# Unifia Environment UE

## Application & Security Overview

# Unifia Environment UE
# Application & Security Overview

The Olympus Unifia Environment UE application tracks and records the reprocessing status of endoscopes through the entire workflow, from 'cabinet-to-cabinet'. Essential reprocessing data, e.g., date, time, action, scope ID, staff ID, and other, are logged at each step of the workflow, and are seamlessly entered without the need of keyboard or touch screen. This tracking system is complimented by versatile data visualization and analysis capabilities to further support critical management decisions.

The UE application is suitable for any endoscopic practice that performs endoscope reprocessing, and also supports endoscopes and reprocessors from other vendors. The application, however, provides enhanced capabilities when integrated with the latest Olympus equipment.

This document provides an overview of the features developed into the product to provide system security. Below is a component view of the system.

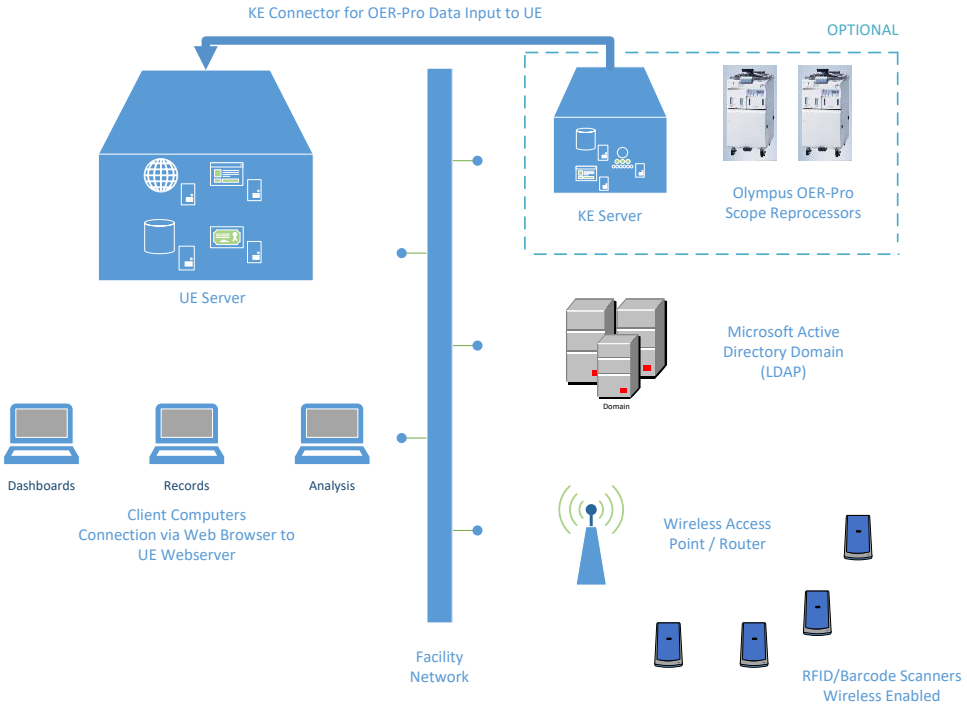



**Table of Contents**



# Customer Responsibilities

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

- Installing of Anti-Virus and Anti-Malware software
- Keeping Microsoft® operating system patches up to date
- Backing up of SQL Server® 2017 Express/Standard with Culmative Update 9 (customer can provide SQL Standard)
    - Database backup and restore, if required
- Ensuring network availability
    - Physical Network (1000 Mbps preferred)
    - Wireless Network (WPA/WPA-2 Personal protocols are supported)
    - Domain Name Service (DNS) is available
    - Application and remote support ports are not blocked by firewalls

# Platform


- **Physical or Virtual System**
- **Microsoft Windows® 2012**
- **Microsoft .NET Framework 4.62**
- **User Management Using Active Directory®**

The system can be physical or virtual, and must meet system specifications per the Olympus *Unifia Environment UE IT Specifications* document.

The application server must be Microsoft Windows 2012 r2 64-bit Server, and must be dedicated to the UE application. The operating system must be patched with the latest Microsoft patches at the time of installation. The base software requires that Microsoft .NET framework 4.62 (or higher) be installed on the system prior to installing the UE application.
**Note:** If the customer is providing Microsoft SQL Server 2017 Standard with license, the platform also requires Microsoft .NET Framework 3.5x. See the Olympus *Unifia Environment UE IT Specifications* document for additional information.

