# Unifia Environment UE

## IT Specifications

This page is intentionally left blank.

# Unifia Environment UE
# IT Specifications

## UE SERVER MINIMUM SPECIFICATIONS

- **Operating System:** Microsoft Windows Server® Standard 2012 R2 64-bit or Windows Server Standard 2016 64-bit
- **Processor:** 2 Core (4 recommended) x64 compatible, 2.4 GHz
- **Memory:** 16 GB (dedicated if virtual)
- **Disk Space:** 100 GB recommended (available for UE install and data storage)
- **Ethernet:** 100 MB Ethernet Adapter (Gigabit 1000 MB preferred)
- **Optical Drive:** DVD or USB drive (required for install)
- **Video:** 1024 x 768 or higher
- **Software:** Microsoft .NET Framework 4.62 (or higher) (Microsoft .NET Framework 4.51 is part of Windows 2012 R2: must be patched to at least 4.62)

**Note:** This server must be dedicated to the UE software. This can be a virtual server using VMWare or Hyper-V virtualization as long as the virtual system meets specifications.

## ADDITIONAL SERVER SOFTWARE

**MS SQL Server 2017 Standard with Cumulative Update 9 or higher (optionally installed and licensed by customer)**

- Microsoft SQL Server® 2017 Standard with Cumulative Update 9 or higher

**Note:** Do not install SQL Management Studio. Microsoft .NET Framework 3.5x is required by SQL Server Standard and must be installed before the SQL Server Standard installation. After the installation is complete, then .NET Framework can be upgraded to version 4.6.2 as required by UE. The UE prerequisite installer will install SQL Management Studio.

The following features must be installed:

- Database Engine Services
- Client Tools Connectivity
- Client Tools SDK
- SQL Client Connectivity SDK

Database instance, must be named *UESQLSVR*. In addition, mixed mode security is needed.

**UE Server Components (installed by Installer Package)**

- Microsoft SQL Server 2017 Express with Cumulative Update 9 (if SQL Standard not previously installed)
- Microsoft SQL Server Management Studio 17
- QlikView® Server 64-bit, Ver. 12.10 SR8
- Internet Information Services (IIS) 8.5

## UE CLIENT SPECIFICATIONS

**UE Client Components**

- Google Chrome™ version 79 or above (preferred) or Microsoft Internet Explorer® 11 (Microsoft Edge® is not supported at this time)
- Recommended Video:
  - Video: 720p (1280 x 720) or higher for Administration
  - Video: 1080p (1920 x 1080) or higher for Daily Dashboard

## UE KOAMTAC® SCANNER SPECIFICATIONS

- **Scanner Model:** IT-HW-00082
- **Interface:** Wireless network (WLAN) (2.4 GHz band only)
- **Battery:** Lithium-ion (3.7V DC, 1130 mAh)
- **Ingress Protection Rating:** IP65
- **Scanning Capability:** NFC and Barcode
- **Display:** 1” OLED
- **Weight:** 3.0 oz. (85 g)
- **Size:** 43 mm x 94 mm x 24 mm (1.69” x 3.70” x 0.94”)
- **Server Limit:** 150 scanners per server

**UE Scanner Cradle Specifications (one required per scanner, desktop or wall-mount):**

- **Desktop:** IT-HW-00083 1-Slot Charging Cradle
- **Power Requirements:** Standard 110 v, includes 5 ft cable
- **Wall-Mount:** IT-HW-00093 custom mount with up to 9” extension and charging cradle
- **Power Requirements:** Standard 110 v, includes 8 ft cable

## UE UNITECH® SCANNER SPECIFICATIONS

- **Scanner Model:** Unitech PA726 MCA (Mobile Clinical Assistant) model UNIFIA-SCNR-PA726
- **Interface:** Wireless network (WLAN) IEEE 802.11

  (Needs access to NTP time server)
- **Battery:** 3.6V 3220 mAh
- **Ingress Protection Rating:** IP65
- **OS:** Android 7.1.2

A full specification sheet is available, if requested.

