Knowledge Exchange (KE) V2.0 System Cyber Security Plan

Introduction

Olympus Knowledge Exchange System KE (hereinafter KE) connects to Olympus medical devices installed in a healthcare facility, collects endoscopy exam images and information, and provides integrated management on them. Installing the KE system provides smooth information exchange and utilization among endoscopic settings.

This document provides a security overview of the KE system. Customers should read this document and understand what kind of information will be protected and handled before preparing an environment for the KE system. For system requirements of devices mentioned in this document, refer to *Knowledge Exchange (KE) V2.0 System IT Specifications* (TR0136).

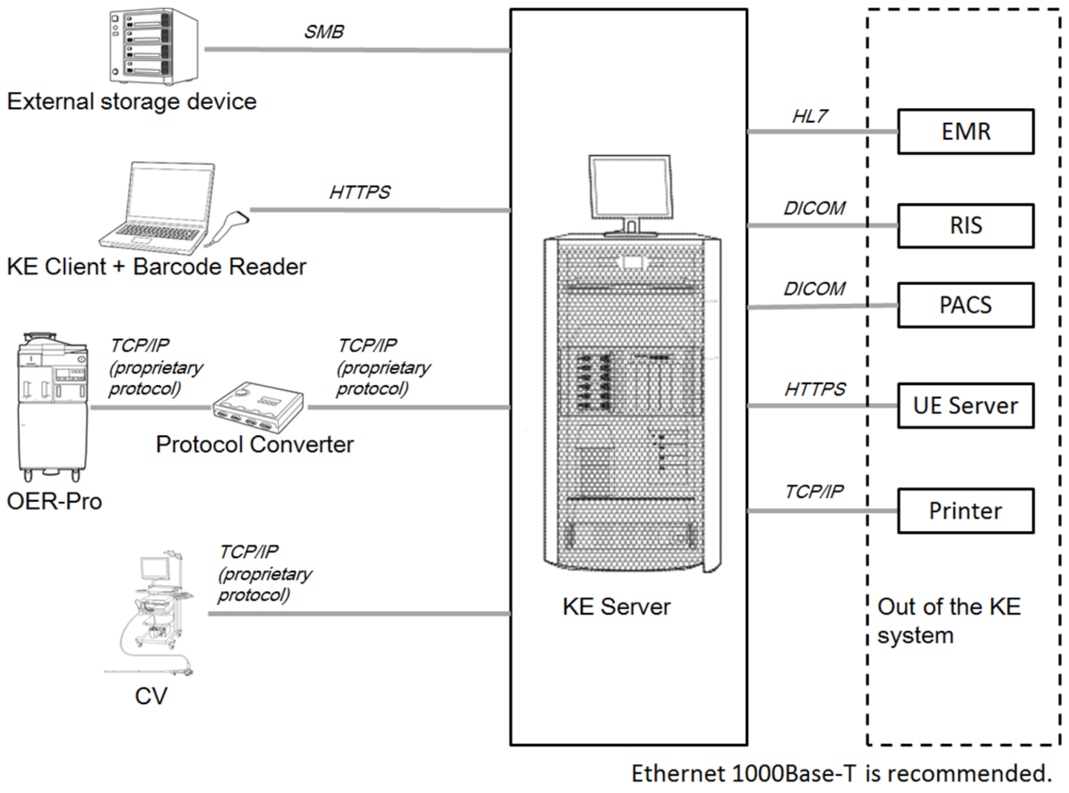
TERMS AND DEFINITIONS

Terms used in this document are defined below:

Term	Definition
KE client	Computer that connects to the KE server and operates web applications: RMM, Interface Management
KE application	General term of the following applications: • Web applications: RMM, Interface Management • Admin application
Web applications (RMM, Interface management)	Applications used by doctors and nurses to manage reprocessing information and utilize exam information; used via browser access
Admin application	Application used by customers to manage various settings and accounts of the KE application
Service tool	Tool used by FSR for installation and maintenance operation
KE software	General term of all programs provided by the product (including GUI like the KE application and service tool, gateway functions, and server functions)
KE server	Computer where the KE software is installed
KE system	The whole system that contains the KE server, medical devices, and peripherals
FSR	Field Service Resources (i.e., Olympus personnel)
DB	Database
Security appliance	Devices specific to security functions. In the KE system, they are used to encrypt communication between the KE server and medical devices.
Medical device	Olympus medical devices such as OER, CV, and CV peripherals
Medical information system	System that handles medical information (e.g., EMR, RIS, PACS)
UE	Unifia Environment UE
PHI	Protected Healthcare Information; this document defines the following information as PHI: • Patient ID • Patient name • Patient date of birth • Patient age

