SOFTWARE TEAM A Nihon Kohden Company Version: 16	Technical Documentation **SmartLink 3** (v3.26) Basic UDI: 805750990SMARTLINK3WM **TECHNICAL REQUIREMENTS**

Document Change Management

Version	Date	Description
01	05 Apr 2018	First issue.
02	08 Jan 2019	Layout revision and added network requirements info
03	18 Jan 2019	Revised contents in terms of requirements/recommendations
04	06 Nov 2019	More detailed supported operating systems, supported web browsers for the SmartLink server, more detailed supported Android versions, support for Zebra industrial smartphones
05	03 Feb 2020	Added new assessed Zebra smartphones
06	15 Oct 2020	Added new supported protocol converters (chapters 8.4.2, 8.4.3), Added Ascom Myco models to the supported smartphones (chapter 11)
07	9 Nov 2020	Updated the Network Requirements table and added Bluetooth column (chapter 8.1), added more options to the “Connection to data and alarms sources (chapter 8.4.2), added more recent Team Viewer versions for remote support (chapter 8.4.5), updated the list of the supported server operating systems (chapter 9.1), better specified the need of a clean machine even for SmartLink upgrades (chapter 9.1), updated the Main Alarm Station requirements (chapter 10)
08	16 Nov 2020	Fixed table of contents numbering
09	23 Nov 2020	Type corrections
10	29 Mar 2022	Certified smartphones table updated
11	30 Mar 2022	Certified smartphones table updated
12	31 Mar 2022	Certified smartphones table updated
13	03 Jun 2022	Certified smartphones table updated
14	21 Mar 2023	Certified smartphones table updated Removed certified smartphones below Android 9 Added antivirus exceptions (added as chapter 9.2) Added ports for I/O operations (added as 8.4) Changed previous chapter 8.4 and its subchapters to 8.5 and 8.5.1 etc. Updated server requirements Updated client requirements
15	01 Jun 2023	Updated server requirements Updated client requirements Updated antivirus exceptions
16	Refer to signature date	Updated server requirements Updated pager requirements Updated antivirus exceptions

SOFTWARE TEAM A Nihon Kohden Company Version: 16	Technical Documentation **SmartLink 3** (v3.26) Basic UDI: 805750990SMARTLINK3WM **TECHNICAL REQUIREMENTS**

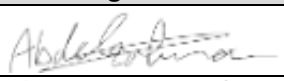
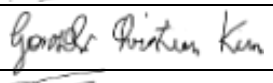
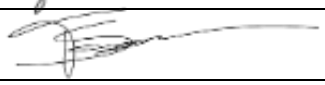
	Name	Function	Date	Signature
Written by	Abdelrahman Abdellatif	R&D	2024-07-08	
Written by	Christian Gonzalo	R&D	2024-07-08	
Reviewed by	Thainà Scherer	QARA	2024-07-08	
Approved by	Andrea Forcolin Cominotto	TDIR	2024-07-08	

Table of Contents

1. DOCUMENT INTENDED PURPOSE AND READERS 4
2. GENERAL INFORMATION 4
    2.1. MANUFACTURER CONTACT DETAILS 4
    2.2. TRADEMARKS 4
3. NOTICE 4
4. PERMISSION TO USE SMARTLINK 5
5. HOW TO READ THIS DOCUMENT 5
6. ENVIRONMENTAL REQUIREMENTS 6
7. NETWORK REQUIREMENTS 7
    7.1. General Network Requirements 7
    7.2. Wired Network 7
    7.3. Wireless Network 7
    7.4. Ports Required for SmartLink's I/O Operations 8
    7.5. Connection to Data and Alarms Sources, CIS, HIS Systems, Third-Party Systems 10
        7.5.1. Important Notice 10
        7.5.2. Connection to Data and Alarms Sources (Bedside Devices) 10
        7.5.3. Connection to Hospital CIS, HIS systems 11
        7.5.4. Connection to Third-Party Systems 11

7.5.5. Remote Access for Maintenance 11
8. SMARTLINK SERVER REQUIREMENTS 13
8.1. General Requirements for Physical and Virtual Servers 13
8.2. Antivirus Exceptions for SmartLink 14
9. MAIN ALARM STATION REQUIREMENTS 16
10. PAGERS REQUIREMENTS 16
11. BACKUP AND RESTORE 17

1. DOCUMENT INTENDED PURPOSE AND READERS

This document lists the minimal environmental requirements (Hardware, Operating Systems, Networking, …) to be set up to install and run **SmartLink 3 release 26** and its components.

