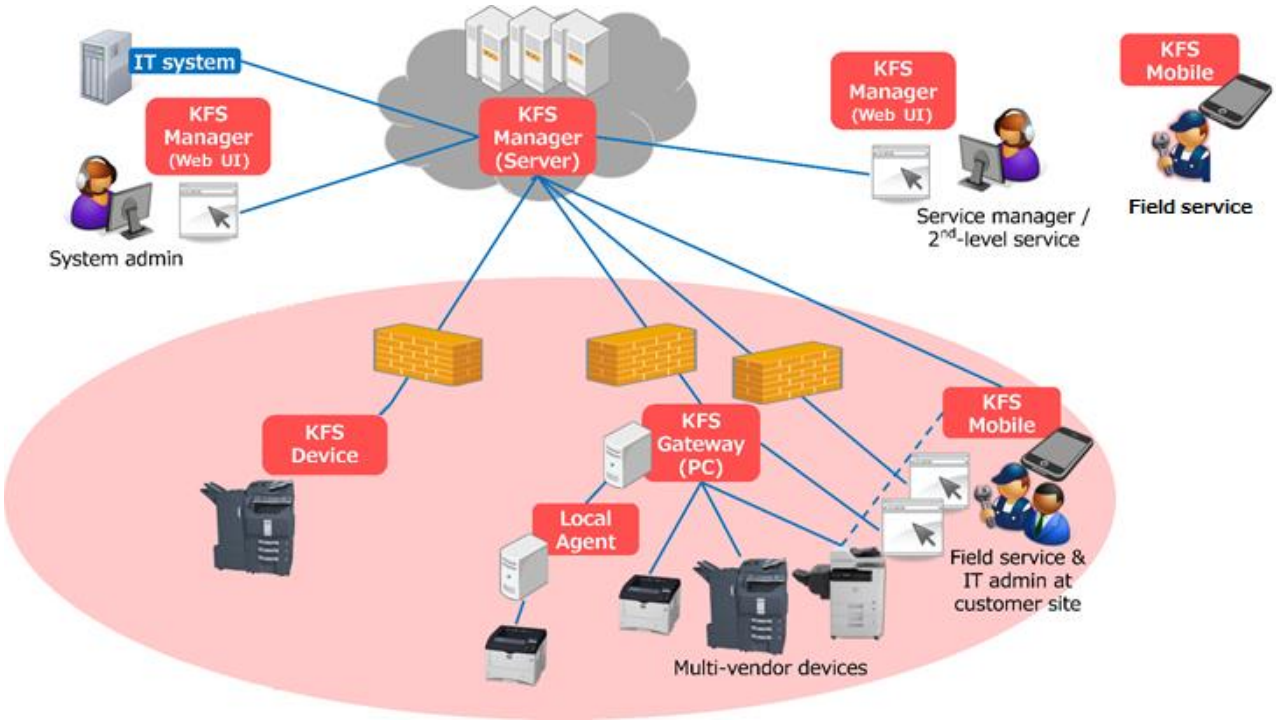

Figure 1 TA/UTAX Fleetmanager Configuration

3. Protection of Information Assets

When using TA/UTAX Fleetmanager, the following information assets handled through TA/UTAX Fleetmanager are strictly protected(*2).

(*2) See Security section for protection measures

3.1. 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 TA/UTAX Fleetmanager Device, for example. The device information is sent to TA/UTAX Fleetmanager regularly once a day. To maintain an XMPP connection/MQTT connection between TA/UTAX Fleetmanager and TA/UTAX Device/TA/UTAX Fleetmanager 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/108Kbytes 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 208Kbytes, respectively.

(*3) However in Monitor mode, either an XMPP connection nor an MOTT connection is established between TA/UTAX Fleetmanager Device/ TA/UTAX Fleetmanager Gateway and TA/UTAX Fleetmanager 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 communication per day	The total amount of datacommunications 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	208 Kbytes
•Device Notification	Per each alert event	20 Kbytes	
•Connection: Keep-Alive	Every four minutes	108 Kbytes	
• Device Setting	During remote	0 Kbytes	

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

Table 3 shows the amount of data transmitted from TA/UTAX Fleetmanager Gateway (NetGateway) to TA/UTAX Fleetmanager Manager. The device information is sent to TA/UTAX Fleetmanager 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 TA/UTAX Gateway to TA/UTAX Fleetmanager

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	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 - From V2.1, user can expand up to 6 times a day.	13 Kbytes (10 discovery settings) (The amount of data communication per day increases according to the frequency. e.g. if 6 times is set, 78 Kbytes (10 discovery settings))

Table 4 shows the amount of data transmitted from TA/UTAX Fleetmanager Gateway (NetGateway) to the devices, which indicates the average usage of a NetGateway 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 a NetGateway 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 TA/UTAX Fleetmanager Gateway (NetGateway) 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	1,000-301	300-101	100-26	25-1	1,000-601	600-201	200-101	100-26	25-1
High priority category	60 (min)	15 (min)	5 (min)	1 (min)	12 (hours)	6 (hours)	2 (hours)	60 (min)	60 (min)
Middle priority category	x2			1 (min)	x2				60 (min)
Low priority category	x4			1 (min)	x4				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 TA/UTAX Fleetmanager Manager.

TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager 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)

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

  The service personnel obtain the snapshot from the device by operating TA/UTAX Fleet-manager 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 TA/UTAX Fleetmanager 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 TA/UTAX Fleet-manager Manager.

  The service personnel change the maintenance mode setting and send it to the device from TA/UTAX Fleetmanager Manager.

- **Data capture(*4)**

  Customers' print data is sent to TA/UTAX Fleetmanager 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.

  TA/UTAX Fleetmanager Device generates USB Logs and sends it to TA/UTAX Fleetmanager Manager.

  TA/UTAX Fleetmanager Manager stores the USB logs received from TA/UTAX Fleetmanager Device.

  The service personnel can download the USB logs to PC from TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager 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
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

3.2. Information utilized in TA/UTAX Fleetmanager

TA/UTAX Fleetmanager Component	Information Assets (Used for the purpose of identification and communication within TA/UTAX Fleetmanager)
TA/UTAX Fleetmanager Manager	• Authentication information of each TA/UTAX Fleet-manager user • Access codes used by TA/UTAX Fleetmanager Devices (TA/UTAX Fleetmanager Gateway and TA/UTAX Fleetmanager Mobile) • Server certificates used for secure communications between TA/UTAX Fleetmanager Manager and various agents or clients, such as Web browsers, TA/UTAX Fleetmanager Devices, TA/UTAX Fleet-manager Gateways and TA/UTAX Fleetmanager Mobile, as well as between internal components of TA/UTAX Fleetmanager Manager • MAC addresses of each TA/UTAX Fleetmanager Device or TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager Manager or TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager Mobile is installed [In case the serial number cannot be obtained from the mobile device, its IMEI may be used for the same purpose.]

TA/UTAX Fleetmanager Device	• MAC address of the device in which TA/UTAX Fleetmanager Device is embedded • Proxy authentication information entered from the device panel, or by other means, and used by TA/UTAX Fleetmanager Gateway itself or TA/UTAX Fleetmanager Device to connect to TA/UTAX Fleetmanager Manager through the proxy server • Authentication token generated by TA/UTAX Fleetmanager Manager and downloaded to a TA/UTAX Fleetmanager Device • Server Certificate generated by the Device and registered to an MQTT server.