CONFIGURATION OF THE KE SYSTEM AND RELEVANT DEVICES

Configuration of the KE system and relevant devices is as follows:


SMB
External storage device
HTTPS
KE Client + Barcode Reader
TCP/IP (proprietary protocol)
TCP/IP (proprietary protocol)
Protocol Converter
OER-Pro
TCP/IP (proprietary protocol)
CV
KE Server
HL7
EMR
DICOM
RIS
DICOM
PACS
HTTPS
UE Server
TCP/IP
Printer
Out of the KE system
Ethernet 1000Base-T is recommended.

For maximum number of connectable devices and required hardware specifications, refer to *Knowledge Exchange (KE) V2.0 System IT Specifications* (TR0136).

Customer Responsibilities

The following recommendations should be implemented according to the facility policy and schedule. Details for these recommendations are provided in the following sections of this document.

- Network construction
- Ensuring availability and confidentiality of network
- Ensuring confidentiality of physical devices
- Monitoring and audit of the KE system
- Installation and regular updates of antivirus software
- Application of patches to the OS and middleware to keep the system up to date
- Complete data erase at disposal of the KE system
- Management of the OS and KE software accounts
- Setting encryption policy

Software Security

Installation

The KE system is installed by field service resources (FSRs). An outline of the operation procedures is as follows:

1. Customers prepare an environment that meets the requirements in *Knowledge Exchange (KE) V2.0 System IT Specifications* (TR0136) and this document to install the KE system.
2. Customers configure the KE server as instructed in the instruction manual.
3. FSRs install the KE software by using the installer, as instructed in the installation instructions.
4. FSRs configure initial settings of the KE software.

Use the KE server as a dedicated device to install and operate the KE system. Do not use the KE server for other purposes.

For safer use of the KE software, it is recommended for customers to install antivirus software[1] in step 1 (refer to *Knowledge Exchange (KE) V2.0 System IT Specifications* (TR0136)).

[1] *NIST SP 800-83 Revision 1: Guide to Malware Incident Prevention & Handling*

The FSR configures initial settings of the KE software by using the KE application and service tool in step 4. During this step, the FSR must log on to the KE application and service tool. When the FSR logs on initially, the KE application and service tool require registration or change of initial account information. As account information is managed by the customer, the FSR requests information from the customer to register or change initial account information.[2] It is the customer's responsibility to maintain passwords.

It is recommended to register a password that is compliant with facility's security policy. When registering and changing account information, the KE application does not allow the user to register a password that does not meet requirements specified by password policy function.[3] It is recommended for customers to use the password policy function of the KE application and specify values compliant with the facility's security policy. It is recommended to create a password that is relatively long, and forms a sentence (a password in long length and forms sentence(s) is considered as both easy-to-remember and strong).

Default password policies:

- Minimum password length: 8 *
- Maximum password length: 64 *
- Maximum number of repeated characters: 2 *
- Password expiration period: 365 days +
- Repeated incorrect logon counts: 5 °
- Password same as user name: Unacceptable

*A password that does not meet the specified value cannot be registered.
+ Password that exceeds the expiration period is forced to be changed.
°An account that exceeds the specified counts is locked.

The above default values are recommended password policies for the KE software. Password policies of the KE application can be changed on the Admin application. It is recommended for customers to specify values of equal or higher security level than the default values.

Passwords registered by customers in the KE software are saved in a hashed format. A hash value is generated via BCrypt with salt and stretching to make it extremely hard to calculate the original password.[4]

Upgrade

When upgrading the KE software, password policies specified before the upgrade are inherited; these values may not meet the default password policies (see *Installation* on page 4). It is recommended to manually reconfigure password policies to create secure passwords. After the upgrade, the KE software requires change of account information at initial logon. It is recommended to change passwords of exiting accounts according to reconfigured password policies.

[2] *NIST SP 800-123: Guide to General Server Security*

[3] *NIST SP 800-53 Revision 4: Security & Privacy Controls for Federal Information Systems & Organizations*

[4] *NIST SP 800-63B: Digital Identity Guidelines – Authentication & Lifecycle Management*

Account Management

Accounts of the KE software are divided into two types of authorities provided by the KE application and maintenance authority provided by service tool.[5] The KE application and service tool independently manage accounts via respective GUI.