To help prepare the environment for installation and deployment, a pre-installation worksheet is completed to collect information such as:  number of scanner locations, number of scanners required, scanner positioning, and wireless strength. In addition to IT specifications, the facility's IT department is provided with a readiness checklist.

Olympus tests on virtual systems using VMWare and Microsoft Hyper-V®. If using a virtual system, it must meet required specifications and must be accessible via wired and wireless networks in the facility.

A key consideration of our design is the use of readily-available solutions tied into the operating system where possible. Examples include user management local and LDAP (Lightweight Directory Access Protocol), web services (IIS), supported encryption technologies of certificates, etc. As such, the application is developed using Agile methodology. In addition, Olympus follows industry best practices where applicable. Since the application is web server-based (using IIS on the application server), client machines do not need software installed to access the application. Access is gained via Internet Explorer® or Google Chrome™.

The application records changes to the database that are made using the data reconciliation functionality. These recordings are known as audit logs. Protected Health Information (PHI) is stored within the application, which is limited to the field that the facility elects to use as patient identifier. Files and folders, that may contain PHI are identified in the *Unifia Environment UE Maintenance Guide*. Safeguard these files and folders per your facility security policies.

It is recommended that User Access Control (UAC) is turned off during installation. It is also suggested that the UE server and clients use a network time source for date and time sync. All servers and clients must be in the same time zone.

# Installation

- **Internet Information Services (IIS)**
- **Microsoft SQL Server 2017 Express/Standard**
- **QlikView® Server**
- **Application Installation**

Application installation is performed in two (2) parts with the aid of the facility IT staff and Olympus field personnel:

**Part 1**

A prerequisite installer installs major software components the application uses. This installs the operating system features, Internet Information Services (IIS), and Microsoft SQL Server 2017 Express* with Cumulative Update 9. This installer also installs QlikView Server, which is used for reporting.

*If the customer provides the SQL Server Standard license and installation, skip the installation of SQL Server 2017 Express.

**Part 2**

The second installer is for configuration and application installation. Users that need to be created for application function are created by this installer.

The installer configures a database (DB) user, so mixed mode security is needed. After installation is complete, it is recommended that the SA user be disabled. The application uses a secondary DB user for application function. This DB user is ‘Unifia’.

As the installer and application use the facility’s local system or LDAP domain for account management, the facility’s password policy is applicable. Currently, all systems must reside in the same domain or workgroup.

The application assumes the following: 1) it is being installed in an environment where only one domain or workgroup exists, and 2) all client machines are part of the same domain or workgroup. If installing a machine on a domain, it must be installed on an Organizational Unit (OU) that has no/limited policies applied to it (e.g., password policy).