- **Scanning Capability:** NFC and Barcode
- **Display:** 4.7” Color LCD Gorilla Glass with 5-point touch
- **Weight:** 10.1 oz. (with Battery)
- **Size:** 171.3 mm x 29.3 x 80 mm (6.7” x 3.1” x 1.1”)
- **Server Limit:** 150 scanners per server
- **Enclosure:** White housing with antimicrobial materials for medical facilities

**Accessories (Optional):**

- Unitech Desk Charging Station (UNIFIA-SCNR-1DT-CH)
- Unitech Spare Battery (UNIFIA-SCNR-BATT)
- Unitech 4 Bay Charging Station (UNIFIA-SCNR-4DT-CH)
- ProClip Wall Mount for Unitech PA 726 MCA (UNIFIA-SCNR-1W-CH)

## CUSTOMER RESPONSIBILITIES

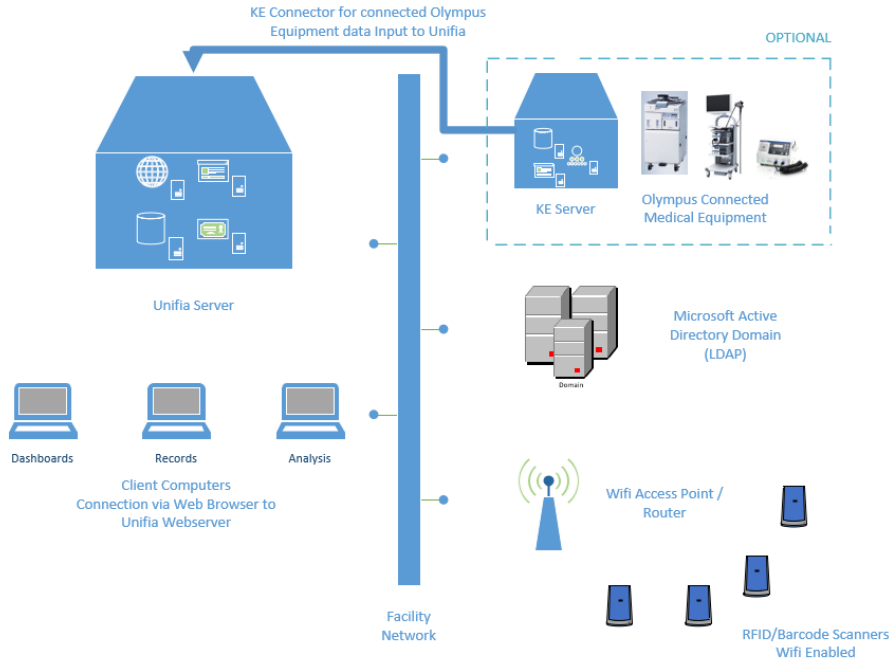
**The following items are to be performed based on facility policy and schedule:**

- Unitech Scanners require a customer-provided certificate/Root Certificate.
- Certificate format:
  - RSA-SHA-256 2048-bit
  - Request Fully Qualified Domain Name (FQDN) must match FQDN of Unifia Server
  - Certificate Signing Request (CSR) must include:
    - Key Encipherment
    - Client Authentication
    - Server Authentication
    - Subject Alternative Name Set to FQDN of the Unifia Server

  **Note:** If the FQDN of the Unifia server ends in '.Local', the certificate can only be provided from an internal certificate authority. Third-party certificate authorities no longer provide certificates for '.Local' domains.
- Installation of Operating System patches
- Optional: Microsoft SQL Server 2017 Standard with Cumulative Update 9 or higher installed and licensed according to Olympus specifications (refer to the *Additional Server Software* section on page 3)
- Installation of Anti-Virus Software and Anti-Malware Software
- Backup of SQL Server 2017 database
  (located in *%programfiles%\Microsoft SQL Server\MSSQL14.UESQLSVR\MSSQL\DATA\Unifia_Primary.mdf/*ldf
  **or**
  *%ProgramData%\Olympus\Unifia\UEDB\UserData\Unifia_Primary.mdf/ldf*)
- Network connections, wired and wireless

## CONNECTIVITY/SECURITY

### System connectivity concept




**Port Requirements**

The following is a breakdown of known ports the UE application requires.

| PORT | DESCRIPTION |
|---|---|
| TCP 443, 9722, 80 (backup port for gatekeeper) | Remote Support Services R7 (SecureLink®)<br>**Note:** These ports are external facing. |
| TCP 9754, 9755, 4780 | Application Communication and Configuration Software<br>**Note:** These ports are internal facing. (9754 is only required if Olympus Knowledge Exchange (KE) System is also purchased. 4780 is only required locally for administration) |

**Certificate Requirements** (See SP3217 *Unifia Environment UE Application & Security Overview* for more details)

**KOAMTAC Scanner:** The UE installer configures the application to use self-signed certificates. These are generated from IIS, as SHA-1 SSL 2048 bit certificates by default. Customer-provided certificates can be used and are considered a post-install activity. Customer-provided certificates are optional and must be configured as SHA-256 RSA 2048 bit certificates.