TA/UTAX Fleetmanager Gateway	• Authentication information used by an IT administrator to log in to TA/UTAX Fleetmanager Gateway • Authentication information used by a visiting service technician to log in to TA/UTAX Fleetmanager Gateway(*7) • MAC address of the machine on which TA/UTAX Fleetmanager Gateway is installed • Access code used by TA/UTAX Fleetmanager Gateway to register itself to TA/UTAX Fleetmanager Manager [The same code may be used by TA/UTAX Fleetmanager Gateway to register devices in the case of automatic discovery and registration.] • Proxy authentication information used by a TA/UTAX Fleetmanager Gateway or TA/UTAX Fleetmanager Device when connecting to TA/UTAX Fleetmanager Manager through the proxy server • Authentication token generated by TA/UTAX Fleet-manager Manager and downloaded to TA/UTAX Fleetmanager Gateway • SNMP credentials (e.g. SNMPv1/v2 community name, SNMPv3 username and password, etc.), entered from either TA/UTAX Fleetmanager Manager or TA/UTAX Fleetmanager Gateway as part of device discovery settings and used to connect to the devices by SNMP • Authentication information used by TA/UTAX Fleet-manager Gateway to communicate with devices by proprietary protocols

(*7) not supported by TA/UTAX Fleetmanager Gateway (NetGateway)

TA/UTAX Fleetmanager Mobile	• Serial numbers of each mobile device (smartphone or tablet) on which TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager Manager and downloaded to TA/UTAX Fleetmanager Mobile • Authentication information entered by the user of TA/UTAX Fleetmanager Mobile to log in to TA/UTAX Fleetmanager Manager • Proxy authentication information used by a TA/UTAX Fleetmanager Mobile and paired TA/UTAX Fleetmanager Device when connecting to TA/UTAX Fleetmanager Manager through the proxy server

4. Security

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

(*8) Tenant indicates users who use TA/UTAX Fleetmanager.

4.1. Group and User Account

TA/UTAX Fleetmanager realizes multi-tenant(*9) to accommodate multiple dealers and sales companies, and uses the concept of "Group Management" in order to enforce appropriate user and device data access control, and prevent leakage of information to other tenants. This Group Management treats a sales company or a dealer as one unit and access control is enforced through applying the hierarchically structured groups. There are user accounts in each group and the combination of these are used to control access to TA/UTAX Fleetmanager. Thus a dealer cannot be able to view the data of another dealer.

(*9) Multi-tenant indicates a system that multiple customers use.

4.1.1. Group Management

Group Management means managing and sharing user data and device data belonging to a group(*10) only within one organization comprised of these groups. Such organization is structured hierarchically with a **parent** group at the top. The parent group can only access the **child** groups beneath it in the structure, but the child groups cannot access the parent group.

For example, a Dealer Headquarters (DLA) that is in charge of the sales of a specific region will be the parent group for that region. Under this parent group are sub-groups of dealers (DLB), who are responsible for sales in different countries in the region. Under the dealer sub-groups are other dealers (DLC) who are responsible for sales in particular areas of a country.

The DLA parent group can access and manage the DLBs and DLCs beneath it, but the groups beneath it cannot access the DLA parent group. This is also true for the DLB sub-groups, which can access and manage any groups beneath each individual sub-group, but the sub-groups cannot see the group above them.

Group Management does not access across different DLAs, DLBs or different DLCs. In addition, a user can belong to only one group.

As an additional security measure, user accounts with Service, Analyst, or Customer roles cannot access groups to which they belong until a Manager or System Administrator grant them access.

Group management units can be a **Delegated Group** or a **Group.**

A **Delegated Group** is a unit to manage devices, users, TA/UTAX Fleetmanager Gateway and other resources (e.g. report templates, notification templates, firmware packages, etc.). The "Root Group" at the top of the hierarchy is considered a **Delegated Group** since it manages all of these resources.

A **Group** is a unit to manage devices and TA/UTAX Fleetmanager Gateway. If Manager does not exist for DLC3 (see Figure 2), the devices and TA/UTAX Fleetmanager Gateway of DLC3 will be managed by DLB.

Management data such as user data and device data managed on a per-group basis can be shared and managed only within one hierarchically structured organization to which these groups belong. Users in the group positioned at the top of the hierarchy can only access data in its child groups. Therefore, the data are logically separated and access from groups belonging to a different organization is not allowed.

(*10) Group data, user data and device data are immediately logically deleted upon receipt of a deletion request of group. Even if the data is deleted in error, it can be recovered. However, the data that has passed 14 days after the group deletion request is completely deleted. Delete an individual user or device, the data is permanently deleted immediately (Device data is information that identifies the device.).

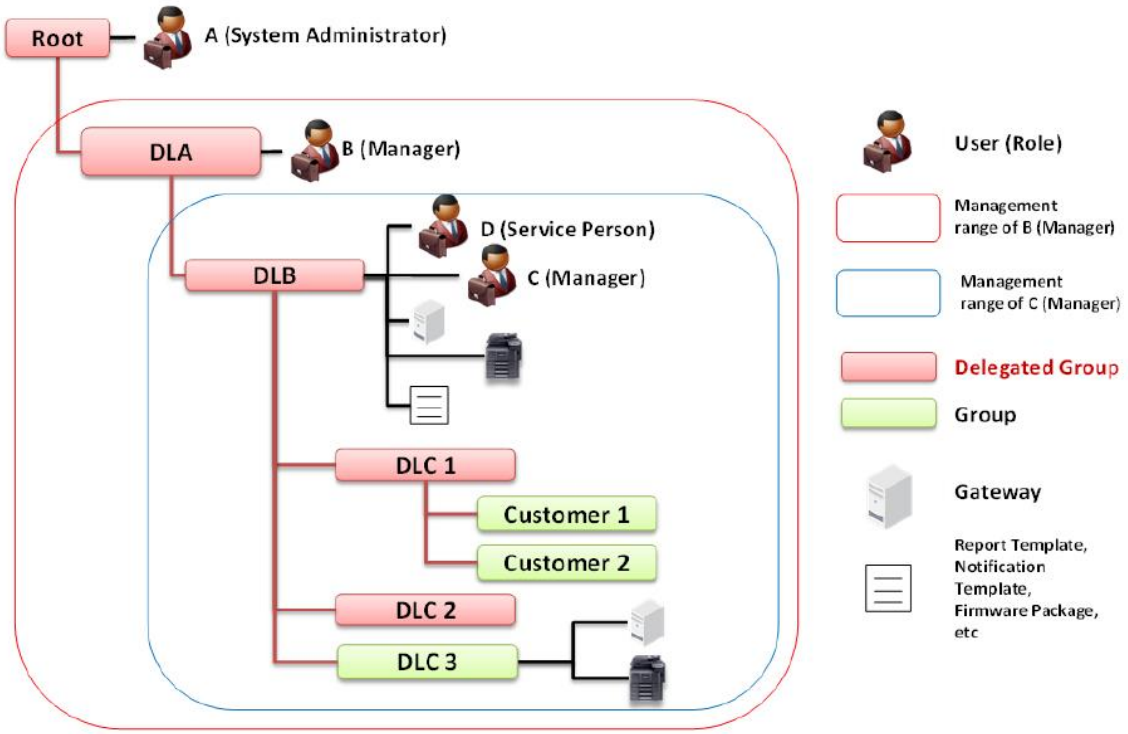

Figure 2 Data Management

4.1.2. User Account Management

User Account is created and managed within a group.

One of the following roles is assigned to every user.

Positioning System Administrator at the top of the roles, Manager, Service, Analyst and Customer,

the roles include the privileges of the lower roles.

- System Administrator
- Manager
- Service
- Analyst
- Customer

- **System Administrator**

  System Administrator has the highest level of authorization among all TA/UTAX Fleetmanager roles. This role

  is assigned to a user in the Root Group, which is positioned at the top tier in the hierarchy

  structure. System Administrator manages TA/UTAX Fleetmanager Manager. System Administrator manages configuration, partial changes, maintenance and monitoring of TA/UTAX Fleetmanager status.

- **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.

- **Service**

  Service can perform maintenance (e.g. Firmware upgrade, snapshot, etc.) and register

  device at customer site.