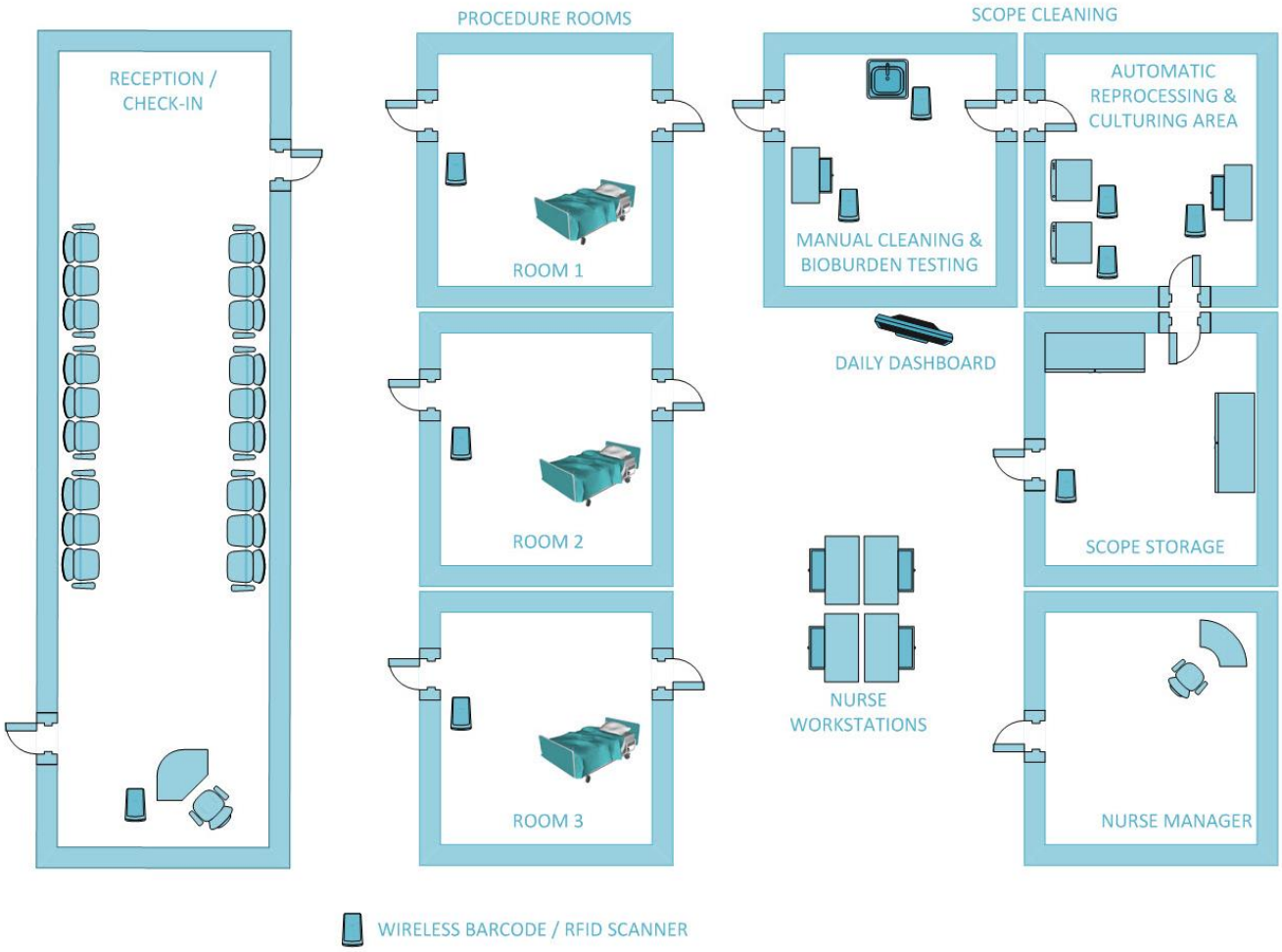
The application also needs to be installed with a local administrator account, named ‘administrator’. This account should not be modified, and the install must be executed with ‘Run as administrator’ elevated privileges. Any accounts created by the installer must be allowed to be created with ‘logon as a service’ rights.

The application installation creates a user called ‘qvservice’, which is used for QlikView Server service management. This account’s password should never expire and the ‘logon as a service’ property of the account must not be removed by policy to ensure correct function of the application.

The application creates an account local to the system called ‘uadmin’, which is used for initial application setup. It is recommended that this account be disabled at a future time if another user is assigned the administrative role for the application.

# Conceptual Facility Layout

## FACILITY LAYOUT / EXAMPLE



# Wireless Security


- **Supports WPA and WPA-2 Personal Security**
- **Support for SHA-1 and SHA-256 Certificates**

The application receives input from scanners that connect to the facility's wireless network. The scanners can connect only to wireless networks that support WPA and WPA-2 Personal security at present. The recommendation is to connect via WPA-2 Personal, if available. The facility must provide a wireless network that covers all functional areas of the implementation and ensures that the wireless network is of sufficient signal strength and speed.

Wireless SSID and password information is entered into the application through the admin functionality. The scanners are configured by a series of barcodes printed from the application.

It is recommended that the SSID of the wireless network is not broadcast openly, as an added security measure. It is also recommended that the wireless network used for the UE application be dedicated to the implementation. Once scanners are configured, the barcodes printed for configuration should be stored safely or destroyed. Anyone with a barcode reader could, potentially, read the wireless SSID and password from the barcodes.

# Application Certificates – Security


- **Self-Signed Certificates Using SHA-1 RSA 2048-Bit**
- **DNS Must Run in Environment**
- **Facility-Provided Certificate SHA-256 RSA 2048-Bit**

The installer creates self-signed certificates (for https communication to the websites hosted on the application server) in Internet Information Services (IIS) using SHA-1 RSA 2048-bit key length, based on the application server fully qualified domain name (FQDN).

