SIMULATIONiQ™ Enterprise

On-Premises IT Guidelines

Education Management Solutions, LLC
436 Creamery Way, Suite 300
Exton, PA 19341
Phone: 877.EMS.5050 (877.367.5050)
www.SIMULATIONiQ.com

Contents

Copyright Declaration

Disclaimer: The information is being provided on "as is" basis and is subject to change. Education Management Solutions (EMS) makes no warranties or guarantees about the accuracy, completeness, or adequacy regarding the information provided and expressly disclaims all liability for any damages resulting from its use.

October 2020

Open Source Declaration

Here is the list of the open source components in SIMULATIONiQ Enterprise. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. If you have any questions or wish to receive a copy of any free and open source software, please contact legal@simulationiq.com.

Name	License information
VLC Player	https://www.videolan.org/legal.html
FFmpeg	https://ffmpeg.org/legal.html
VideoJS	https://github.com/videojs/video.js/blob/master/LICENSE
BootStrap	https://github.com/twbs/bootstrap
MediaInfo	https://www.nuget.org/packages/MediaInfo.Wrapper/
Log4Net	https://logging.apache.org/log4net/license.html
NewtownSoft	https://www.nuget.org/packages/Newtonsoft.Json/
SharpZipLib	https://www.nuget.org/packages/SharpZipLib/
FFDSHOW	http://ffdshow-tryout.sourceforge.net/

IT Checklist

Administrator User Account (Domain/Local)		☐
☐ EMS service-level account (strictly for our own services in back-end of the application) ☐ Control/Debriefing Station		
Back-up and restore	See **Backup and Restore** on page 24.	☐
Browser plugins: REQUIRED for video over web, must be installed as local admin	See **Web Browser Compatibility** on page 20.	☐
Firewall Exception List	See **Network Security** on page 15.	☐
IP addresses for server, simulators (required)	See: • **Website Address** on page 19 • **AV Controller** on page 26	☐
Ports	See **Network Security** on page 15.	☐
Service Account	See **Service Account** on page 15.	☐
TSL security certificate	See **Network Security** on page 15.	☐
URL must be listed as a trusted site	See **Web Browser Compatibility** on page 20	☐
User access control	Set **User Access Control to "Never notify"** or disable.	☐
Video graphics driver requirements	Latest video graphics driver required. By not having this you may see green or gray video screens and you will not see smooth video playback or live.	☐
Web site addresses (user-friendly) – optional		☐
Streaming server license	See **Network Security** on page 15.	☐

1. Welcome!

The purpose of this document is to provide Education Management Solutions' (EMS) client IT Groups with a broad understanding of the Enterprise application deployment environment and the expectations placed on IT for successful implementation. The IT group is an important partner for EMS to provide assistance in network configurations and policy compliance for the Enterprise application solution in the client environment. This document presents the application architecture, along with IT and network needs, to allow efficient project planning and proper implementation of a successful solution.

2. Enterprise

2.1. Introduction

Enterprise is a distributed web-based application solution that includes programs and database servers communicating with other AV and computing devices. Enterprise product suites consist of two major software applications hosted across numerous computer servers. The following table provides the breakdown of the server and other component needs:

Product Name	Web Server	Database Server	DVR and Storage Server	Workstation/ Laptop
Enterprise	✓	✓		✓
Enterprise AV	✓	✓	✓	✓

***Note**: Typical installation will need one Web server and one Database server. The number of Digital Video Recorder (DVR) or Network Video Recorder (NVR), and Storage Servers and Workstation/Laptops depends on the user requirements.*

2.2. Applications

The Enterprise Solution is made up of two applications. One is Enterprise that is a web-based application to support the needs of Standardized-patient (SP) based and mannequin-based training and evaluation. All audio-video digital recording and streaming is part of the second application called Enterprise AV.

2.2.1. Enterprise

The Enterprise software integrates, automates and manages the complete clinical skills and simulation training and exam process including:

The solution is web-based and supports the learning and operational needs of a clinical skills learning center and a simulation center. The system creates a centralized database for SP and student information, history, statistics and data analysis and easily integrates with Microsoft Active Directory or LDAP-compliant User Directory services. The minimum version required for Microsoft Active Directory is Windows 2000. The system supports multiple departments or outside users and supports satellite or remote facilities and connections. When integrated with Enterprise AV, the system can perform fully automated recorded sessions for your students.