GUI accessible from each authority is as follows:

Function	Authority	
	Administrator	User
Web application (RMM) *	X	X
Web application (Interface Management)	X	-
Admin application	X	-

* Editable fields vary depending if an authority is Administrator or User.

Accounts with maintenance authority are accessible only via the service tool. Authority types are as follows:

Authority	Description
Administrator	Authority permitted for system administrator to perform the following items: • Management and monitoring of accounts • Errors • Communication with devices • Interfaces
User	Authority for healthcare providers like doctors and nurses to use the KE application functions
Maintenance	Authority for FSRs (Olympus personnel) to install and maintain the KE software by using service tool

Customers should assign the KE software accounts only to staff who use the KE software. Each account should be provided with appropriate authority according to each user role. When an FSR needs to operate the KE application for installation and maintenance purposes, customers should provide FSR with an account of the KE application.

[5] *NIST SP 800-53 Revision 4: Security & Privacy Controls for Federal Information Systems & Organizations*

Data in Rest

The KE software stores four types of data that contain PHI (DB data, logs, backup, exam images), along with a setting file in which facility-specific settings in the KE application are specified. Details of the four types of PHI-containing data are as follows:

Data	Description	
DB data	Data stored in the DB. Refer to *Database Security* on page 11 for details.	
Log	Logs handled by the KE software are shown below. Logs other than the access log are used only by FSRs.	
	Log Type	**Description**
	Access log	Records user access to PHI. Contains PHI. Can be used for audit by users.
	Trace log	Used for fault analysis. Contains patient ID.
	Detail log	Records information that is not recorded in trace log. Used for fault analysis. Does not contain PHI.
	DB access log	Records DB access history such as SQL. Contains PHI.
	Communication log	Records communication information such as HL7 communication, DICOM communication, and telegram. The communication information contains exam information, which contains PHI.
	Middleware log	Exported by middleware like Oracle or GlassFish. Does not contain PHI.
Backup	Data backed up by backup function of the KE software as follows:	
	Data Type	**Description**
	DB	DB body. Refer to *Database Security* on page 11 for details.
	DB archive log	Records updates of DB.
	Setting file	Describes settings of the application.
	Access log	See the Access log above.
	Exam image	See the Exam image section below.
Exam image	Image captured in endoscopy exam. Contains PHI.	

The above four types of data contain PHI. The facility-specific setting files contain authentication information. It is recommended to protect these files following your facility's security policy (e.g., security authentication of OS).

File Export

The KE software has a function to export data containing PHI in a file format. The file is zipped; password protection can be added. The password-protected zip file is encrypted (AES-256)*[6] and can be safely brought out of the facility. Although this file can also be exported without password protection, adding password protection is recommended. Otherwise, the security risk remains uncontrolled.

*The file is compressed and encrypted in a format more secure than Windows standard compression function. Unzipping the data requires a third party tool (e.g., 7-zip).

Files exportable as password-protected zip files are as follows:

Data types	Description
CSV	The following information in the DB is exported to CSV file (containing PHI): • Reprocessing information • Consumables • Maintenance information of endoscopes
Trace log	At error occurrence, FSRs or customers collect trace logs (PHI), detail logs (no PHI), Windows Event Viewer Application logs and System logs (no PHI) by using the log collection tool for fault analysis. The log collection tool has a masking function to replace PHI (Patient ID) in trace logs with different characters and enables FSRs and customers to export trace logs that do not contain PHI.
Exam image	Exam images (including PHI) can be exported from the KE application.

Audit

It is recommended that customers audit the KE system for secure system operation.[7] Examples of items to audit include the following:

- Management and operation of physical devices
- Existence of network abnormality
- Notifications from the KE software
- Users of the KE system

Information of users who perform the following operations is recorded in access logs:

- Success and failure of logon and logoff
- Display, creation, update, deletion of PHI-containing data registered in the KE application
- Execution of backup and restoration

Access logs are stored starting from time of installation of the KE software (without being deleted). Customers should remove or delete the logs, as necessary, per facility policy.

[6] *NIST SP 800-66 Revision 1: An Introductory Resource Guide for Implementing the HIPAA Security Rule*

[7] *NIST SP 800-92: Guide to Computer Security Log Management*

The KE software additionally specifies OS folder audit settings to the following folders at time of installation. When a user accesses (views, edits, deletes, etc.) the following files or folders, the user name (Windows OS ID) and operation description are logged in the Security log in Windows Event Viewer.