The application screens are not accessible using http, and the system must always be addressed using the FQDN. As this is a requirement, DNS must be running in the environment. If the facility does not have a DNS server currently running, this can be configured on the application server.

It is recommended, for added security, that a facility-provided certificate be used for https configuration. This should be a SHA-256 RSA 2048-bit key length certificate that matches the FQDN of the application server. This can be requested from the IIS server on the application server, and be provided from the facility certificate authority (CA), or a third-party certificate provider, such as VeriSign™ or Thwarte™.

At present, the website for receiving data from the scanners cannot use a customer-provided certificate. Therefore, scanner communication to the application must use the self-signed SHA-1 certificate. This website does not display any web pages and does not pass any sensitive data.

If a facility uses Internet Explorer, they may be warned about SHA-1 certificate use. If a facility uses Google Chrome, the SHA-1 certificates are treated as a minor security issue.

# Database – Security


- **Microsoft SQL Server 2017 Express/Standard with Cumulative Update 9**
- **Only for UE Application**
- **Protected Health Information (PHI) Encrypted at Database Level**
- **Maximum Size of 10 GB**
- **Holds Approximately 250,000 Exams**

The application installs and uses Microsoft SQL Server 2017 Express, and is updated to Cumulative Update 9 at time of installation, unless Microsoft SQL Server 2017 Standard updated to Cumulative Update 9, with license is provided by the customer.

The database must be used only for the UE application and not for any other purpose. The application is not designed for the database to reside on another server or in a shared-database implementation. Any fields stored in the database that could contain protected health information, or personally-identifiable information, are encrypted at the database level. The database has a maximum size of 10 GB, which can hold approximately 250,000 exam records.

It is the facility's responsibility to back up the SQL database on a regular basis (per the facility's policy). The database is backed up to aid recovery in case of a system failure. All other information is reconstructed by the installer. This is located in the following files:

- *%Programfiles%*\Microsoft *SQL Server\MSSQL14.UESQLSVR\MSSQL\DATA\Unifia_Primary.mdf*
- *%Programfiles%*\Microsoft *SQL Server\MSSQL14.UESQLSVR\MSSQL\DATA\Unifia_Primary.ldf*

Microsoft publishes SQL Server recommended backup and restore procedures via the SQL Server Management Studio on its website.

# Remote Maintenance and Support


- SecureLink
- FIPS 140-2
- Hosted at Olympus and Data Not Shared

Olympus provides remote maintenance and support functions, to customers with active maintenance agreements, using a product called SecureLink®. SecureLink uses a gatekeeper on each application server that communicates with Olympus, using FIPS 140-2 encryption methods over SSH reverse tunneling. All communication is performed using encryption. SecureLink is an industry leader in remote maintenance and support.
See *https://rss.olympusamerica.com* for further details. The SecureLink server is hosted at Olympus in an isolated, secure environment, and data is not shared. Olympus installs a SecureLink Gatekeeper application on the application server to facilitate remote maintenance and support. The Gatekeeper uses SSH technology over a non-standard port. Implementation may require firewall configuration to allow remote support.

If your facility is a SecureLink user, the Olympus SecureLink server can link with your system.

All Olympus access to a customer system is logged in SecureLink. Customers using their Gatekeeper logon accounts have full access to their connectivity logs.

# User Management – Security


- User Management Using Local User Groups
- Application Install in Active Directory Domain