**Unitech Scanner:** The UE installer requires a customer-provided certificate from an external certificate authority, such as Symantec® or Thawte™, or from the Root Certificate from an internal certificate authority.

**Olympus Knowledge Exchange (KE) System Integration**

For Olympus KE System customers, additional software called *KE Connector* will be installed on one Knowledge Exchange (KE) server. This will allow Olympus equipment connected to that KE server to transmit data to the UE server.

## CONNECTIVITY/SECURITY (CONTINUED)

### Networking and Data Requirements

- Wired Ethernet required for local server.
- Access to Internet required for remote support services (see *Port Requirements* above).
- Domain Name System (DNS) server must be in the environment for referencing the UE server by fully qualified domain name (FQDN).
- Customer-provided Wireless network (WLAN):
  - Wireless network (WLAN) Compliance for UE scanners (KOAMTAC: 2.4 GHz, Unitech: 2.4 GHz and 5 GHz).
  - Wireless network (WLAN) SSID password has a maximum character length of 128.
- Configure UE server and clients to use a network time source for date and time sync.
- All servers and clients must be in the same time zone.
- Customer-provided wired network:
  - Wired network requires a connection to the wireless network used for the scanners.
  - UE requires a minimum 20 Mbps network speed for connection between server and clients.
- UE is limited to 15 Analysis users per UE server.
- All communication is secured using HTTPS, conforming with TLS 1.0, 1.1, and 1.2. One of these TLS cipher suites must be available in the installation environment.

### Security Features

- Secure wireless network (WLAN) support (see *UE Scanner Specifications* section):
  - KOAMTAC scanners: WPA-2 Personal supported.
  - Unitech scanners: WPA-2 Personal and WPA-2 Enterprise supported.
  - Cannot connect to wireless networks that require webpage log on or SSID, username, and password.
  - Wireless SSID password has a maximum character length of 128.
- LDAP/Domain integration:
  - Operating system and application support
- Key data column level encryption in database
- HTTPS for all connections (except online help)
- Non-generic port usage (e.g., not TCP port 80 or 8080)
- The following special characters cannot be used for the SSID or SSID password: ***& * ( )***

## SECURITY REQUIREMENTS

- Server software installation requires administrative privileges and the use of a **local administrator** account, named *administrator*.
- Microsoft Windows 2012 Active Directory™ is preferred. Additional installation steps may be required if different.
- UE can be installed into a Domain or Workgroup environment. The software uses windows user administration for either environment. When in a domain, it uses LDAP authentication (this is preferred).

  **Note:** Moving a system from a workgroup to a domain is not supported.
- When joining to a facility domain, place in Domain Organizational Unit (OU) where **no** domain policies are applied during installation phase.

  **Note:** If you need to change the OU to an OU that has policies after the installation, consult with your field representative, as this might affect application functionality.
- During the installation phase, do not change the operating system (OS) in any way from the default install, as that may impact the application install.
- The application requires the creation of accounts with 'logon as service' rights. In addition, the installer creates accounts with the following password policy: 10 characters (including at least one capital letter, one number, and one special character). The main policy should not contradict these requirements.
  If your environment has different password requirements, ensure that the OU the UE server is placed in aligns with this requirement.
- Create a user account for troubleshooting and share the user name and password with Olympus.
- UE assumes that the software, and all devices used by the software, will be in a single domain and a single OU.
- It is recommended that User Access Control be turned off during installation of the application.

For the latest version of this document and other supporting documents for Unifia Environment UE, check the following URLs:

http://medical.olympusamerica.com/customer-resources/cleaning-disinfection-sterilization/reprocessing-products/unifia

or

https://www.olympusconnect.com

3500 Corporate Parkway, P.O. Box 610,

Center Valley, PA 18034

Fax: (484) 896-7128 Telephone: (484) 896-5000