- **Analyst**

  Analyst issues a report of device status such as counter information, and analyzes the

  customer's environment . Analysts can create a report template to issue the report.

  The report template can be shared with users in the same delegated group. However,

  unlike Service, Analysts cannot perform maintenance of the device.

✧ **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 TA/UTAX Fleetmanager Manager, TA/UTAX Fleetmanager 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, TA/UTAX Fleetmanager 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 temporary password will no longer be valid.

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

4.1.3. Data Access Control Policy

Access to data stored in TA/UTAX Fleetmanager 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.

Service can access device data in their group and in child groups. However, access rights need to be set by Manager. The device data includes device property, snapshots, image data, capture data and panel screenshots.

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

Users (**Manager, Service,Analyst 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.

System Administrator, Manager and Service can access device log data, but Analyst and Customer cannot access the device log data.

4.2. Registration into TA/UTAX Fleetmanager

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

When devices are registered in TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager 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.

4.3. Connection Mode

During TA/UTAX Fleetmanager Device/ TA/UTAX Fleetmanager Gateway registration to TA/UTAX Fleetmanager Manager, users can select a Connection Mode: Manage mode or Monitor mode. Users who use TA/UTAX FM 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 TA/UTAX Fleetmanager Manager can be restricted.

In Manage mode, TA/UTAX FM Device uses a bidirectional connection. An XMPP connection or an MQTT connection is established between TA/UTAX FM Device/ TA/UTAX FM Gateway and TA/UTAX FM Manager.

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

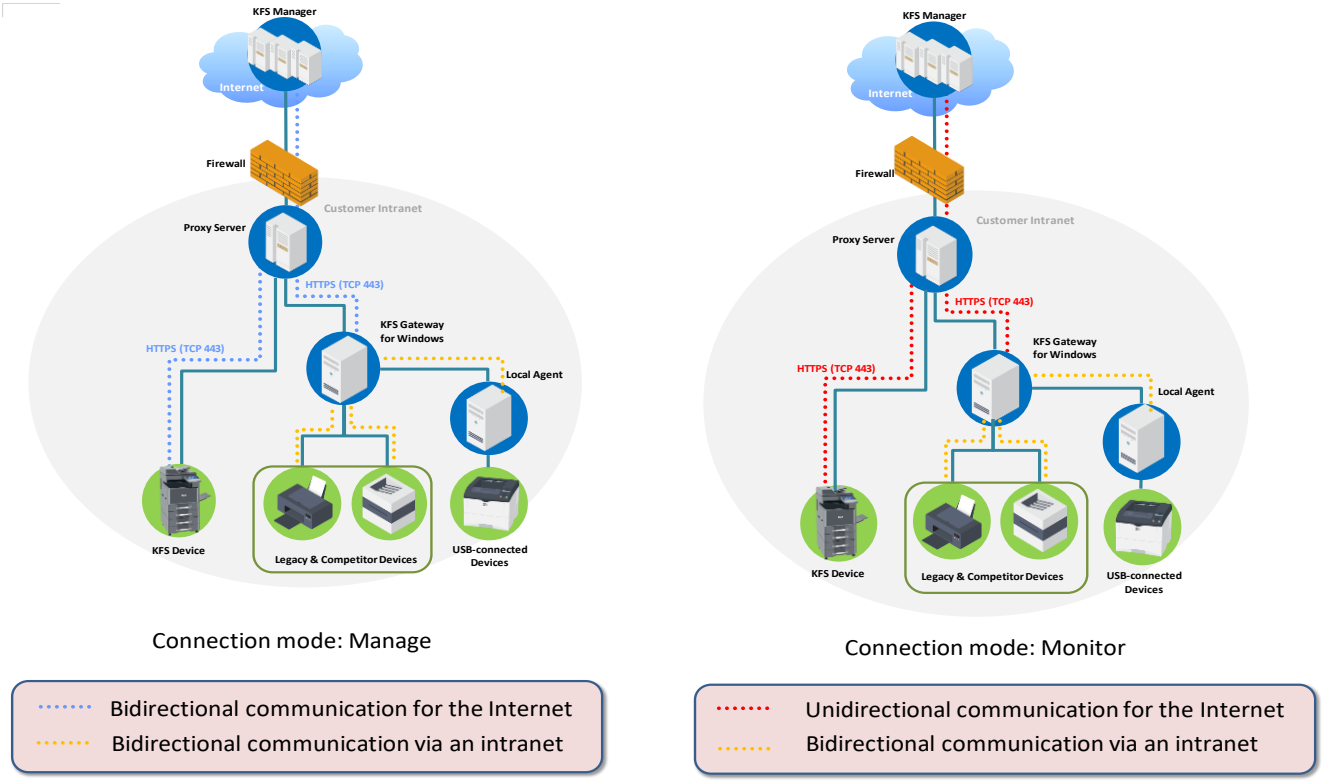

Figure 3 Connection Mode

4.4. Single-Point of Outgoing Connection

TA/UTAX Fleetmanager 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.

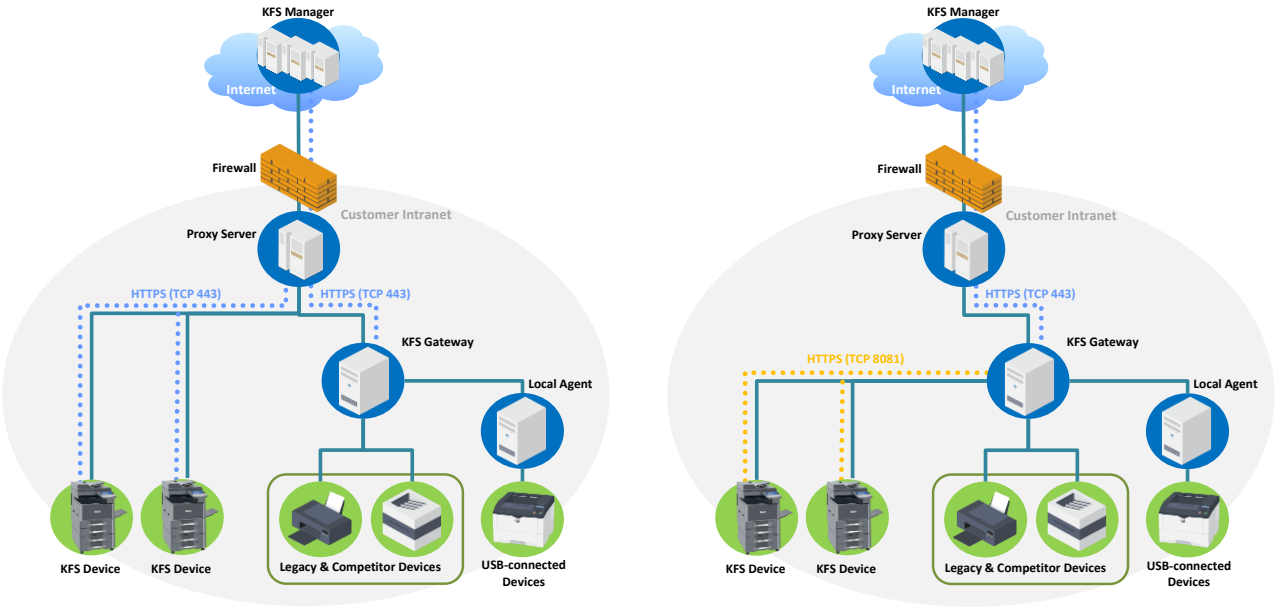

Figure 4 Comparison of Connection With (the Right Figure) and Without (the Left Figure) Single-Point of Outgoing Connection

Note: TA/UTAX Fleetmanager Gateway availability will vary by region.