This document purpose is to provide useful information to communicate or check the SmartLink 3 operating environment in order to market the product, install and give technical support.

Concerned readers of this document are sales, marketing, technical operators involved in SmartLink projects, commercial offers, installation and maintenance, the customers and anybody involved in the supply, installation and maintenance of SmartLink, including the persons responsible of the infrastructures hosting SmartLink or used by SmartLink for communication purposes.

From now on, in this document, the word “SmartLink” will refer to “SmartLink 3 release 26” and to its components.

2. GENERAL INFORMATION

2.1. MANUFACTURER CONTACT DETAILS

Legal manufacturer name: Software Team srl Tecnologie Informatiche Avanzate
Address: Via Carducci 39 – 20099 – Sesto San Giovanni (Milano – Italy)
SRN: IT-MF-000024883
e-mail: softwareteam@swt.it
Phone: +39 02 84148166
Fax: +39 02 87183477

2.2. TRADEMARKS

Trademarks, trade names and company names used in this document are for identification purposes only and are the property of their respective owners.

3. NOTICE

The listed requirements are intended as minimal requirements.

In the following tables:

- “Not allowed” means that the feature must not be present (possible malfunctioning),
- “Required” means that the compliance with the requirement is mandatory,
- “Recommended” means that the compliance with the requirement will improve the efficiency and/or the reliability of the installation,

- "Supported" means that the feature/condition is managed by SmartLink,
- "Not supported" means that the feature/condition is not managed by SmartLink.

Other features have not been listed since they either don't affect any internal test result or are not clearly related to possible interferences with SmartLink operation.

4. PERMISSION TO USE SMARTLINK

IMPORTANT NOTICE:
The contents of this document apply, from the date of this document on, to:

- all the new SmartLink installations
- updates of existing SmartLink 3 installations from release 11 to current release.

Upgrades of existing installations from previous SmartLink versions to SmartLink 3 is not applicable and then a new SmartLink 3 installation must be considered.

Unless noted otherwise, the listed requirements are intended as minimal features/performances REQUIRED, NOT SUGGESTED to use SmartLink.

In case of non-compliance with these minimal requirements, SmartLink must not be used (except for testing or demonstration).

On behalf of Software Team, in case of non-compliant configurations there will be no permission or allowance to use SmartLink.

Users that despite of this information will run and use SmartLink in a non-compliant configuration will be the only responsible of any possible direct or indirect consequence of malfunctioning, including injuries to the patients.

5. HOW TO READ THIS DOCUMENT

The document provides information about the environmental, network, hardware, operating systems, and other requirements, needed for the installation and for a good and secure operation of SmartLink and its components.

All the contents of this documents are important and we recommend designing the SmartLink installation following the sequence of chapters 6 to 11 of this document.

6. Environmental requirements
7. Network Requirements

7.1 – General Network Requirements
7.2 – Wired Network
7.3 – Wireless network
7.4 - Ports Required for SmartLink's I/O Operations
7.5 – Connection to Data and Alarm Sources, CIS, HIS Systems, Third-Party Systems
7.5.1 – Important Notice
7.5.2 – Connection of the data and alarms sources (bedside devices)
7.5.3 – Connection to hospital CIS, HIS systems
7.5.4 – Connection to third party systems
7.5.5 – Remote access for maintenance
8. SmartLink Server Requirements
8.1 – General Requirements for Physical and Virtual Servers
8.2 – Antivirus exceptions for SmartLink
9. Main Alarms Station requirements
10. Pagers requirements
11. Backup and Restore.

6. ENVIRONMENTAL REQUIREMENTS

The SmartLink server and the active network devices (including Wi-Fi infrastructures) involved in the SmartLink/SmartPager operation must be protected against AC power interruptions, to guarantee working continuity and to avoid malfunctioning or loss of data.

The active network components, the servers and in general all the active components must be protected with Uninterruptible Power Supplies (UPS) and, when possible, with redundant power supplies.

In addition, these components must be power supplied by the emergency hospital backup power.

Network equipment rooms must meet environmental conditions as specified by device manufacturers for stable operation of equipment.

The environmental conditions of these components must comply with the respective manufacturer's specifications.