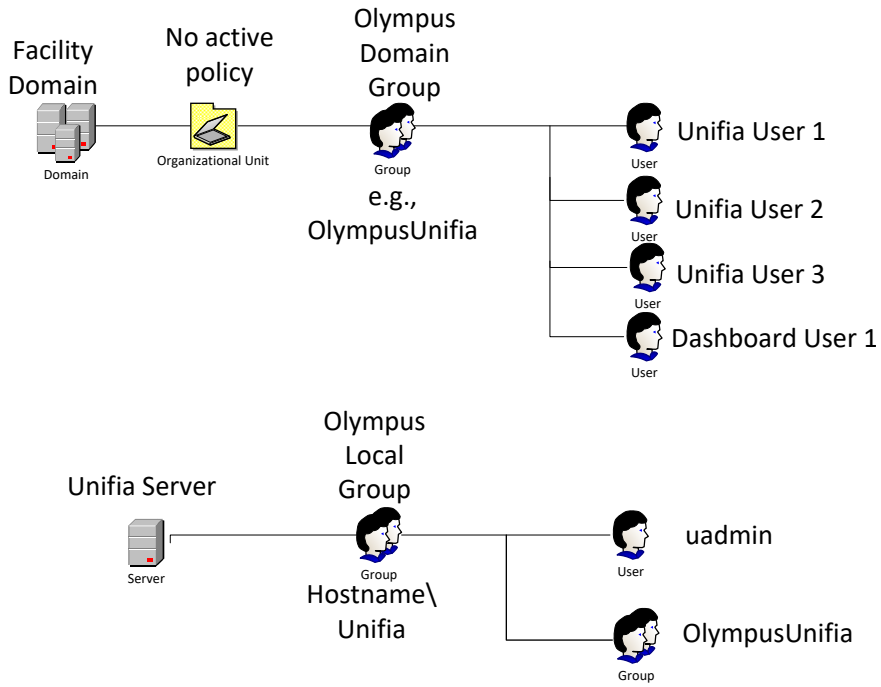
User management is done using the operating system local user groups. The installation process creates a ‘Unifia’ group on the server. In this group, a single user is created called ‘uadmin’. This user is used to log on to the Admin webpage for the application and assign roles to users.

When the application is installed in an Active Directory domain (the preferred environment), it is recommended that a Domain Group on the Active Directory is created and domain users that need access to the application are placed in this group as shown on the next page. The ‘uadmin’ user shown in the diagram is created by the application installer and does not need to be created separately.

It is recommended that standard domain policy for logon management be employed, such as multiple logon attempts that result in the lock out of the user account.

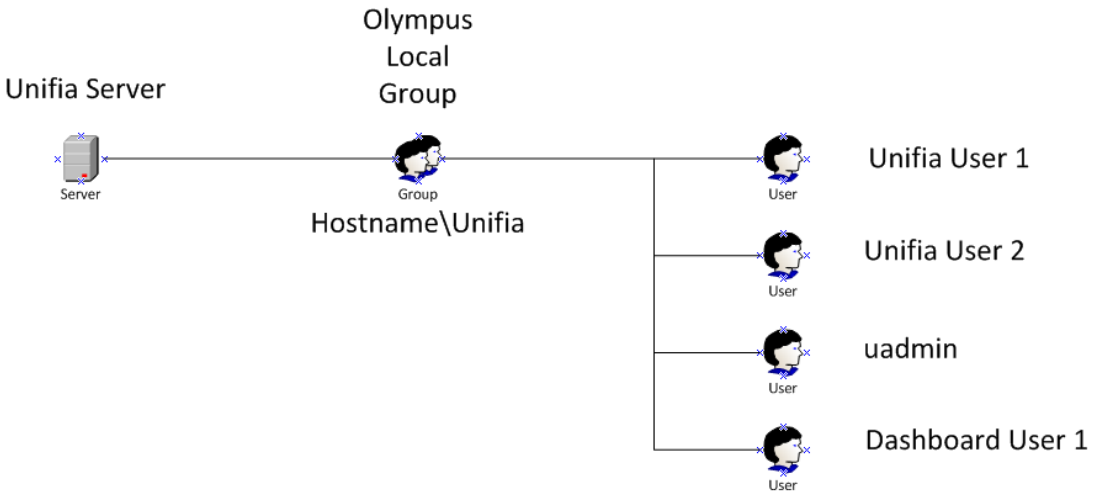
It is requested that a user account be created for troubleshooting the application. If performing an installation using an active directory domain, make the account a member of the ‘Unifia’ domain group.