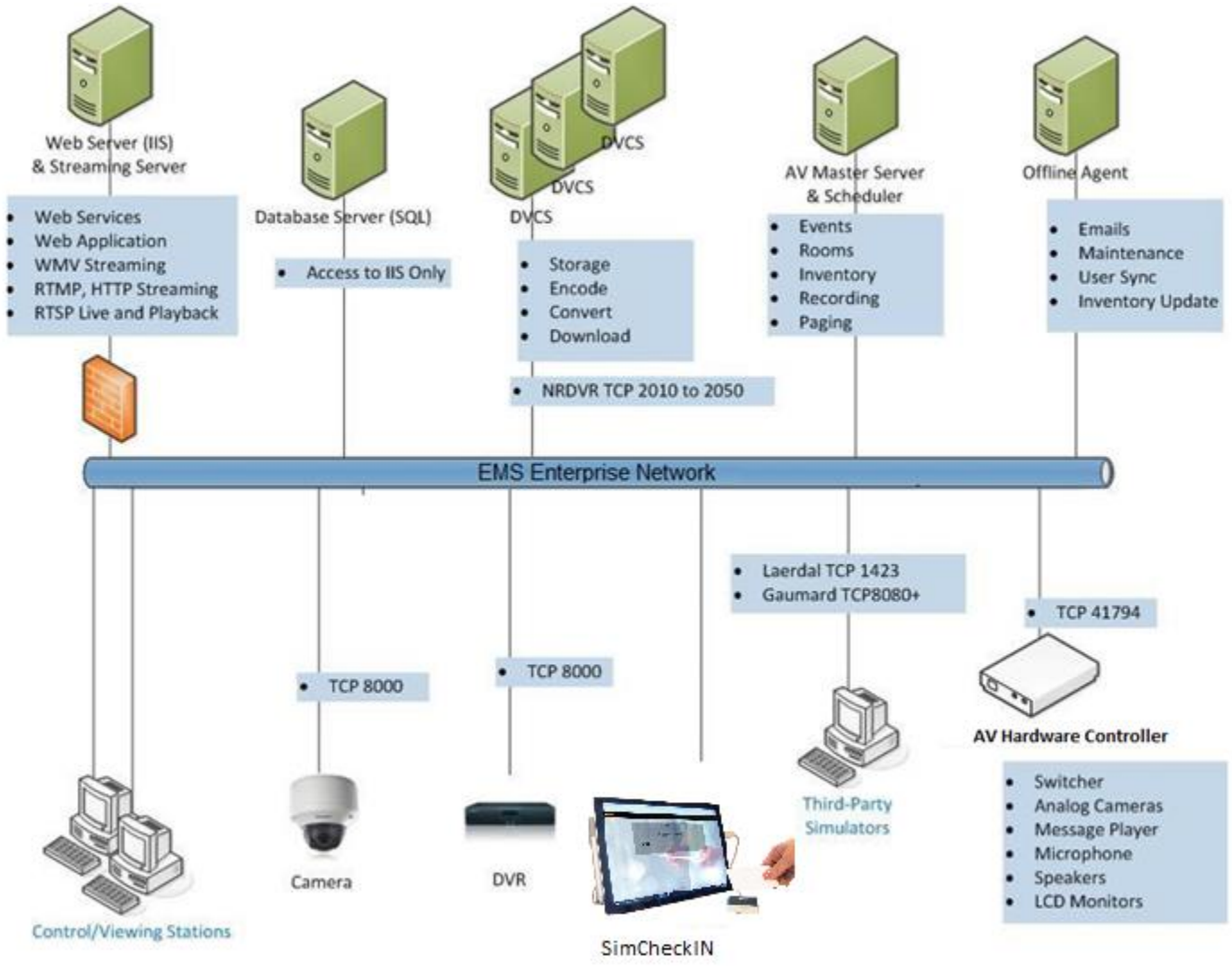
In addition, it can interface with mannequin-based patient simulators from third-party vendors, such as Laerdal, Gaumard, CAE and Simulaids. Please note the level of this integration, in terms of information access and sharing, is dependent on the interface protocol provided by simulator manufacturer. In simulation environments, Enterprise AV records audio and video from the simulation rooms as well as captures patient monitor display information and event logs from the simulators themselves, providing a complete recording of the simulation session.

2.2.2. Enterprise AV

Enterprise AV has a number of hardware and software components. It allows the user in a clinical skills environment to manage and support the digital recording and announcements in the rooms as well as control the camera pan, tilt and zoom capability. Enterprise AV provides a completely automated and integrated solution for the center. It automates remote access of the video through a web-enabled environment for both live and recorded videos. Enterprise AV automates the complete backup process for digital video recordings and provides flexible and secure access for students, faculty, or other users through an integrated streaming server.

2.3. Architecture

The distributed architecture of the solution appears below:



Enterprise IT Architecture

The Enterprise IT components include:

1. **Web Server (IIS)** – This server will host the Enterprise website (also referred to as IIS server).
2. **Streaming Server** – This server hosts the video streaming application. For a typical installation the streaming server application is hosted on the Web Server. EMS design engineers will propose a separate server only if required based on client needs and requirements.
3. **Database Server (SQL)** – This server will host the application database (also referred to as SQL server).

4. **Enterprise AV Master Server** – The Enterprise AV Master Server manages all network-based servers for Enterprise AV. The server is required for Enterprise AV and controls all communications within the application solutions.
5. **Offline Server** – This server manages emails, maintenance, user sync and inventory updates.
6. **Recording Devices (DVRs/NVRs)** – These servers host the video recording and provide the secondary storage of the video recordings. The quantity is determined by the scope of the project as designed by EMS design engineers.
7. **DVCS** – These windows-based servers provide the transcoding and primary video storage for the video recordings. The transcoding of the video allows the video to be available for multiple bandwidth streams for playback over the network and the web.
8. **Streaming Server** (ESS) – This server provides cross-browser support for low-latency live streaming of audio and video from the recording devices over the network.
9. **Control Station** – This desktop hosts the Enterprise AV Control Station application. An EMS-provided PC (optional) is located in the central control room for center-wide management. Multiple control stations are sometimes proposed as determined by the scope of the project.
10. **Viewer/Debrief Station(s)** – These desktops/laptops host the Enterprise AV Viewer and AV Debrief application. Multiple stations are sometimes proposed as determined by the scope of the project.
11. **SIM Client** – This is an Enterprise AV Simulator interface application that is installed on the simulator control workstations and allows automated connectivity for information transfer between simulators and the Enterprise AV system. Please note the extent of this information access and sharing depends on the interface protocol defined by the simulator manufacturer.
12. **SP Room Stations*** – These desktops/laptops are provided in Clinical Patient rooms for patients to complete their learner evaluations. Multiple stations are proposed as determined by the scope of the project.
13. **Student Post Encounter Stations* –** These desktops/laptops are provided outside clinical patient rooms for learners to complete their patient evaluation. Multiple stations are proposed as determined by the scope of the project.
14. **Faculty/Office Stations*** – These stations are client users who can access the Enterprise website using their computer workstations.
15. **Web Viewer Stations*** – These stations are client users who can access the Enterprise website using their computer workstations.
16. **Video Display Panel** – This application enables the Control Room operator to monitor all camera views on a large display (screen size ranges from 22” to 42”). Please note that this functionality can also be made available using a multiplexer or racks of 4” Video Monitors.
17. **AV Hardware Controller** – This is an external AV controller from Crestron, AMX, etc., that allows control of AV hardware, including cameras, matrix switchers, audio DSP, etc., using IP protocols. The solution is part of Enterprise AV and the quantity of these units is based on the solution requirements – number of rooms, cameras etc.
18. **SimCheckIN™ app** – This product is part of the Companion Apps for the SIMULATIONiQ Platform. SimCheckIN app is a tablet-based participant check-in system that captures data though customized workflows to help you analyze center utilization and accurately track simulation and clinical skills session attendance. SimCheckIN can be integrated with SIMULATIONiQ™ Enterprise and a badge scanner option is available to enable learners, educators, standardized patients, and visitors to check in at your facility and register for available sessions quickly and efficiently. *Please contact your EMS Customer Success Manager for more information.*