4.5. Automatic Upgrade for TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager Gateway Preferences tab. From both a security and convenience point of view, the automatic upgrade for TA/UTAX Fleetmanager Gateway is recommended to be used.

4.6. Data anonymization mode by TA/UTAX Fleetmanager Gateway

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

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

4.7. Identification and Authentication

When accessing TA/UTAX Fleetmanager, a user must log in with the registered User ID (*11)(*17)(*18)(*19). An unauthorized user cannot access TA/UTAX Fleetmanager.

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

The following features are supported as security features for login.

(*11) 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 TA/UTAX Fleetmanager are managed and kept as confidential. Users should not let others use their 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.

Two-factor authentication can be enabled. Users can choose a method they like to get an authentication code either by using e-mail method (*17) or authenticator application (*18) method as described in the table below:

	E-mail Method(*17)	Authenticator Application (*18)
Authentication Code Generation Method	Manual core re-generation operation on TA/UTAX Fleetmanager (An authentication code is sent to the pre-registered user's email address.)	Automatic refresh on Authenticator application (Authenticator application needs to be first installed on user's mobile phone. A 6-digit number is then generated and input into the TA/UTAX Fleetmanager two-factor authentication screen.)
Authentication Code Expiration Interval	10 minutes	30 seconds
Authentication Code Length	6-digit number	6-digit number

In this way, two-factor authentication using time-restricted authentication codes (i.e., authentication code expiration interval) protects sensitive data handled through TA/UTAX Fleetmanager and communication with TA/UTAX Fleetmanager.

(*19) Re-authentication is required before editing the user's authentication information. This feature prevents an account hacking by a malicious person who changes the authorized user's email address to an unauthorized email address.

4.7.1. 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 TA/UTAX Fleetmanager from password cracking attacks.

4.7.2. Password Policy

A user needs to employ a strong password that is difficult to be analyzed and must be applicable to the TA/UTAX Fleetmanager TA/UTAX Fleetmanager 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
Password Re-Use Prohibition	Cannot be changed to the same password used previously
User ID/email address Use Prohibition	Must not contain either the user ID or the user's email address

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.

4.8. Audit Logs

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

4.8.1. Audit Logs of TA/UTAX Fleetmanager

An audit record is generated by TA/UTAX Fleetmanager for the following events:

- Successful/unsuccessful user identification and authentication
- Add/Edit/Move/Delete group and user account
- Register/Terminate/Move/Delete TA/UTAX Fleetmanager Device/ TA/UTAX Fleetmanager Gateway/ TA/UTAX Fleetmanager 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

4.8.2. Audit Logs of TA/UTAX Fleetmanager Gateway

An audit record is generated by TA/UTAX Fleetmanager Gateway for the following events(*15):

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

The history above shows the time/date(*12) 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.

(*12) 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.
(*15) It will be deleted at the latest 67 days after the audit logs is generated (email logs as well).

4.9. Protection of Stored Data

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

4.9.1. Encryption/Hashing

The sensitive information assets stored in TA/UTAX Fleetmanager components such as TA/UTAX Fleetmanager Manager(*16), TA/UTAX Fleetmanager Gateway, TA/UTAX Fleetmanager Device and TA/UTAX Fleetmanager Mobile, are encrypted with the following encryption algorithms. The sensitive information assets stored in TA/UTAX Fleetmanager Mobile indicates for example, user password of TA/UTAX Fleetmanager Manager, refresh token for setting up a secure communication channel with TA/UTAX Fleetmanager Manager, and password for proxy server authentication. These sensitive information assets are protected by encryption. In addition, the sensitive informationen assets such as login password stored in TA/UTAX Fleetmanager and TA/UTAX 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.

(*16) 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
TA/UTAX Fleetmanager Manager	128 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.
TA/UTAX Fleetmanager Gateway (NetGateway)	256 bit	Keys are generated during registration to TA/UTAX Fleetmanager Manager and stored in the local DB.
TA/UTAX Fleetmanager 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.
TA/UTAX Fleetmanager Mobile (iOS)	256 bit	Keys are generated beforehand and embedded in application (same for all devices)
TA/UTAX Fleetmanager Device	256 bit	Keys are generated to be a unique number on the device basis during launch for each device following TA's/UTAX own algorithm and are saved to the volatile memory of the device.

Table 11 Hashing – Hash Algorithm

System Name	Hash Algorithm
TA/UTAX Fleetmanager Manager	Salted SHA -256
TA/UTAX Gateway (NetGateway)	Unsalted SHA -256

4.9.2. 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

System & Current Data	Backup Timing:	Frequency:	Retention Period
	- 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.

4.10. Protection of Communication Data

TA/UTAX Fleetmanager realizes protection of communication data regarding user access to use TA/UTAX Fleetmanager, data communication to transfer data between TA/UTAX Fleetmanager and device, and tasks, respectively.

In order to protect TA/UTAX Fleetmanager communication data from masquerading, tapping or modifying the data, the communication data is encrypted, and TA/UTAX Fleetmanager components are mutually authenticated.

4.10.1. User Access

When a TA/UTAX Fleetmanager user accesses TA/UTAX Fleetmanager via a web browser or mobile application, an authenticated communication channel is established.

Communication to access TA/UTAX Fleetmanager via Web browser or mobile application

TA/UTAX Fleetmanager user can access TA/UTAX Fleetmanager Manager from the Web browser's client UI or mobile application UI regardless of the user role. When a user accesses TA/UTAX Fleetmanager Manager, the user is always identified and authenticated. If this identification and authentication are successful, the user can access TA/UTAX Fleetmanager Manager based on his/her role. TA/UTAX Fleetmanager Manager protects the communication data through HTTPS.

4.10.2. Data Communication

TA/UTAX Fleetmanager sends and receives encrypted data to and from devices located in a users' environment via the internet and local area network.

