Security Concept

An Integral Part of Development

Security Philosophy

- Integral to the product at every stage of development
- Ongoing testing and architectural reviews
- Ensure products remain secure over time in the field
- Proactively identify risks

Approach

Olympus provides a multilayer security concept which secures each product´s appliance (nCare/VaultStream) and the server communication by implementing the following measures:

Windows IoT

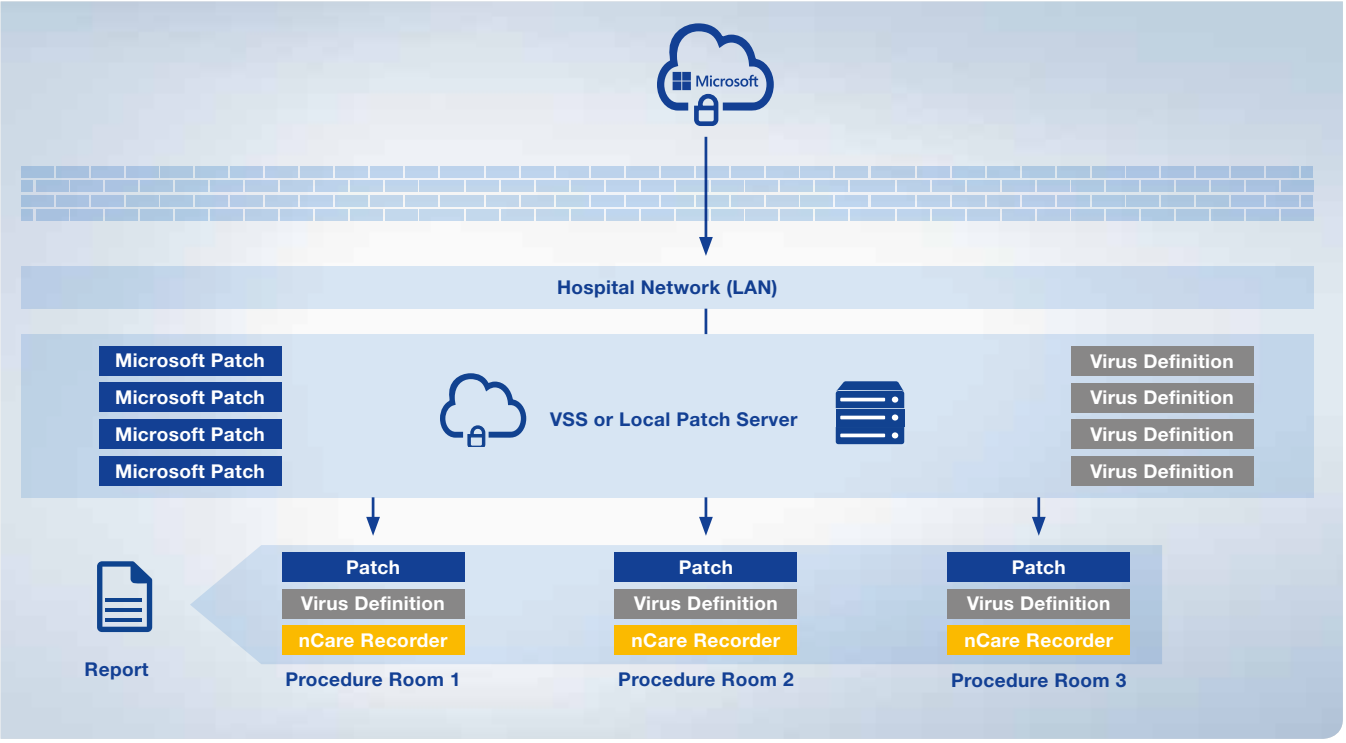
The nCare platforms are built from Windows 10 IoT LTSB. The custom image contains only the required components necessary for the device to function.

Microsoft AppLocker

Microsoft AppLocker Whitelisting allows the execution of only known and signed (trusted) applications.

Windows Defender

Windows Defender provides built-in protection against malicious software within the products and **Windows Server Update Services** to fully manage the distribution of updates that are released through Microsoft Update to computers on a hospital's network. Olympus Image Stream Medical (ISM) performs monthly testing of Windows security updates to ensure compatibility. It is very rare for a Windows security patch to be incompatible with Olympus ISM products.



Security Concept

An Integral Part of Development

Microsoft BitLocker
Microsoft BitLocker is a data protection feature that integrates with the operating system and is used to encrypt hard drives and USB drives to prevent unauthorised access.