19. **SimINVENTORY™ app** – This product is part of the Companion Apps for the SIMULATIONiQ Platform. SimINVENTORY is a mobile app for iOS and Android to manage inventory using barcodes within SIMULATIONiQ™ Enterprise. The SimINVENTORY app also allows inventory to be assigned to events and rooms. *Please contact your EMS Customer Success Manager for more information.*
20. **DashboardKPI™** – This product is part of the Companion Apps for the SIMULATIONiQ Platform. DashboardKPI is a web-based system to monitor SIMULATIONiQ™ Enterprise and AV usage trends and provides a variety of charts using key performance indicators. *Please contact your EMS Customer Success Manager for more information.*
21. **VideoCAPTURE** – This product is part of the Companion Apps for the SIMULATIONiQ Platform. VideoCAPTURE is a mobile app for iOS and Android to record, playback, bookmark, and annotate videos. Recorded videos are automatically uploaded to SIMULATIONiQ Enterprise for video management within cases, scenarios, and sessions. *Please contact your EMS Customer Success Manager for more information.*

*** EMS no longer supports the Windows XP operating system.**

*** EMS supports Microsoft Office 2007 and above**

Additional AV and IT-related hardware items may be required based on the unique design needs of the user. A few examples include UPS battery support, video teleconferencing, data backup solutions, etc.

2.4. Hardware Requirements

A Gigabit network is required to support all servers and workstations that are part of the SIMULATIONiQ Enterprise solution, including all switches that are part of the infrastructure supporting the SIMULATIONiQ Enterprise solution.

1. **Web Server (IIS) Minimum Requirements**
   - Dual Processor: Ten-Core Intel® Xeon® 2.20 GHz E5-2630 25 MB Cache (2 x ten-core)
   - Motherboard should be similar or better than Intel C612 Chipeset
   - Memory: 32 GB rated at PC4-19200 and minimum 2400 MHz
   - Chassis: Thinkmate RAX-1304-SH 1U Chassis w/ 4x Hot-Swap 3.5” SATA/SAS3 and 400W Redundant Power
   - Slim SATA DVD-RW
   - 4-Port SATA PCI-E Raid Controller
   - Boot Hard Drive 1 X 1 TB SSD SATA 6.0 Gb/s Solid State Drive
   - Operating System: Windows Server 2012 R2 64-bit mode
   - Hard Drive 4 x 2 TB Serial ATA 7200 RPM
   - RAID Level RAID 5
   - Network Controller: Dual Port Gigabit Ethernet

***Note*:** The server will be connected with a KVM for access. It is recommended that the server be hosted in a datacenter with redundant or backup power, redundant data communications and environmental controls. EMS only supports fail-over clustering mode and not load-balancing for the IIS web server.

2. **Database Server (SQL) Specifications:**
   - Dual Processor: Ten-Core Intel® Xeon® 2.20 GHz E5-2630 25 MB Cache (2 x ten-core)
   - Motherboard should be similar or better than Intel C612 Chipeset
   - Memory: 32 GB rated at PC4-19200 and minimum 2400 MHz
   - Chassis: Thinkmate RAX-1304-SH 1U Chassis w/ 4x Hot-Swap 3.5” SATA/SAS3 and 400W Redundant Power
   - Slim SATA DVD-RW
   - 4-Port SATA PCI-E Raid Controller

- Boot Hard Drive 1 X 1 TB SSD SATA 6.0 Gb/s Solid State Drive
- Operating System: Windows Server 2012 R2 64-bit mode
- Hard Drive 4 x 2 TB Serial ATA 7200 RPM
- RAID Level RAID 5
- Network Controller: Dual Port Gigabit Ethernet

***Note*:** The server will be connected with a KVM for access. It is recommended that the server be hosted in a datacenter with redundant or backup power, redundant data communications and environmental controls.

3. **DVCS Servers**
   - Dual Processor: Eight-Core Intel® Xeon® 2.10 GHz E5-2620 20 MB Cache (2 x eight-core)
   - Motherboard should be similar or better than Intel C612 Chipeset
   - Memory: 32 GB rated at PC4-19200 and minimum 2400 MHz
   - Chassis: Thinkmate RAX-1304-SH 1U Chassis w/ 4x Hot-Swap 3.5" SATA/SAS3 and 400W Redundant Power
   - Slim SATA DVD-RW
   - 4-Port SATA PCI-E Raid Controller
   - Boot Hard Drive 512 GB SSD SATA 6.0 Gb/s Solid State Drive
   - Operating System: Windows Server 2012 R2 64-bit mode
   - Hard Drive 4 x 4 TB Serial ATA 7200 RPM
   - RAID Level RAID 5
   - Network Controller: Dual Port Gigabit Ethernet

***Note*:** The server will be connected with a KVM for access. It is recommended that the server be hosted in a datacenter with redundant or backup power, redundant data communications, and environmental controls.