Domain / Active Directory Configuration Example



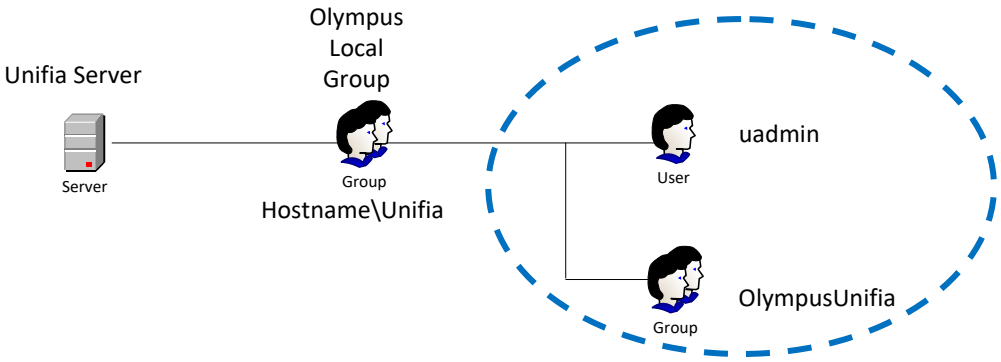

It is possible for the application to be in a workgroup environment. In that configuration, all users are created on the application server and must be placed in the ‘Unifia’ group as shown below.

Workgroup User Configuration example



It is recommended if a facility moves from a workgroup environment configuration to a domain configuration, that the local 'Unifia' group on the application server is cleaned up so only the active directory group and the 'uadmin' user are present:




# User Roles

SECURITY

- **Features are Role Based**
- **Only One Role Per User Account**

All users accounts put into the local 'Unifia' group on the application server, are authenticated using the local windows user policy or by the user policy of the facility's Active Directory domain. The application feature/task/screen each user can access, however, is determined by the user account's assigned role. The following table provides more detail.

| | **Feature/Task/Screen** | | | | | | |
|---|---|---|---|---|---|---|---|
| **Role** | Admin | Analysis | Daily Dashboard | Materials and Assets | Infection Prevention | Operations | Audit Log and record modification |
| Admin | x | | | | | | |
| Dashboard | | | x | | | | |
| Materials Manager | | | x | x | | | |
| Data Analyst | | x | x | | | | |
| Staff | | | x | x | x | x | |
| Manager/Supervisor | | x | x | x | x | x | x |

Only one role can be assigned to each user account. Therefore, if a single user needs to perform more than one role,

that user will need a separate account for each additional role. There is a maximum limitation of 15 Analysis users per UE server.

Also, it is recommended that a specific user account be created for displaying the Dashboard with access restricted to only the display machine, in an open area such as the nurses' station.

# Obsolescence and Vulnerability Procedures


- **Industry Standard Vulnerability Scanner**
- **Multiple Releases**
- **Allow all Operating System Patches as They are Available**

During the development cycle, our commitment to quality is evident through regular reviews of findings, third-party component release schedules, security risk assessments, and patient risk assessments. Our team performs code reviews, and employs both manual and automated testing principles.
Olympus allows all Microsoft operating system patches to be installed on the application server. This enables vulnerabilities to be addressed as soon as patches are available (per a facility's schedule). If there is an issue with a specific patch, Olympus will work with the facility to address the issue using established support procedures (e.g., the Technical Assistance Center [TAC]).

During development of software releases, Olympus continually performs vulnerability scans to help identify issues. Output from these scans are reviewed and assessed for potential system risk and security concerns. Remediation is prioritized based on the perceived risk by the Olympus development team. Additionally, Olympus reviews third-party components for updates and follows the same procedure.

# Scanners


- **Secure Wiresless Enabled**
- **Reads RFID and Barcodes**
- **Secure Erase Function**

As indicated previously in this document, the application uses scanners to obtain input into the application. Olympus has chosen a scanner manufactured by Koamtac that is wireless-enabled and can connect to WPA and WPA-2 personal wireless networks. The scanner supports multiple-speed networks, such as 'b', 'g', 'n', in 2.4 GHz frequency networks (with channels 1-11 supported). It is the facility's responsibility to ensure their wireless network strength is applicable in all areas needed; ideally, with a signal strength of -15 to -65 dBm.

The scanners can read barcodes and RFID tags, such as those found in Olympus endoscopes. Barcodes are used for scanning information into the system (e.g., the start of a procedure, or a physician ID).

In the event of a wireless outage, scanners have the ability to store scans in memory and then send over a secure wireless connection to our application. Authentication is via SSID name, SSID password, and website certificate generated by the application where the application is installed. Additional information can be found under the Security section of this document.

Since the scanners can store information, we developed a secure erase function with Koamtac, in the event devices need to be returned for repair.

UE is limited to a maximum of 150 scanners per single UE server.


3500 Corporate Parkway, P. O. Box 610,

Center Valley, PA 18034

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