7. NETWORK REQUIREMENTS

7.1. General Network Requirements

GENERAL NETWORK REQUIREMENTS		
Description	**Wired Network**	**Wi-Fi Network**
Monitoring of the usage of the network trunks shared by SmartLink and other systems / packages	Recommended	Recommended
Connection between SmartLink server and the hospital network	1000 Mbps	Not allowed
Connection between the data/alarm sources and the SmartLink server	Dedicated connection 1000 Mbps certified	Supported
Connection between SmartLink server and SmartLink Main Alarm Station	1000 Mbps *(It is recommended, if applicable, that the SmartLink server and the Main Alarm Station are connected to the same LAN/VLAN)*	Supported
Connection between the paging devices and SmartLink server	Not allowed	100 Mbps *(dedicated to SmartLink)*

7.2. Wired Network

WIRED NETWORK REQUIREMENTS		
Feature	**Requirement**	**Required**
Cabling	Cat 5e or better	Required

7.3. Wireless Network

WIRELESS NETWORK REQUIREMENTS	
Feature	**Wi-Fi Network**
Broadcast SSID	Recommended
WPA2-PSK	Required
Separate VLAN for SmartPager	Required
WLAN network speed	100Mbps (dedicated for SmartLink)

WIRELESS NETWORK REQUIREMENTS	
Feature	**Wi-Fi Network**
Notes	

The Wi-Fi network must be set up and configured to guarantee the entire coverage area where SmartPager will be used (ward, rooms, aisles, ...).

Wireless Capacity

A Wi-Fi connection bandwidth usage (peak value) under 50% is recommended to ensure that all the SmartLink paging devices can communicate correctly with the SmartLink server. Casual traffic peaks over 50% are acceptable.

Received Signal Strength measurement

Can be done during a site survey and verified using one SmartPager smartphone during a ward walk-through. Map the areas where the SmartPager loses connection (it becomes red), if any, and extend the wi-fi coverage if the case.

7.4. Ports Required for SmartLink's I/O Operations

SmartLink's components require access to the following ports for its operations:

Port	***Protocol***	***Direction***	***Server IP address***	***Client IP address***
20001	UDP	IN/OUT	SmartLink server IP	SmartWaves clients IP
20002	UDP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
20003	UDP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
20004	UDP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
20005	UDP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1

Port	*Protocol*	*Direction*	*Server IP address*	*Client IP address*
20006	TCP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
20007	TCP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
20008	UDP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
20009	UDP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
20010	TCP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
20014	UDP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
20021	UDP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1
61613	TCP	IN/OUT	SmartLink server IP or 127.0.0.1	SmartLink server IP or 127.0.0.1 MAS computer IP address SmartPagers IP addresses
25 *	TCP	OUT	SMTP server IP address	SmartLink server IP
5938	TCP/UDP	OUT	Team Viewer server (external)	SmartLink server IP

Note:

Communication **port 25** must be opened to allow SmartLink to send emails with the technical status of the installed system. These emails are sent to the SmartLink technical staff only, even in case of issues detected by the system itself.

Note:

The specified communication ports must be opened in both directions for the TCP and UDP traffic.

7.5. Connection to Data and Alarms Sources, CIS, HIS Systems, Third-Party Systems

7.5.1. Important Notice

Please ask Software Team for the up-to-date devices' connection adapter list.

In case a device connection adapter is not available yet for a specific bedside device and/or third-party solution, ask Software Team for an availability time estimation. Additionally consider:

- The devices/systems manufacturers frequently improve their products releasing new software versions, updating existing versions of software/firmware. There are no commitments by law and/or standard ways to be informed on time of these improvements.
- To guarantee a full operational and reliable installation of the devices/systems connection adapters, Software Team checks with the manufacturers the current compatibility of the devices in use by the customer and, if needed, updates the SmartLink software adapter and makes the functional tests and assessment required due to the SmartLink medical device certification.
- Updates or upgrades might be required by the manufacturers on the devices/systems to be connected, to allow them to interoperate with SmartLink. Software Team will support you in finding this information.

7.5.2. Connection to Data and Alarms Sources (Bedside Devices)

This connection can be made through either Ethernet wired network or Wi-fi network.

In case the hospital has a separate network for the medical devices, a bridge between this network and the SmartLink network is needed. A separate network card on the SmartLink server or an added network (IP class/subnet) on the SmartLink virtual server can be suitable for this. This connection must be agreed with the IT responsible of the hospital.

In case of alarm sources equipped with serial communication ports, a protocol converter must be used (here below the list of supported converters):

SUPPORTED PROTOCOL CONVERTERS	
Brand	**Model**
Lantronix	EDS-MD8
Lantronix	EDS-MD16
Silex	SD-330AC

7.5.3. Connection to Hospital CIS, HIS systems

This connection is made connecting the SmartLink network to the hospital network and installing the proper software adapters.