4. **Streaming Server (ESS)**
   This server provides cross-browser support for low-latency live streaming of audio and video from the recording devices over the network. EMS recommends the following minimum hardware specifications for optimal application performance:

   - Quad-Core Processor 3.30GHz 8MB Cache
   - 16GB RAM 2400MHz DDR4 DIMM or higher
   - 960GB Solid State Drive or equivalent
   - Minimum 1GBase-T Ethernet LAN

5. **Control and Debrief Stations**

   IMPORTANT! Control/Debrief stations require dedicated IP addresses and cannot be dynamic. Zones and microphone mapping will be lost if the IP address changes.

   Control Station workstation is the central control for the AV solution. The station provides complete real-time control and monitoring of video preview and recording. The minimum hardware specifications for the workstation are below.

   Debrief Stations host the AV viewer application that allows users to access and playback video recordings. These workstations can be configured for dual monitor setup with the second monitor being a large display panel or projector, thereby allowing group viewing. The minimum hardware specifications for the **desktop/laptop** workstations are:

- Intel® Core™ i7
- 16 GB RAM or higher
- 512 GB SSD for media
- 1000 Mbps Network Interface
- Windows 8.1 Professional Edition (64-bit) or higher
- 19" or bigger LCD monitor with minimum screen resolution support 1280 x 1024
- Video Display Card: MSI NVIDIA® GeForce GT 620 2GB DDR3 (1xDVI, 1xHDMI, 1xVGA) {or equivalent}
- USB Keyboard and Mouse

IMPORTANT! Please note the following limitation on the SIMULATIONiQ™ Enterprise Quartz SP2 release & up:

Applications affected:	AV Control & AV Viewer
Features affected:	Video playback, Edit video & Export Video
Operating Systems:	Windows 10 & Windows 10 Pro
Workaround:	Disable "User Account Control Admin Approval Mode" local security policy

Note: Disabling "User Account Control Admin Approval Mode" may result in some of the apps including Edge browser not working.

6. SP Room Stations

These workstations are placed in the clinical or simulation room and used for user data entry and video review. The participants in the clinical encounters use these stations to evaluate the learner. The stations are required for Enterprise SP and are optional for Enterprise SIM. The minimum hardware specifications for these workstations are:

- Intel® Core™ i5 or higher
- 8 GB RAM or higher
- 500 GB Hard Drive or higher
- 1000 Mbps Network Interface or higher
- Windows 8.1 Professional Edition (64-bit) or higher
- 19" or bigger LCD monitor with minimum screen resolution support 1280 x 1024
- Video Display Card: MSI NVIDIA® GeForce GT 620 2GB DDR3 (1xDVI, 1xHDMI, 1xVGA) {or equivalent}
- USB Keyboard and Mouse

IMPORTANT! For SP workstations using Video Wall on the web, see the Control and Debrief Stations specifications above.

7. Student Encounter Stations

These workstations are placed outside the clinical or simulation room and are used for data entry. The learners in the clinical encounters use these stations to complete their patient evaluation and provide

feedback on the clinical experience. The stations are required for Enterprise SP and are optional for Enterprise SIM. The minimum hardware specifications for these workstations are:

- Intel® Core™ i5 or higher
- 8 GB RAM or higher
- 500 GB Hard Drive or higher
- 1000 Mbps Network Interface or higher
- Windows 8.1 Professional Edition (64-bit) or higher
- 19" or bigger LCD monitor with minimum screen resolution support 1280 x 1024
- Video Display Card: MSI NVIDIA® GeForce GT 620 2GB DDR3 (1xDVI, 1xHDMI, 1xVGA) {or equivalent}
- USB Keyboard and Mouse

IMPORTANT! For Student Encounter Stations using Video Wall on the web, see the Control and Debrief Stations specifications above.

8. Faculty/Office and Web Viewer Stations

These user workstations are used to access the Enterprise website for individual use at office desks and observation stations. EMS does not provide these workstations but recommend the following minimum hardware specifications for optimal application performance.

- Intel® Core™ i7
- 16 GB RAM or higher
- 512 GB SSD for media
- 1000 Mbps Network Interface or higher
- Windows 8.1 Professional Edition (64-bit) or higher
- 19" or bigger LCD monitor with minimum screen resolution support 1280 x 1024
- Video Display Card: MSI NVIDIA® GeForce GT 620 2GB DDR3 (1xDVI, 1xHDMI, 1xVGA) {or equivalent}
- USB Keyboard and Mouse

IMPORTANT! For Faculty/Office and Web Viewer Stations using Video Wall on the web, see the Control and Debrief Stations specifications above.

2.5. Virtual Server Requirements

The Enterprise solution has been tested with the following Virtualization Software solutions:

1. Windows 2012 RC2 64-Bit with Hyper V from Microsoft.
2. VMware ESX Server from VMware Inc.

All virtual servers configured for Database and IIS functionality should comply with the minimum server requirements mentioned above. EMS should be notified in case the client wants to use virtualization software not mentioned in the list.

IMPORTANT! VM resources must be dedicated, not pooled or throttled, and must meet or exceed the minimum server requirements mentioned above.