WCF Certificate
The communications certificate allows two systems to communicate with each other. The **WCF certificates** must match in order for the two systems to communicate. The security certificates are unique identifiers used to ensure that only authenticated devices are allowed into the **VaultStream** and **nCare** system.

Firewall
An embedded firewall within systems sets policies to define allowable communications and enforces these policies by limiting communication to just the approved, required IP addresses, ports and protocols.

Secure Server Deployment
Server applications are deployed to site-supplied Windows 2012 or Windows 2016. Customer group policy may be leveraged to control baseline security on this platform. Apps and services are run as a domain service account provided by the customer. Communications between all applications are done via private encrypted channels.

Access Controls

Accounts and Passwords
There are two types of accounts in Olympus ISM products: system and application accounts.

System Accounts
System accounts are accounts which exist in the underlying operating system. All applications run with a system account of some sort. nCare also has a back-end account for services.

Application Accounts
Application accounts exist within the scope of the Image Stream applications for the purpose of providing unique user identity and role-based access within the Image Stream applications only. These user accounts can be “borrowed” from the customer’s active directory, or they can be created and managed using the native user accounts system which is installed on all Image Stream platforms.

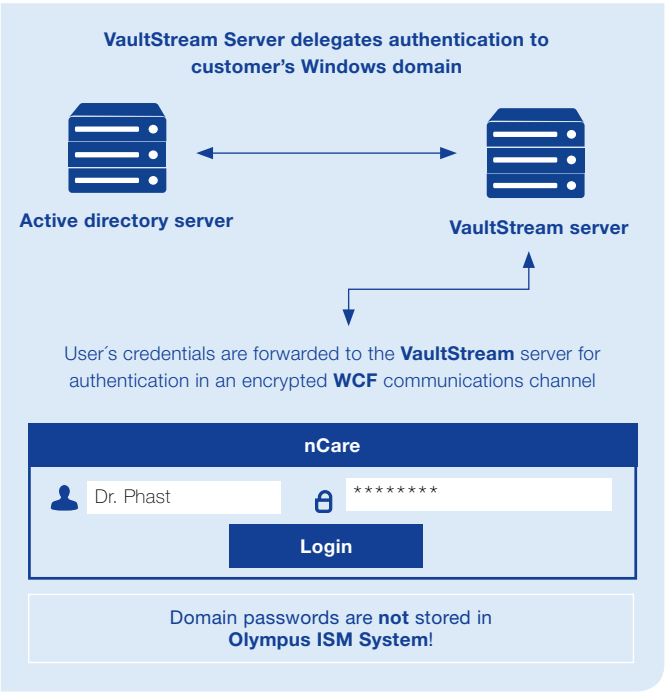
Ports and Protocols

HTTP/HTTPS
EasyView, EasyCut, and LiveStream portal can use HTTPS.

WCF
The majority of communication between the applications and services uses Windows Communication Foundation framework. These channels are SHA-2-encrypted.

Vulnerability Testing

Third-party Security Assessment
Olympus Image Stream contracted Black Hills to perform vulnerability assessments and architectural evaluations for security. This vulnerability assessment includes penetration testing and an architectural review.



Security Concept

Logging System

Overview

Olympus ISM products maintain logs at two levels: operating system (Windows Event Logs) and application (Image Stream native logging system). At both levels there exist security logs and diagnostic logs. The application logging system is installed on each host machine (nCare and Vaultstream Server) and runs as a service.

Log File Type	Description	Storage/Deletion
OS System Diagnostic Logs	· Non-Olympus ISM components that are included with the base operating system installation (like drivers etc.)	· Set to grow to 20 MB with older log entries being deleted
OS System Security Logs	· Base operating system security events like login success/failure and file processing · Supplement the Olympus Image Stream application security logs by providing a view of the underlying operating system	· Set to grow to 1 GB with older entries being deleted · Can be exported directly via VSS and nCare
Application Security Logs	· Used by customer's IT department for auditing purposes · Security logs contain identifiable data · There is no verbosity control for security logs	· These security log files are never automatically deleted
Application Diagnostic Logs	· Support Olympus engineers in diagnosing problem · Log verbosity setting of 3	· The diagnostic log files are automatically deleted after 60 days

For complete product details see Instructions for Use.

OLYMPUS

OLYMPUS AUSTRALIA PTY LTD
3 Acacia Place, Notting Hill VIC 3168, Australia
Customer Service: 1300 132 992 | www.olympusaustralia.com.au

OLYMPUS NEW ZEALAND LIMITED
28 Corinthian Drive, Albany, Auckland NZ 0632
Customer Service: 0508 659 6787 | www.olympus.co.nz