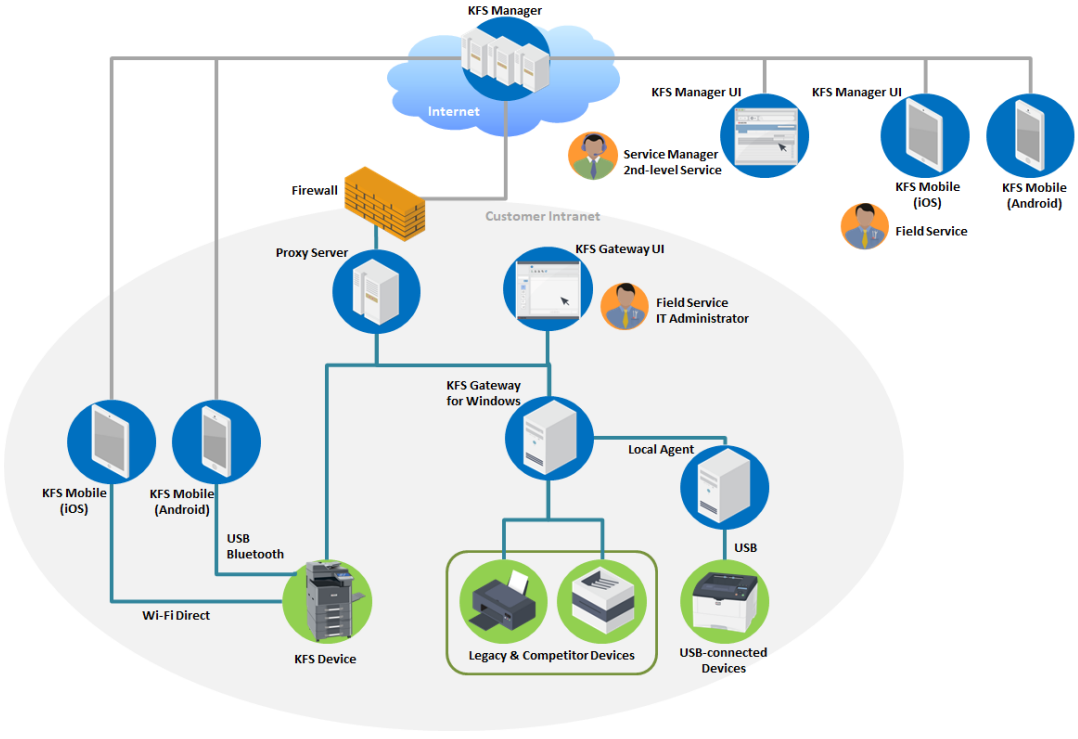

Figure 5 TA/UTAX Fleetmanager Components and Data Flows

Communication with TA/UTAX Fleetmanager via the Internet

TA/UTAX Fleetmanager network communication is set up by XMPP/ MQTT server and TA/UTAX Fleetmanager Manager in the cloud. XMPP/MQTT protocol uses HTTPS protocol for transporting. XMPP/MQTT protocol is used for the communication between TA/UTAX Fleetmanager Manager and XMPP/MQTT server in the cloud, or for the communication between TA/UTAX Fleetmanager Gateway/ TA/UTAX Fleetmanager Device and XMPP/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 TA/UTAX Fleetmanager via Local Area Network

The web service between TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager Components

One-to-one secure communication between TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager Manager and XMPP Server ➢ Communication between XMPP Server and TA/UTAX Fleetmanager Gateway/ TA/UTAX Fleetmanager Device
• Message Queueing Telemetry Transport (MQTT)	➢ Communication between TA/UTAX FM Manager and MQTT Server ➢ Communication between MQTT Server and TA/UTAX FM Device
• Hyper Text Transport Protocol Secure (HTTPS)/TLS1.2	➢ Communication between Web browser's client UI and TA/UTAX Fleetmanager Manager

	➢ Communication between TA/UTAX Fleetmanager Mobile and TA/UTAX Fleetmanager Manager ➢ Communication between Web browser's client UI and TA/UTAX Fleetmanager Gateway ➢ Communication between TA/UTAX Fleetmanager Manager and XMPP Server ➢ Communication between XMPP Server and TA/UTAX Fleetmanager Gateway/ TA/UTAX Fleetmanager Device ➢ Communication between Web browser and Relay server
• Simple Network Management Protocol (SNMPv3)	➢ Communication between TA/UTAX Fleetmanager Gateway and device
• Simple Object Access Protocol (SOAP WSDL)	➢ Communication between TA/UTAX Fleetmanager Gateway and device
• Bluetooth • Wi-Fi Direct	➢ Communication between TA/UTAX Fleetmanager Mobile and TA/UTAX Fleetmanager Device
• USB	➢ Communication between TA/UTAX Fleetmanager Mobile (Android) and TA/UTAX Fleetmanager Device

4.10.3. Tasks

Maintenance and management tasks are performed by TA/UTAX Fleetmanager users through TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager, 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 TA/UTAX Fleetmanager Device

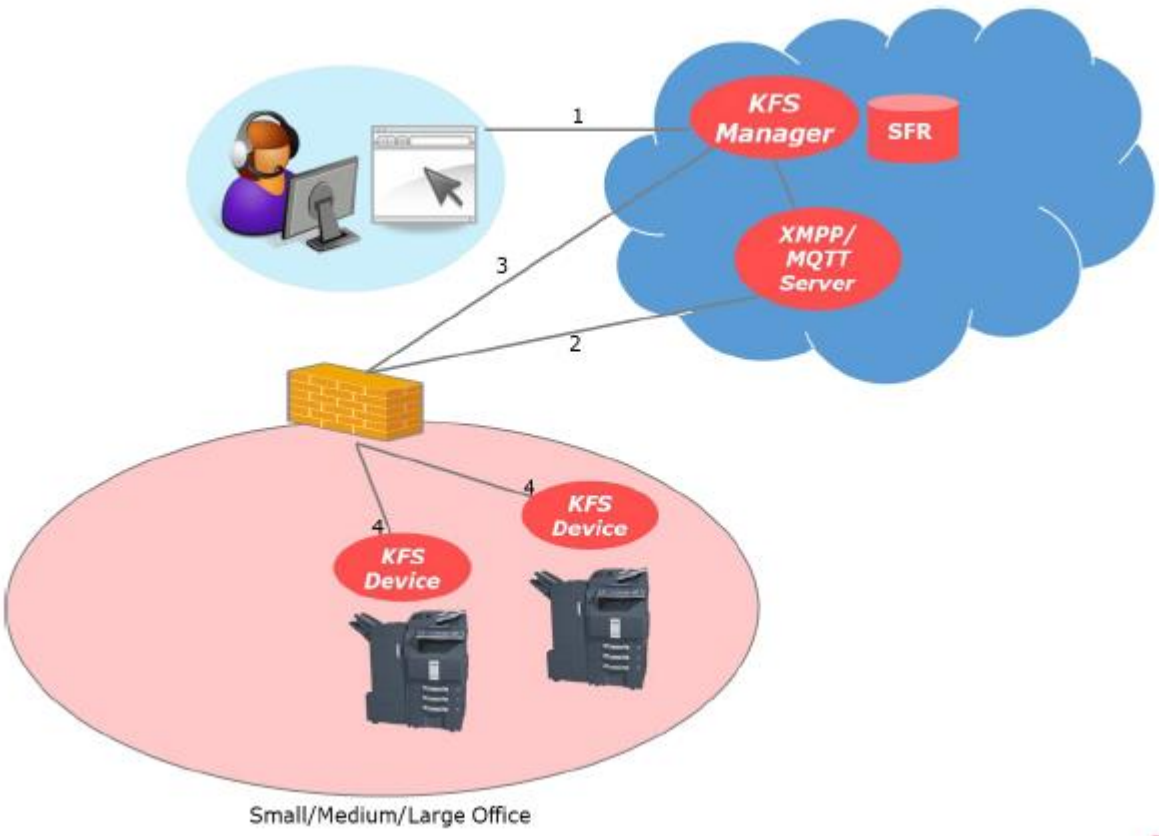

Figure 6 Communication flow of firmware upgrade from TA/UTAX Fleetmanager Device

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

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

Firmware upgrade communication from TA/UTAX Fleetmanager Mobile

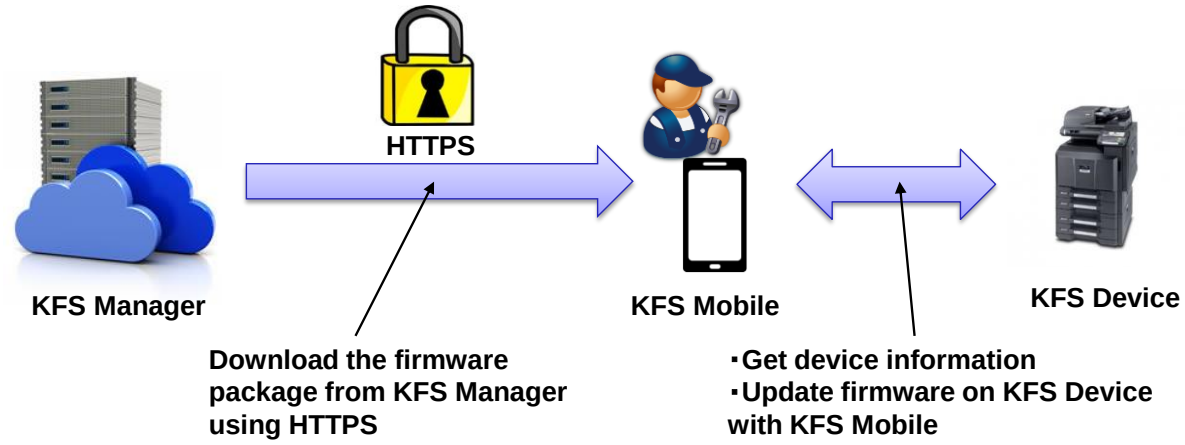

Figure 7 Communication flow of firmware upgrade from TA/UTAX Fleetmanager Mobile

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

1. The service personnel use TA/UTAX Fleetmanager Mobile to check the latest firmware package from TA/UTAX Fleetmanager Manager.