Database Server (SQL) Specifications:

- Dual Processor: Four-Core Intel® Xeon® 2.20 GHz E5-2620 15 MB Cache (2 x four-core)
- For virtual: 8 CPUs
- Motherboard - Intel C602 Chipset - Dual Intel Gigabit Ethernet - 8x SATA
- Memory - 16 GB rated at PC4-17000 and minimum 2133 MHz
- 1U Chassis - 4x Hot-Swap 3.5" SATA/SAS - 700W Redundant Power
- Boot Hard Drive - 1 TB Intel DC S3500 Series 2.5" SATA 6.0Gb/s Solid State Drive (7mm)
- (MLC)
- 4 x 1.2TB SATA 6.0Gb/s 10000RPM - 3.5" - Seagate Constellation ES.3
- RAID Level RAID 5
- Slim 8x DVD-RW / 24x CDR Combo (SATA)
- LSI MegaRAID 9341-4i SAS 12Gb/s 4-Port Controller
- Operating System: Windows Server 2008 R2 - 64-bit mode
- SQL 2012 and SQL 2014 Standard Edition with 100 CALs – based on number of users
- Network Controller: Dual Port Gigabit Ethernet

Web Server (IIS) Minimum Requirements

- Four-Core Intel® Xeon® (2 x four-core)
- For virtual: 8 CPUs
- Memory: 12 GB
- Slim SATA DVD-RW
- 4-Port SATA PCI-E Raid Controller
- Boot Hard Drive 1 X 512 GB SSD SATA 6.0 Gb/s Solid State Drive
- Operating System: Windows Server 2008 R2 64-bit mode
- Hard Drive 4 x 1.2 TB Serial ATA 7200 RPM
- RAID Level RAID 5
- Network Controller: Dual Port Gigabit Ethernet

DVCS Specifications:

- Dual Processor: Four-Core Intel® Xeon® 2.40 GHz E5-2620 15 MB Cache (2 x four-core)
- For virtual: 8 CPUs
- Motherboard should be similar or better than Intel C612 Chipset
- Memory: 16 GB rated at PC4-17000 and minimum 2133 MHz
- Chassis: Equivalent of 1 RU Super micro SC825TQ-R760LPB with 700W 1+1 hot-swap
- redundant PFC (Black)
- Slim SATA DVD-RW
- 4-Port SATA PCI-E Raid Controller
- Boot Hard Drive 1 TB SSD SATA 6.0 Gb/s Solid State Drive
- Operating System: Windows Server 2008 R2 64-bit mode
- Hard Drive 4 x 3 TB Serial ATA 7200 RPM
- RAID Level RAID 5
- Network Controller: Dual Port Gigabit Ethernet

Streaming Server (ESS)

- Quad-Core Processor 3.30GHz 8MB Cache
- 16GB RAM 2400MHz DDR4 DIMM or higher
- 960GB Solid State Drive or equivalent
- Minimum 1GBase-T Ethernet LAN

IMPORTANT! The entire system must have a 1Gbps network connection from end-to-end.

2.6. Optional Server Configurations

2.6.1. Blade Server Requirements

The Enterprise solution is hosted in servers located at client datacenters or simulation center server rooms. All hardware is mounted in industry-standard server racks. The needs for Database and IIS server can be accomplished by using blade servers that meet the minimum server requirements for the application. Please refer to the minimum server requirements in the **Hardware Requirements** section on page 9 to configure and confirm blade server configuration.

2.6.2. Clustering Requirements

The Enterprise solution does not require any special cluster configuration for its operating needs. The final configurations is driven by the client IT infrastructure support policy. EMS recommends that all such configurations be verified by EMS before the servers are configured by the client. EMS only supports fail-over clustering mode and not load-balancing for the IIS web server.

3. IP Network Specifications

This section describes the needs and requirements for the network to be available and configured for optimal performance of the application. The Enterprise solution is configured under the user LAN and requires a minimum 1000BASE-T network. The specific needs and considerations for the network are detailed in the following sub-sections.

3.1. Domain Name Space

The Enterprise solution requires the computers and IP hardware to be placed in a domain to allow secured communications and data transfer required by the application. Also, user access to the system can be made secure and available throughout the network. Using a domain name space allows seamless video storage and streaming over the network. Please note that the web application is not dependent on this. The solution is configured within the user domain and if not present, EMS will create its own domain within the system.

3.2. Service Account

The Enterprise solution provides security for information access by using a domain user credentials to communicate and complete user requests for data and video access. **IMPORTANT!** The client must provide EMS with a Windows Service account for system configuration, which does not have any password expiration and is not part of any user domain policy. This information is provided by the client as part of the IT planning phase of the project and documented in the project documents.

3.3. Network Connectivity

All IP-enabled components included in Enterprise require network connectivity using industry standard RJ-45 Ethernet connectors. The network cabling should at least meet Cat 5e specification. EMS recommends Cat 6 cabling for new and remodeled labs.

For user workstations, the network connectivity can be both wired as well as wireless (minimum IEEE 802.11n). EMS recommends wired connectivity on most frequently used workstations for video viewing.

3.4. Network Type

The Enterprise solution requires a LAN that is open for access (network space) within the limits of its component. All access to the system is validated against user-authentication and network security placed and configured on the user network. The solution can be configured under a VLAN (Virtual Private LAN) as desired by the user; however, it is not recommended as access to the information will be restricted within the VLAN.

3.5. Network Security

The Enterprise solution is based on message communications between its components, the network security needs to be configured with respect to Firewall and Transport Layer Security (also referred to as SSL). The Enterprise solution requires specific ports to be opened for its components.

Also, all Enterprise applications installed on the workstation need to be included in the firewall exception list to ensure proper functioning of the system.

Enterprise web services can be configured for TLS security. The TLS security certificate is required and needs to be supplied by the user. EMS will configure the system with the supplied certificate. This information is gathered during the project design process in consultation between EMS and the client.

EMS recommends that systems have anti-malware software (Virus, SPAM protection) installed on all computers. Because each client may have different local IT policies requiring different anti-malware software, EMS does not provide this software unless specifically requested to do so. In addition, the client is required to install all Microsoft Windows updates and patches as soon as possible without impacting the operational needs for the system.

With Windows 2012 servers, there is a host-based firewall that is built-in with the operating systems. This "Windows Firewall with Advanced Security" is configured by EMS during system implementation to allow secured access to data and applications.