CONNECTION TO HOSPITAL CIS, HIS SYSTEMS	
Requirement	**Note**
Added dedicated network card on the SmartLink server	Recommended
Added separate network configuration (IP address class / subnet) on the SmartLink server network card.	Supported. As alternate solution to a dedicated network card. This might be necessary in case of server virtualization.

Notes:

1) Once realized the physical/logical connection to the hospital systems, SmartLink will not be ready to interoperate with these systems. Specific software communication drivers must be supplied by Software Team and installed for each application to be connected.
2) Updates or upgrades might be required on the hospital systems to allow them to interoperate. For these updates, please contact the hospital system manufacturer/supplier.

7.5.4. Connection to Third-Party Systems

This connection can be made done through Wired or Wireless Ethernet network.

Once realized the physical/logical connection to the third-party system, SmartLink will not be ready to interoperate with these systems. Specific software communication adapter must be supplied by Software Team and installed for each third-party system to be connected.

Updates or upgrades might be required on the third-party system to allow it to interoperate. For these updates, please contact the third-party system manufacturer/supplier.

7.5.5. Remote Access for Maintenance

This is required to guarantee the highest level of safety and security of the SmartLink systems, during the installation and configuration and once the system is made operational.

The remote access is used, by Software Team technicians and by Software Team authorized technicians, to:

- Access SmartLink to identify and fix issues

- Allow SmartLink to send emails to the Software Team technical support with information of the correct operation of the system
- Allow SmartLink to send emails in case of issues identified by SmartLink itself (these emails are automatic support requests)
- Install, during controlled sessions, SmartLink updates and upgrades of the system and check the SmartLink system operation after running the updates/upgrades.

The following table lists the standard remote access solution adopted by Software Team:

SMARTLINK STANDARD REMOTE ACCESS SOLUTION	
Solution name/tool and version	**Type of remote connection**
VPN connection	The customer must provide to Software Team the VPN client with a valid client license and a configuration file to be loaded to setup the VPN access. The VPN access account details (User, Password, other) must be provided too
Other remote access solutions	Other remote access solutions can be agreed with the customer. In this case the customer must provide to Software Team all the required software packages, software licenses and technical support for activating the remote access

.

8. SMARTLINK SERVER REQUIREMENTS

8.1. General Requirements for Physical and Virtual Servers

These requirements are for a single server machine.

One server machine is required per each ward using SmartLink.

In case of multi-ward installations, ask Software Team to define the required server configuration.

Physical Server and Virtual Server have basically the same configuration.

Automatic Windows Updates must be disabled. Windows updates installation must be agreed with Software Team and followed by a SmartLink operation test. These operation tests require a remote access to the SmartLink server by the Software Team technicians.

The SmartLink server and storage physical security is a responsibility of the technical IT staff of the customer.

As physical security shall be intended the protection of the virtual machines and of server systems hosting the virtual machines and of the data storage system.

The backup system and the backup data support must be physically protected too.

SMARTLINK SERVER REQUIREMENTS

Feature	Requirement
RAM	16 GB DDR4 (or 2133Mhz>) or more
CPU	2.2 Ghz or faster with 4 or more cores
Total free hard disk space	300 GB or more
Operating System for SmartLink	Windows Server 2019 Windows Server 2022 (**Recommended**) **IMPORTANT NOTICES (First installation):** SmartLink server software must be installed on “clean” machines, that means computers with a fresh new installation of the operating system followed by all the available operating system updates, before running the SmartLink installation package.
Network Card	1000 Mbps or more
Virtualization	VMware virtual machines. Other Virtualization systems: ask Software Team.

Automatic Windows Updates	Disabled
Internet Browser	Google Chrome (or other Chromium based browsers) to access the web configuration wizard

8.2. Antivirus Exceptions for SmartLink

Antiviruses might detect some of SmartLink's components as viruses/malware, these are false positives and are to be whitelisted, should it be necessary.