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

Firmware upgrade communication from TA/UTAX Gateway

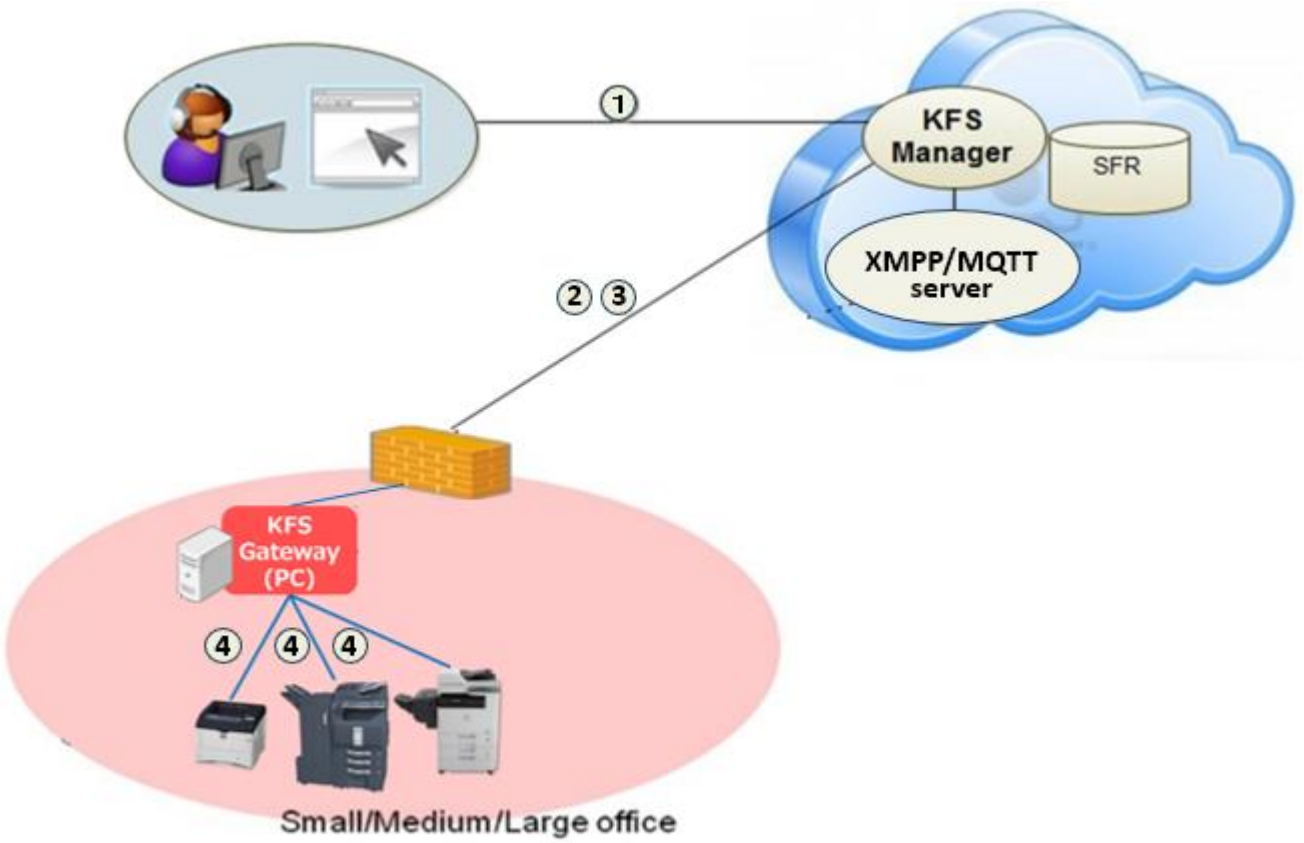

Figure 8 Communication flow of firmware upgrade from TA/UTAX Gateway

As shown in Figure 8, a secure firmware upgrade to devices through TA/UTAX Gateway is achieved with the above-mentioned secure communication through the following steps:

1. User selects a firmware package for a device through TA/UTAX Fleetmanager Web browser's client UI or mobile application UI. The communication between Web browser's client UI and TA/UTAX Fleetmanager is protected through HTTPS.
2. TA/UTAX Gateway initiates secure communication with TA/UTAX Fleetmanager through the HTTPS protocol, and retrieves firmware upgrade task from TA/UTAX Fleetmanager.
3. TA/UTAX Gateway securely downloads firmware package from TA/UTAX Fleetmanager through HTTPS.
4. TA/UTAX Gateway initiates communication with device in local network, sends firmware upgrade command to the device, and then updates the firmware.

Communication of Remote Device Panel Capture

TA/UTAX Fleetmanager provides a remote device panel capture feature that can display the current panel image of a managed device on TA/UTAX Fleetmanager 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.

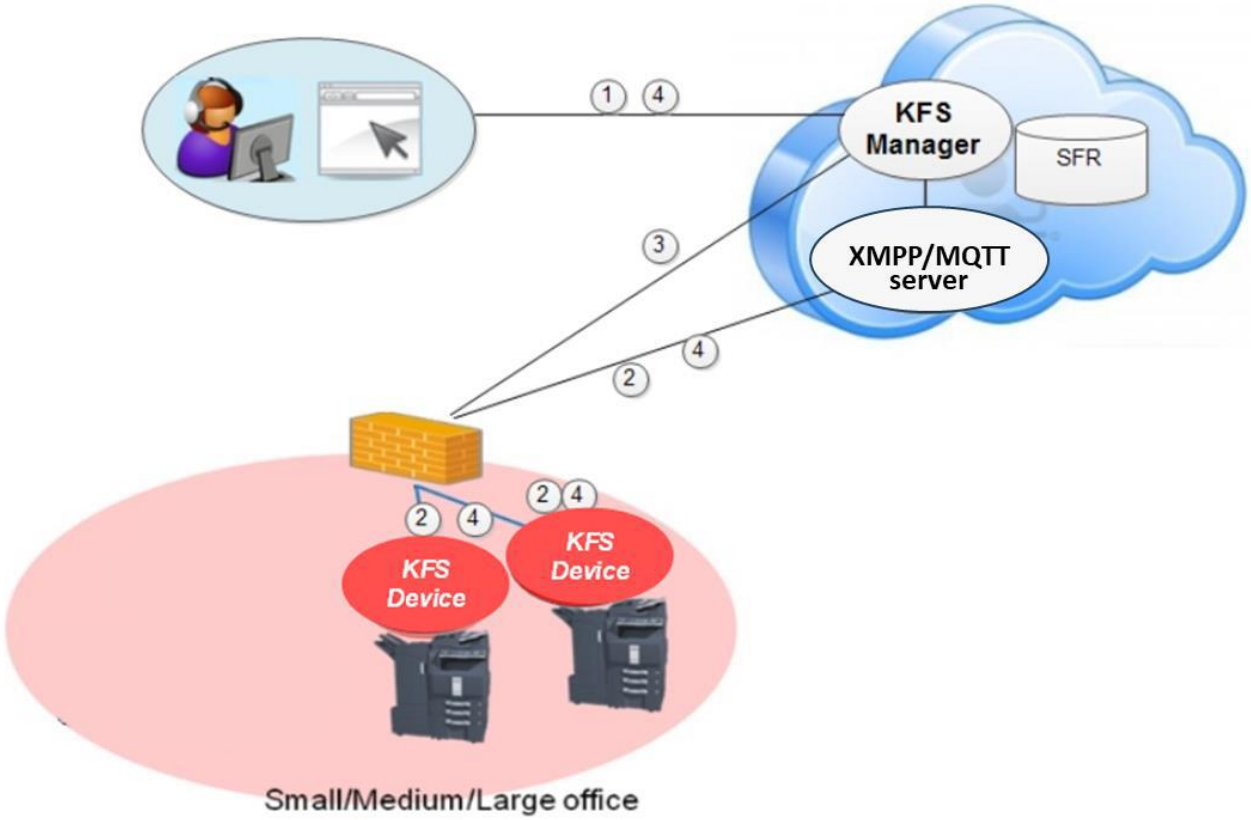

Figure 9 Communication flow of remote device panel capture

As shown in Figure 9, the remote device panel capture is achieved with a secure communication through the following steps:

1. TA/UTAX Fleetmanager user requests capture device panel information from TA/UTAX Fleetmanager Web UI through HTTPS.
2. TA/UTAX Fleetmanager initiates communication with TA/UTAX Fleetmanager device through a secure XMPP/MQTT protocol communication and sends captured device panel information to KFS Device.
3. TA/UTAX Fleetmanager Device sends the image of the device's current panel information to TA/UTAX Fleetmanager through HTTPS. TA/UTAX Fleetmanager Device updates the captured image every time the panel screen of the device is updated.

4. TA/UTAX Fleetmanager can terminate this process by sending a stop command to TA/UTAX Fleetmanager Device through a secure XMPP/MQTT communication channel.

Communication for obtaining Remote Device Snapshot Data

To support a TA/UTAX Fleetmanager user in performing device diagnostics, the following device snapshot data can be obtained from TA/UTAX Fleetmanager 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

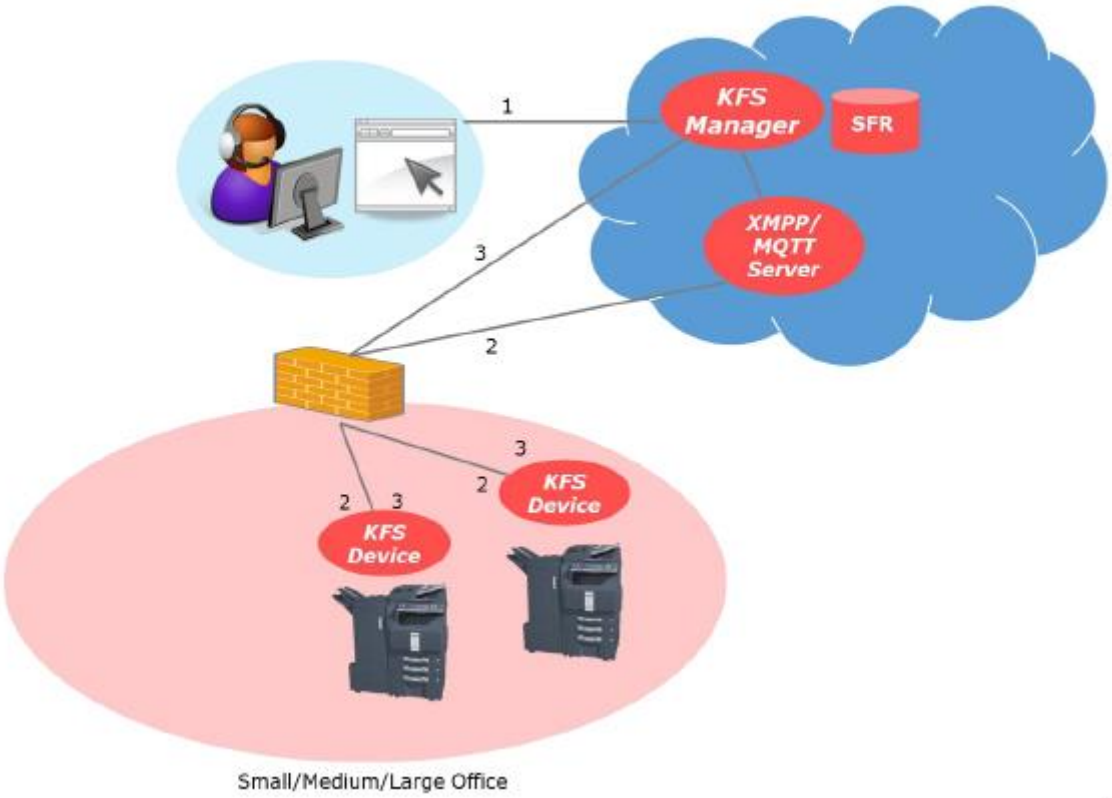

Figure 10 The flow of obtaining remote snapshot data

As shown in Figure 10, the TA/UTAX Fleetmanager remote device snapshot feature uses secure communication :

1. TA/UTAX Fleetmanager Manager user requests device snapshot information from either TA/UTAX Fleetmanager Manager Web UI or mobile application UI through HTTPS.
2. TA/UTAX Fleetmanager Manager initiates communication with TA/UTAX Fleetmanager Gateway/ TA/UTAX Fleetmanager Device through a secure XMPP/MQTT protocol, and sends the snapshot command.
3. TA/UTAX Fleetmanager Gateway/ TA/UTAX Fleetmanager Device retrieves snapshot information from a specified managed device, and sends the snapshot information to TA/UTAX Fleetmanager Manager through HTTPS.

Communication of Remote HyPAS Management

TA/UTAX Fleetmanager provides remote HyPAS management such as remote installation, uninstallation, activation and deactivation of HyPAS application on TA/UTAX Fleetmanager Device.

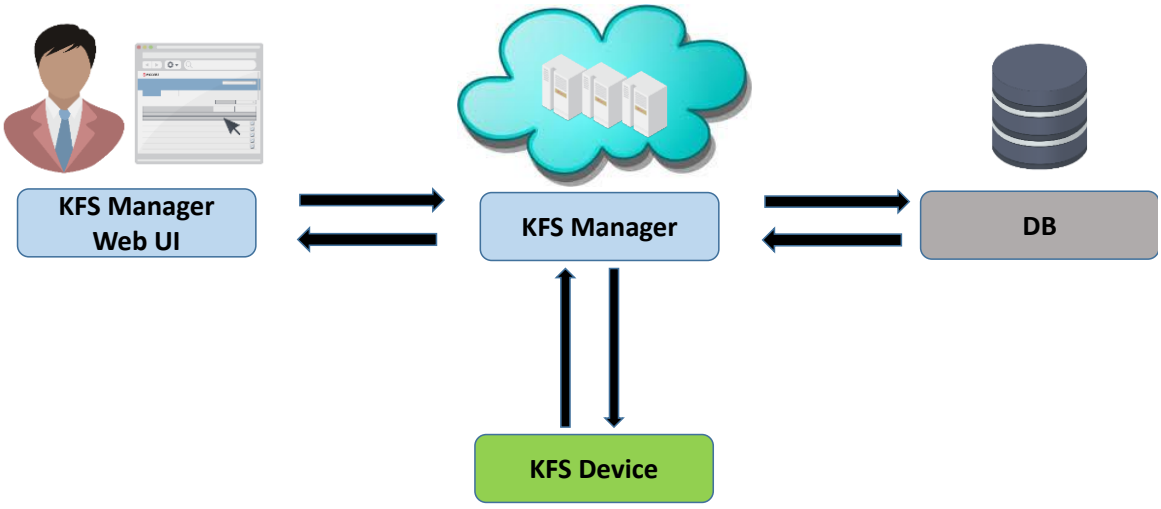

Figure 11 The flow of remote HyPAS management

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

1. TA/UTAX Fleetmanager Manager user requests a list of HyPAS applications from TA/UTAX Fleetmanager Manager Web UI through HTTPS.
2. TA/UTAX Fleetmanager Manager initiates communication with TA/UTAX Fleetmanager Device through a secure XMPP/MQTT protocol communication, and sends TA/UTAX Fleetmanager 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. TA/UTAX Fleetmanager Device downloads the encrypted HyPAS application package file from TA/UTAX Fleetmanager Manager through HTTPS (in the case of installing the application).
4. TA/UTAX Fleetmanager Manager can terminate this process upon receipt of notification directly from TA/UTAX Fleetmanager Device when action is complete.