Stored Item	Path
Logs	%INSYSTEM%\Olympus\AccessLogs %INSYSTEM%\Olympus\ComLogs %INSYSTEM%\Olympus\DBLogs %INSYSTEM%\Olympus\Logs %INSYSTEM%\Olympus\Temporary\HISGateway
Exam images	%INDATA%\Olympus\Files\Images %INSYSTEM%\Olympus\Temporary\CVGateway %INSYSTEM%\Olympus\Temporary\DICOMGateway
Facility-specific settings	%INSYSTEM%\Olympus\Config

%INSYSTEM%: Location to install middleware and the KE application
%INDATA%: Location to install DB

It is recommended for the customer to store, manage, and analyze Windows Event Viewer Security logs. Appropriate storage, management, and analysis of the above logs helps to detect and prevent unauthorized access to or falsification of the files in the table above.

The default capacity of the Security logs is 20 MB. When logs exceeding 20 MB are recorded, old logs are overwritten. The type and amount of logs exported to Security depends on Windows audit policy settings. The stronger the security policies, the more logs are exported. The KE server specifies HDD capacity based on the minimum log amount required to securely operate the system. When stronger security policies are specified, logs exceeding the specified capacity may be exported.

Customers are responsible for specifying log storage capacity according to the required period listed in the table on the next page. Increase of audit logs is a general issue and frequently addressed. Customers should review the information below, configure the appropriate capacity, and remove or delete security logs from the KE server as necessary.

Storage period and capacity of Windows Event Viewer security logs:

Storage Period	Log Space*
30 days	20GB
90 days	55GB
180 days	105GB
1 year	210GB
3 years	620GB
5 years	1030GB

* Log space sizes above are based on all audit settings being enabled.

Backup and Restoration

The KE software includes a backup and restoration function.[8] When an error occurs in the KE software, it can be restored to the status before the error occurred by accessing a backup. When the facility does not use the backup function of the KE software, it is the customer's responsibility to install third-party software and back up data regularly.

Details of backup and restoration functions are as follows:

Function	Description
Automatic backup	Automatic backup has the following three functions: • The KE software acquires a backup of data at a scheduled time every day. Users can specify the time. • The KE software acquires a backup of DB archive logs at a regular interval. Users can specify the backup interval from 1 to 23 hours. • The KE software acquires a backup of exam images, application setting files, and access logs at a regular interval. Users can specify the backup interval from 5 to 60 minutes.
Manual backup	Manual backup has the following two functions: • Users can acquire a backup of data manually on demand. • Users can acquire a differential from the latest acquired backup. Backed up data include DB archive logs, setting files, access logs, and exam images.

Furthermore, it is recommended to configure audit functions (see *Audit* on page 8) and access limits (see *Data in Rest* on page 7) for more security-enhanced storage of backup data.[9]

Restoration Function:

Function	Description
DB/AP restoration	At error occurrence, restores application settings, DB, access logs, and images.
Exam image restoration	Restores exam images at error occurrence.

[8] *NIST SP 800-34 Revision 1: Contingency Planning Guide for Federal Information Systems*

[9] *NIST SP 800-92: Guide to Computer Security Log Management*

Uninstallation

The Uninstaller of the KE software does not delete backup files and data that customers saved outside of the hardware. In addition, data deleted by the uninstaller may be restored by a third-party restoration tool.

When uninstalling the KE software, it is recommended to completely delete data in hardware, media, and external storage device used for the KE system by using third-party software to securely dispose data.[10] Customers are responsible for data disposal.

Database Security

The KE software installs and uses Oracle Database 12.1.0.2. Information stored in the DB may contain PHI. The KE software encrypts columns that possibly store PHI for enhanced confidentiality.[11] Furthermore, although the password is not subject to PHI, it is hashed when stored in the DB.

When deleting DB data from the KE software, the data is logically deleted.* Although it is hidden from GUI, the data itself remains in the DB. Make sure to operate the KE software taking this into account.

* When deleting only patient information manually registered via WEB application (RMM), it is physically deleted.

Offline

When a network error occurs, and medical devices and the KE server are disconnected, they can run alone respectively. After the connection is recovered, data accumulated in medical devices during offline operation can be sent and registered in the KE server.

[10] *NIST SP 800-88 Revision 1: Guidelines for Media Sanitization*

[11] *NIST SP 800-111: Guide to Storage Encryption Technologies for End User Devices*

Communication Between the KE Server and the KE Client

The KE system adopts HTTPS as the communication method between the KE server and the KE client. The KE software installs Microsoft Internet Information Services (IIS) to realize HTTPS communication. HTTPS uses TCP port 443. When port 80 is accessed, the communication is redirected to HTTPS.[12]

HTTPS communication uses a self-signed certificate generated by IIS. It is recommended to use a public certificate to enhance security level and establish safer communication between the KE server and the KE client.