To ensure SmartLink operates at its intended behaviour, it is required to whitelist the following folders from the antivirus' operation:

- C:\apache-activemq-5.15.11
- C:\iMonitor
- C:\SetupSmartLink
- C:\xframework
- C:\Program Files\MainAlarmStation
- C:\Program Files\XFramework
- C:\Program Files\MySQL
- C:\Program Files (x86)\MySQL
- C:\Program Files (x86)\Smartlink Services

In scenarios in which it is not possible to add entire folders from the antivirus exceptions, whitelist the following processes:

- DashBoardReportService.exe (C:\iMonitor\dashboardReport\DashBoardReportService.exe)
- DashBoardSwtService.exe (C:\iMonitor\dashboardSwt\DashBoardSwtService.exe)
- iMonitorService.exe (C:\iMonitor\iMonitorService.exe)
- SmartAlarmService.exe (C:\iMonitor\SmartAlarmService.exe)
- SmartApps2Service.exe (C:\iMonitor\SmartApps2Service.exe)
- SmartControlService.exe (C:\iMonitor\SmartControlService.exe)
- SmartPagerService.exe (C:\iMonitor\SmartPagerService.exe)
- SmartTrendService.exe (C:\iMonitor\SmartTrendService.exe)
- SmartWebService.exe

(C:\iMonitor\SmartWebService.exe)

- WebAlarmService.exe
  (C:\iMonitor\WebAlarm\WebAlarmService.exe)
- XCommunicator Service
  (C:\iMonitor\XCommunicatorService.exe)
- CheckRelease
  (C:\iMonitor\CheckRelease.exe)
- CheckSmartLinkDB
  (C:\iMonitor\CheckSmartLinkDB.exe)
- CheckTypeRecords
  (C:\iMonitor\CheckTypeRecords.exe)
- LiveUpdate
  (C:\iMonitor\LiveUpdate.exe)
- XFrameworkService.exe XFrameworkService 1000
  (C:\XFramework\service\XFrameworkService.exe XFrameworkService 1000)
- XFrameworkService.exe XFM0_ _ (_ _ is a consecutive number, which is equal to the number of devices/beds)

For example:

(C:\XFramework\service\XFrameworkService.exe XFM01) = XFM01
(C:\XFramework\service\XFrameworkService.exe XFM28) = XFM28

- mysqld.exe (MYSQL)
  (C:\Program Files\MySQL\MySQL Server 5.5\bin\mysqld.exe)
- Wrapper.exe (ActiveMQ)
  (C:\apache-activemq-5.15.11\bin\win64\wrapper.exe)

9. MAIN ALARM STATION REQUIREMENTS

SMARTLINK CLIENT COMPUTER	
Feature	**Minimum Requirements**
RAM	8 GB DDR4 (or 2133Mhz>) or more
CPU	2.2 Ghz or faster with 2 or more cores
Total free hard disk space	100 GB
Operating System	Windows 11
Network Card	1000 Mbps
Video Card	Standard
Display size and resolution	24”, 1920 x 1080
Display orientation	Landscape
Virtualization	Supported

10. PAGERS REQUIREMENTS

SmartLink uses common Android smartphones as paging devices.

The certified smartphones suitable to be used with SmartLink (and its paging component named SmartPager), are listed in the following table:

SMARTLINK CERTIFIED SMARTPHONES	
Model	**Android version**
Samsung Galaxy A52	12
Samsung Galaxy XCover 5	13
Google Pixel 6a	14
Samsung Galaxy A54 5G	13
Redmi Note 13 Pro 5G	13
Samsung Galaxy A33	14

To use SmartPager, gesture-based navigation MUST be disabled, as they are conflicting with

SmartPager's own gesture-based functionalities.

Certain distributions of the Android operating system (such as MIUI and OneUI) provide screen overlays such as sidebars, which obstruct the intended usability of SmartPager, therefore, these must be disabled.

IMPORTANT NOTICE:

The table "SmartLink Certified Smartphones" lists all the allowed combinations of Smartphone/Android_Version/SmartLink_Version to be used with SmartLink/SmartPager.

In case the operating system of the smartphones is at a lower version, before installing SmartLink or before upgrading to SmartLink, update the smartphone software to reach the required Android version.

The smartphones must be used for professional purposes (personal smartphones are not allowed) and must be protected using a customer-provided MDM system against any possible configuration change, including the set of installed applications.

In case the customer needs to install on the same SmartPager smartphone other applications for professional use (phone, interphone, nurse call, CIS, or HIS mobile interfaces, other) an assessment test of non-interference must be done by Software Team in conjunction with the customer and/or the supplier of the application. In case of successful assessment, the application can be installed and used on the same SmartPager smartphone.

11. BACKUP AND RESTORE

A separate storage shall be provided by the customer, in which technicians will be able to store all files useful for the restoration of the system in case of failures.

Files can be and are not limited to:

- installation files
- configuration files (such as databases)
- configuration pdf reports
- other

It is the customer's responsibility to create a backup of said separate storage, to ensure its availability for technicians in case of storage failure.