Communication of remote panel

TA/UTAX Fleetmanager provides a remote panel feature that can operate panel from TA/UTAX Fleetmanager Manager in addition to displaying the current panel image of a managed device on TA/UTAX Fleetmanager 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.

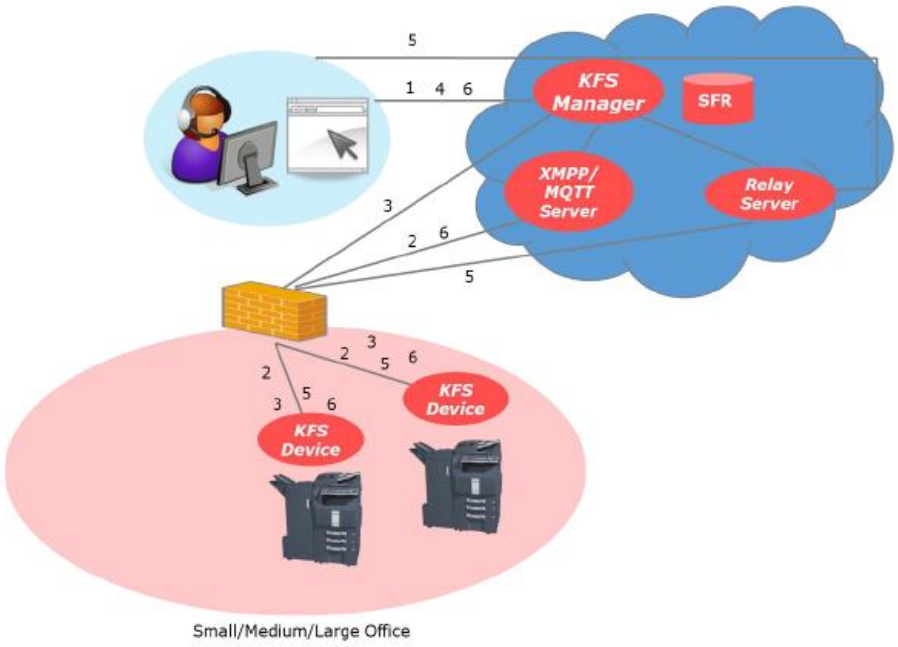

Figure 12 Communication flow of remote panel

As shown in Figure 12, the remote panel is achieved with a secure communication through the following steps:

1. TA/UTAX Fleetmanager Manager user requests remote panel from TA/UTAX Fleetmanager Manager Web UI through HTTPS.
2. TA/UTAX Fleetmanager Manager initiates communication with TA/UTAX Fleetmanager Device through a secure XMPP/MQTT protocol communication and sends remote panel request to TA/UTAX Fleetmanager Device.
3. TA/UTAX Fleetmanager Device obtains the information of relay server for TA/UTAX Fleetmanager Manager through HTTPS and connects with TA/UTAX Fleetmanager Manager in order to achieve remote panel.
4. The user's web browser obtains the information of relay server for TA/UTAX Fleetmanager Manager through HTTPS and connects with TA/UTAX Fleetmanager 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. TA/UTAX Fleetmanager Manager can terminate this process by sending a stop command to TA/UTAX Fleetmanager Device through a secure XMPP/MQTT communication channel.

5. Kyocera's effort for TA/UTAX Fleetmanager Security

Kyocera has obtained ISMS Cloud Security certification (*13) ahead of all other MFP and printer manufacutures as 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 TA/UTAX Fleetmanager. Kyocera develops TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager. Prior to releasing TA/UTAX Fleetmanager 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

Entry	Kyocera Document Solutions Inc.
Date	November 17, 2017
Renewal Date	December 19, 2021
Ranage	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.

(*13) 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.

6. Security Technical Details

This section describes defense against security threats and hosting environment.

6.1. Defense against Security Threats

TA/UTAX Fleetmanager 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 Microsoft Azure Network Security White Paper for more technical details.

At the application level, TA/UTAX Fleetmanager 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, TA/UTAX Fleetmanager responds to a failed authentication request with a delay.

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

6.2. Hosting Environment

TA/UTAX Fleetmanager 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, 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 TA/UTAX Fleetmanager). 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).

7. Health Insurance Portable & Accountability Act (HIPAA)

HIPAA regulations include security standards for the protection of electronic health information. TA/UTAX Fleetmanager is compliant with the HIPAA standards as TA/UTAX Fleetmanager does not perform the critical operation of collecting, storing and transmitting patient information that identifies an individual or a group of patients. Access to TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager. Access to the system is recorded and available for auditing. These audit logs are checked to verify that TA/UTAX Fleetmanager is secure. TA/UTAX Fleetmanager communication data is encrypted and TA/UTAX Fleetmanager components are mutually authenticated. TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager, TA/UTAX will request your authorization.

8. 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, TA/UTAX Fleetmanager Device and TA/UTAX Fleetmanager Manager use the server certificate only to encrypt the communication path. This is because the certification between TA/UTAX Fleetmanager Device and TA/UTAX Fleetmanager Manager adopts the unique method implemented on XMPP. Even if the attacker spoofs the server in some way, TA/UTAX Fleetmanager Device will not connect to that server because specific algorithm of the certification method is not disclosed. In addition, remote operation scenario including TA/UTAX Fleetmanager Device periodically performs manned evaluation using vulnerability diagnosis service in order to ensure the safety.

9. Appendix

Please refer to Figure 4 TA/UTAX Fleetmanager Components and Data Flows.

9.1. On the Intranet Firewall

- TCP port 443 (HTTPS) must be opened to allow outbound traffic. This port is used for TA/UTAX Fleetmanager Device and TA/UTAX Fleetmanager Gateway to connect to TA/UTAX Fleetmanager Manager.
- If your firewall restricts outbound traffic by a destination whitelist, the host names of Web servers in TA/UTAX Fleetmanager Manager should be added to it.
  - ➢ The names of the Web servers vary depending on which Azure data center TA/UTAX Fleetmanager Manager is hosted. This information is provided by the TA/UTAX headquarters in your region.
- In order to simplify the whitelist management of customers' firewall, XMPP/MQTT server end points are unified. This allows extracting the IP address from the existing XMPP/MQTT server and providing it as the end point of the XMPP/MQTT server. So the XMPP/MQTT servers are not required and can be removed from whitelist.
  - ➢ If the customer defines XMPP/MQTT server with host name for the whitelist, new host name needs to be added due to the XMPP/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.

9.2. On the Machine Hosting TA/UTAX Fleetmanager Gateway (NetGateway)

- TCP port 443 (HTTPS) must be opened to allow outbound traffic. This port is used for NetGateway to connect to TA/UTAX Fleetmanager 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.
- TCP port 9100 should be opened to allow outbound traffic if you wish to use the send file feature over raw port printing (RAW).

- TCP port 800 – 899 should be opened for inbound traffic. The only one port of them will be used when firmware upgrade to the 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 TA/UTAX Fleetmanager 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.

9.3. On the Machine Hosting Local Agent

- TCP port 445 should be opened for inbound traffic if you wish to use the feature of TA/UTAX Fleetmanager 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 TA/UTAX Fleetmanager Gateway for Windows 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 TA/UTAX Fleetmanager Gateway for Windows.