Cypher suites[13] that can be used for HTTPS communication between the KE server and the KE client are as follows:

Encrypting algorithm	**Key exchange**	ECDHE_ECDSA, ECDHE_RSA, RSA, ECDH_ECDSA, ECDH_RSA, DHE_RSA, DHE_DSS		RSA_RSA, DHE_RSA, DHE_DSS	ECDHE_ECDSA, ECDHE_RSA, ECDH_ECDSA, ECDH_RSA	
	Encryption	AES128		AES256		
	Mode	CBC				
	Hash function	SHA	SHA256	SHA	SHA256	SHA384
Protocol version		TLS1.1, TLS1.2	TLS1.1, TLS1.2	TLS1.2	TLS1.2	TLS1.2
Key length of self-signed certificate		RSA with 2048-bit key length or longer				
Key length of public certificate		RSA with 2048-bit key length or longer, or ECDSA with 256-bit key length or longer				
Hash function of self-signed certificate and public certificate		SHA256				

Customers are responsible for the installation and management of customer-provided certificates in the KE system.

[12] *NIST SP 800-95: Guide to Secure Web Services*

[13] *NIST SP 800-52 Revision 1: Guidelines for the Selection, Configuration, and Use of TLS Implementations*

Communication Between the KE Server and the UE Server

Communication between the KE server and UE server also adopts HTTPS. It also uses a self-signed certificate, and is capable of using a public certificate as well.[14]

Communication Between the KE Server and Medical Information System

It is the responsibility of the customer to ensure the security of the communication between the KE server and medical information systems (EMR, RIS, PACS, etc.).

Communication Between the KE Server and External Storage Device

When using an external storage device, it is recommended to enable the authentication function of the device. For file-sharing between the KE server and an external storage device, using a protocol equal to or stricter than SMB V3.0 is recommended. If SMB is unavailable, selecting the “Use 128-bit encryption to help protect file sharing connections (recommended)” Windows file sharing connections setting is recommended.

Communication Between Internal Components

Components in the KE software use an authentication function for internal communication to prevent access from unauthorized components.

Ports

The KE software communicates with multiple devices and uses various ports for communications. When installing the KE software, the KE installer configures the firewall to allow communication of ports in use for the KE software (for more information about used ports, refer to *Knowledge Exchange (KE) V2.0 System IT Specifications* (TR0136)).

However, depending on the facility’s device configuration, ports not in use are also allowed for communication. For enhancement of security level and safer operation of the KE system, it is recommended that customers check ports listed in *Knowledge Exchange (KE) V2.0 System IT Specifications* (TR0136) and, according to device configuration, block the ports not in use for the KE system from the communication.[15]

[14] *NIST SP 800-175B: Guideline for Using Cryptographic Standards in the Federal Government - Cryptographic Mechanisms*

[15] *NIST SP 800-128: Guideline for Security-Focused Configuration Management of Information Systems*

Hardware Security

The KE software can be installed on both physical and virtual environments. For requirements of physical devices used in the KE system, refer to *Knowledge Exchange (KE) V2.0 System IT Specifications* (TR0136).

Customers should install the KE server in a secure location where the server is physically difficult to access.[16] In addition, it is recommended to encrypt storage devices by using third-party software to prevent data theft when the KE server is brought out (for third party software that Olympus has verified its performance, refer to *Knowledge Exchange (KE) V2.0 System IT Specifications* (TR0136)).[17]

It is recommended to install UPS to securely power off the KE server when power is unexpectedly cut off due to a power outage.

The KE server can also use an external storage device as a data backup location. When using an external storage device, it is recommended to enable the encrypting function of the external storage device for more secure data storage.

After installing the KE server, customers should construct a network of the KE system. From the viewpoint of availability, it is recommended to construct a wired LAN that meets 1000BASE-T requirements. In addition, wireless communication can only be used between the KE server and the KE client in the KE system. The wireless LAN should be constructed according to the security policies of the facility. To operate the KE server more securely, configuring IP address filtering to a network relay device is recommended.[18]

Installing a security appliance is recommended for more secure communication between the KE server and medical devices. Installing a security appliance allows the establishment of VPN communication and communicating more securely.[19] Configuration of the KE system with a security appliance is shown in the following figure.