EMS Port Exception Listing by Device				
Device/Port Name	**Port**	**Protocol**	**Direction**	**Internal/External**
External Firewall				
HTTP	80	TCP	In/Out	Internal/External
HTTPS	443	TCP	In/Out	Internal/External
HIK Live Enterprise AV Streaming Server	554, 556, 557, 558	TCP/UDP	In/Out	Internal/External
Media Server Ports	1755	TCP/UDP	In/Out	Internal/External
Video Streaming	1935	TCP	In/Out	Internal/External
HTTP Streaming	2323	TCP	In/Out	Internal/External
Remote Desktop	3389	TCP	In/Out	Internal (see note 1)
MMS - Everywhere	1024-5000	UDP	OUT	Internal/External
HIK Live Streaming- Everywhere	10,000-13,000	TCP/UDP	OUT	Internal/External
HIK Live Streaming- Everywhere	50,000-60,000	TCP	OUT	Internal/External
Note 1: If RDP is direct, i.e. no VPN, this port must also be external.				
SQL Server				
HTTP	80	TCP	In/Out	Internal
Networking	137	UDP	In/Out	Internal
Networking	138	UDP	In/Out	Internal
Networking	139	TCP	In/Out	Internal
HTTPS	443	TCP	In/Out	Internal
File Sharing NTFS	445	TCP	In/Out	Internal
SQL with Enterprise Applications	1433	TCP	In/Out	Internal
SQL	1434	UDP	In/Out	Internal
Remote Desktop	3389	TCP	In/Out	Internal
Note 2: If Enterprise AV Server is installed on 2012 Server add 2001, 2004, 2005, 2008 and 3243 to SQL List.				
IIS Server				
HTTP	80	TCP	In/Out	Internal
Networking	137	UDP	In/Out	Internal
Networking	138	UDP	In/Out	Internal
Networking	139	TCP	In/Out	Internal
HTTPS	443	TCP	In/Out	Internal
File Sharing NTFS	445	TCP	In/Out	Internal
HIK Live Enterprise AV Streaming Server	554, 556, 557, 558	TCP	In/Out	Internal
Media Server Ports	1755	TCP/UDP	In/Out	Internal

Video Streaming	1935	TCP	In/Out	Internal
HTTP Streaming	2323	TCP	In/Out	Internal
Remote Desktop	3389	TCP	In/Out	Internal
RTSP	5004	UDP	Out	Internal
RTSP	5005	UDP	In/Out	Internal
MMS	1024-5000	UDP	In/Out	Internal
Crestron Controller Mobile Support	41790 - 41791	TCP	In/Out	Internal
Crestron Controller Support	41794 - 41797	TCP	In/Out	Internal

Note 3: Crestron Control Support ports needed only if using Crestron Controller.

Enterprise AV Server (If installed on separate machine from SQL)				
HTTP	80	TCP	In/Out	Internal
Networking	137	UDP	In/Out	Internal
Networking	138	UDP	In/Out	Internal
Networking	139	TCP	In/Out	Internal
HTTPS	443	TCP	In/Out	Internal
File Sharing NTFS	445	TCP	In/Out	Internal
Enterprise AV Server (Laerdal)	3243	TCP	In/Out	Internal
Remote Desktop	3389	TCP	In/Out	Internal
Digital Video Control Server (DVCS)				
HTTP	80	TCP	In/Out	Internal
Networking	137	UDP	In/Out	Internal
Networking	138	UDP	In/Out	Internal
Networking	139	TCP	In/Out	Internal
HTTPS	443	TCP	In/Out	Internal
File Sharing NTFS	445	TCP	In/Out	Internal
HIK Live Enterprise AV Streaming Server	554, 556, 557, 558	TCP	In/Out	Internal
Remote Desktop	3389	TCP	In/Out	Internal
DVR Communication	5050	TCP	In/Out	Internal
DVR Communication	8000	TCP	In/Out	Internal
DVR Communication	8001	TCP	In/Out	Internal
DVR Communication	8002	TCP	In/Out	Internal
DVR Communication	8080	TCP	In/Out	Internal
Enterprise AV Control Station				
HTTP	80	TCP	In/Out	Internal
Networking	137	UDP	In/Out	Internal
Networking	138	UDP	In/Out	Internal
Networking	139	TCP	In/Out	Internal
HTTPS	443	TCP	In/Out	Internal

File Sharing NTFS	445	TCP	In/Out	Internal
Remote Desktop	3389	TCP	In/Out	Internal
Crestron Controller Mobile Support	41790 - 41791	TCP	In/Out	Internal
Crestron Controller Support	41794 - 41797	TCP	In/Out	Internal
Note 3: Crestron Control Support ports needed only if using Crestron Controller.				
Viewing Station				
HTTP	80	TCP	In/Out	Internal
Networking	137	UDP	In/Out	Internal
Networking	138	UDP	In/Out	Internal
Networking	139	TCP	In/Out	Internal
HTTPS	443	TCP	In/Out	Internal
File Sharing NTFS	445	TCP	In/Out	Internal
Remote Desktop	3389	TCP	In/Out	Internal
Crestron Controller Mobile Support	41790 - 41791	TCP	In/Out	Internal
Crestron Controller Support	41794 - 41797	TCP	In/Out	Internal
Note 3: Crestron Control Support ports needed only if using Crestron Controller.				
Observation Station				
HTTP	80	TCP	In/Out	Internal
Networking	137	UDP	In/Out	Internal
Networking	138	UDP	In/Out	Internal
Networking	139	TCP	In/Out	Internal
HTTPS	443	TCP	In/Out	Internal
File Sharing NTFS	445	TCP	In/Out	Internal
Media Server Ports	1755	TCP/UDP	In/Out	Internal
HTTP Streaming	2323	TCP	In/Out	Internal
Remote Desktop	3389	TCP	In/Out	Internal
DVR Communication	8000	TCP	In/Out	Internal
DVR Communication	8001	TCP	In/Out	Internal
DVR Communication	8002	TCP	In/Out	Internal
DVR Communication	8080	TCP	In/Out	Internal
Crestron Controller				
Crestron Controller Mobile Support	41790 - 41791	TCP	In/Out	Internal
Crestron Controller Support	41794 - 41797	TCP	In/Out	Internal
Note 3: Crestron Control Support ports needed only if using Crestron Controller.				
Pre or Post Encounter Workstation				
HTTP	80	TCP	In/Out	Internal
Networking	137	UDP	In/Out	Internal