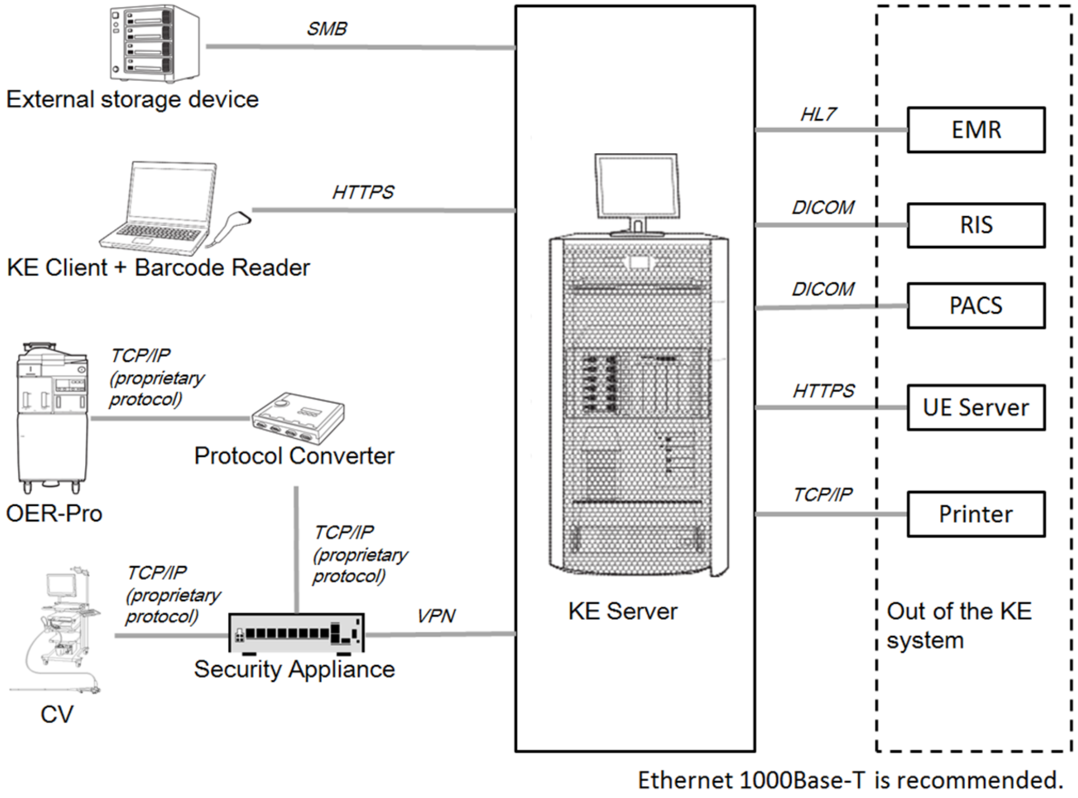
[16] *NIST SP 800-53 Revision 4: Security & Privacy Controls for Federal Information Systems & Organizations*

[17] *NIST SP 800-111: Guide to Storage Encryption Technologies for End User Devices*

[18] *NIST SP 800-41 Revision 1: Guidelines on Firewalls and Firewall Policy*

[19] *NIST SP 800-113: Guide to SSL VPNs*

Configuration of the KE system and relevant devices after installing security appliance:



Installation of a security appliance allows VPN communication between the KE server and medical devices. Compared to before the installation, you can establish communication with enhanced security level.

REGULAR UPDATES AND MAINTENANCE

Updates of OS and Middleware

Do not update any software except for the following software:

- Microsoft security updates
- Adobe Acrobat Reader DC
- Internet Explorer
- Google Chrome
- .NET Framework
- Internet Information Services (IIS)

Olympus is not liable for any application malfunction or data loss caused by the updates using software other than what is listed above. For more information about each software version qualified and approved by Olympus, contact Olympus.

Maintenance

FSRs use the OS admin account and service tool/KE application accounts for maintenance operation. Customers should provide the FSRs with a maximum of three accounts at their request.

Maintenance of the KE software is performed by FSRs with the service tool. The tools that can be started via the service tool are as follows:

- Functions and settings of backup and restoration
- License registration
- Settings of interface with HL7 devices
- Settings of interface with DICOM devices
- Settings of interface with OER
- Collection of CV detail logs
- Update
- Start and shutdown of all services provided by the KE software
- Collection of trace logs
- DB viewing function
- Export function

KE software settings may be changed by FSRs, as necessary, during maintenance operation. It is recommended that customers confirm that the settings are configured as intended.