Networking	138	UDP	In/Out	Internal
Networking	139	TCP	In/Out	Internal
HTTPS	443	TCP	In/Out	Internal
File Sharing NTFS	445	TCP	In/Out	Internal
Media Server Ports	1755	TCP/UDP	In/Out	Internal
HTTP Streaming	2323	TCP	In/Out	Internal
Remote Desktop	3389	TCP	In/Out	Internal
DVR Communication	8000	TCP	In/Out	Internal
DVR Communication	8001	TCP	In/Out	Internal
DVR Communication	8002	TCP	In/Out	Internal
DVR Communication	8080	TCP	In/Out	Internal

3.6. Network File Share

The Enterprise solution uses windows network file share to allow the application to access files and video recordings. The system is configured by EMS to allow full file access to network video shares using a secured user domain account provided by the client. The user-based file sharing provides full security to the information saved in the file shares. Please refer to section **3.1-Domain Name Space** on page 15 for details.

4. Web Application Requirements

4.1. Website Address

By default, the application website uses the computer name and/or the IP address of the web server for the URL web address. The client can add the user-friendly web address (this must be supplied to EMS) as hyperlink to their parent website or via any other website as required. If desired, domain name can be assigned to the application website.

4.2. Web Browser Compatibility

EMS web application is tested and verified for the following versions of the computer operating systems and internet browser:

- Internet Explorer 11.0
- Microsoft Edge 44 or higher
- Google Chrome 83 or higher
- Firefox 78 or higher
- Safari 13.0 or higher is the supported and recommended browser for Mac OS

Note: EMS continues to test its application against the commonly used browsers. Release Notes are provided with the software updates.

Enterprise offers high level user functions via the web and some of these functions can be blocked by the default settings of the Internet browsers.

Additional Plugins and Browser Requirements:

- Active X *(Required for live view in Internet Explorer)*
- SIMULATIONiQ Enterprise site must be listed as a "trusted site"

A dedicated streaming server can be used for optimal performance of the Enterprise application as a high-performance streaming media to computers and mobile devices.

4.3. Network Access

Access to the application website is based on the network access configured by the client IT group. Usually the user will have access to the website within the network. If the user needs offsite access to the website (from home or off-campus), the client IT group has to enable that access.

5. Infrastructure Requirements

5.2. Anti-Virus/Malware/Spyware Protection

Enterprise systems should have anti-malware software (Virus, SPAM protection) installed on all computers. By default, these third-party software applications are not included in the system as each client will have different local IT policies requiring different anti-malware software. The EMS installation team will provide assistance to install and configure the software on the Enterprise system. EMS does not provide this software, but you can request it from EMS for an additional charge. In addition, you are required to install all Microsoft Windows updates and patches as soon as possible without impacting the operational needs for the system.

5.3. Power Requirements

The Enterprise solution is based on the US electrical power standard. All PC workstations and user equipment requires standard 110-volt 60 cycle electrical receptacles (15 Amp minimum).

5.4. Server Room

The Enterprise solution provides server racks that are specifically designed to the needs of the client. The project manager assigned by EMS will furnish the exact power requirements based on the proposed solution design. EMS does not provide installation services for power circuits and will require clients to provide the power receptacles as requested by EMS.

5.5. Network Requirements

EMS solution is based on Ethernet and Wi-Fi network communications. All user access to the application is via network connected workstations and laptops. The access to the network, either via wall plates in the room or wireless access points in the center, needs to be installed and provided by the user.

6. User Access Requirements

6.2. User Authentication

Available authentication methods:

- EMS
- Active Directory (The minimum version required for Microsoft Active Directory is Windows 2000.)
- LDAP
- eDirectory
- Single Sign-On

Upon successful installation, users can access the SIMULATIONiQ Enterprise solution using the client application or website. All users are authenticated against a user-directory for access and role-permission to use the application. Users can be configured to multiple authentication methods.

To configure authentication using Active Directory, LDAP, eDirectory, or Single Sign On, the SIMULATIONiQ Enterprise solution needs the following information:

- Host Server Name
- Configured Port
- Login Username or DN
- Password
- user search DN
- Filter

6.2.1. EMS

The system provides built-in authentication services, where the username and passwords are encrypted and stored within the application database. The system administrator manages the list. The system allows the system administrator to bulk-upload the user list using Excel spreadsheets with specific format that include the following types of information:

Learner ID, **First name**, MI, **Last name**, **User name**, **Primary Email**, Gender, **Password**, Address 1, Address 2, City, State, Zip, Country, Day Phone, Evening Phone, Cell, Pager, Fax, Grad year, MCAT score, Undergrad GPA, AccessCard ID, Secondary Email, Supervisor Email, Employer, Occupation

Only First name, Last Name, User name, Primary Email, and Password are required for each user type. The remaining fields are optional. One spreadsheet should be generated for each defined user role, such as Educator, SP, and Learner.

6.2.2. Active Directory Integration

EMS will require an account and server access to periodically poll the Active Directory (AD). The interval for the import process can be customized based on client needs. The SIMULATIONiQ Enterprise solution permits multiple configurations to import users from different location user groups into user types like Educator, SP, and Learner.

The SIMULATIONiQ Enterprise solution can import users from specific locations to assign certain roles and privileges in the system. EMS highly recommends the user create one or more security groups to identify which users within the AD are assigned their given roles. EMS recommends identifying separate security groups for each defined user role, such as Educator, SP, and Learner. As an example, all the users from a base search (ou=people, dc=microsoft, dc=edu) can be imported as “Educator” to automatically assign specific privileges within the application. Active directory field names including givenname, initials, sn, samaccountname, mail, are mapped to SIMULATIONiQ Enterprise user fields.

Another option is to designate one security group for all users to be imported. The user roles can then be assigned by the SIMULATIONiQ Enterprise administrator separately.

Note: The SIMULATIONiQ Enterprise solution under AD does not store any passwords. All user password change requests are handled by the Directory Services group.

6.2.3. LDAP Integration

The SIMULATIONiQ Enterprise solution also integrates with the client's LDAP (Light Directory Access Protocol) for user authentication. EMS will require an account and server access to periodically poll the LDAP. The interval for the import process can be customized based on client needs. The SIMULATIONiQ Enterprise solution permits multiple configurations to import users from different location user groups into user types like Educator, SP, and Learner.

The SIMULATIONiQ Enterprise solution can import users from specific locations to assign certain roles and privileges in the system. EMS highly recommends the user create one or more security groups to identify which users within the LDAP are assigned their given roles. EMS recommends identifying separate security groups for each defined user role, such as Educator, SP, and Learner.

Another option is to designate one security group for all users to be imported. The user roles can then be assigned by the SIMULATIONiQ Enterprise administrator separately.

Note: The SIMULATIONiQ Enterprise solution under LDAP does not store any passwords. All user password change requests are handled by the Directory Services group.

6.2.4. eDirectory Integration

The SIMULATIONiQ Enterprise solution also integrates with the client's eDirectory for user authentication. EMS will require an account and server access to periodically poll the eDirectory. The interval for the import process can be customized based on client needs. The SIMULATIONiQ Enterprise solution permits multiple configurations to import users from different location user groups into user types like Educator, SP, and Learner.

The SIMULATIONiQ Enterprise solution can import users from specific locations to assign certain roles and privileges in the system. EMS highly recommends the user create one or more security groups to identify which users within the eDirectory are assigned their given roles. EMS recommends identifying separate security groups for each defined user role, such as Educator, SP, and Learner.

Another option is to designate one security group for all users to be imported. The user roles can then be assigned by the SIMULATIONiQ Enterprise administrator separately.

Note: The SIMULATIONiQ Enterprise solution under eDirectory does not store any passwords. All user password change requests are handled by the Directory Services group.

6.2.5. Single Sign On Integration

The SIMULATIONiQ Enterprise solution also integrates with the client's Single Sign On (SSO) server for user authentication. EMS will require an account and server access to periodically poll the SSO. The interval for the import process can be customized based on client needs. The SIMULATIONiQ Enterprise solution permits multiple configurations to import users from different location user groups into user types like Educator, SP, and Learner.

The SIMULATIONiQ Enterprise solution can import users from specific locations to assign certain roles and privileges in the system. EMS highly recommends the user create one or more security groups to identify which users within the SSO are assigned their given roles. EMS recommends identifying separate security groups for each defined user role, such as Educator, SP, and Learner.

Another option is to designate one security group for all users to be imported. The user roles can then be assigned by the SIMULATIONiQ Enterprise administrator separately.

Note: The SIMULATIONiQ Enterprise solution under SSO does not store any passwords. All user password change requests are handled by the Directory Services group.

7. Maintenance and Support

7.2. Remote Support

To provide high level customer support, EMS requires that the client provide remote access to the system. The remote access can be limited to the database and IIS servers. The access protocol/options are based on local IT policies of the client and need to be validated with EMS IT for compliance. The remote access can be via VPN, RDP, VNC, etc. All access, if configured by EMS, is password protected and initially the client is informed before any EMS personnel connect to the system.

7.3. Software Updates

As part of system support and maintenance, EMS provides all system updates and patches for Enterprise through a software update policy. The updates are done by the EMS Customer Support team in consultation with the end-user.

7.4. Computer Updates

All Microsoft Windows-based computers and servers installed at the client site are considered part of the client standard IT policies for updates and patches. The client is responsible for maintaining these machines with all updates and patches. EMS will inform the client only in case a particular patch or update has an adverse effect on the system performance. All other IP-based hardware provided by EMS is managed and maintained by EMS, and all updates required are completed during the software update process.

7.5. Backup and Restore

Enterprise does not include any backup solution. The client is expected to provide information on their backup procedures and policy. EMS will assist in configuration of the system to comply with the local policies. The list of items to be included in the backup plan is:

- Database Backup – full or incremental
- Website backup – include multimedia library
- Video Files – DVCS and any external NAS/SAN

7.6. Video Archiving

The Enterprise solution provides video file administration using client application to manage video files. By default, the system will inform the Support Administrator daily (via monitoring alerts on Enterprise AV Manager) when the available space for video storage falls below 100 hours. At this time, the administrator can delete video files or archive them (for continuing online access) at other storage locations (external NAS or SAN). The system will overwrite the files that are not archived (starting with the oldest recordings) on the application storage server.

7.7. System Monitoring

The Enterprise solution provides real-time system monitoring from the client application – Enterprise AV Manager. In Enterprise AV Control, an Enterprise user can click the System Monitor button at the top of the page to perform a health-check on the system as well as reset the system as required. EMS also offers real-time remote server and network monitoring for its TotalCAREiQ™ Gold and Platinum clients. The system is configured to notify and alert the EMS Customer Support team with any server and network problem. This monitoring service involves using probes (with sensors) installed on the servers to monitor server performance. The probes will communicate with the EMS centralized monitor server to provide regular health check updates. Any alerts from the probe will be received by the EMS Customer Support team, who can then proactively work with you and your IT staff to ensure adequate steps are taken to avoid adverse conditions and prevent problems before they become chronic and result in environment downtime.

8. System Configurations

8.2. Email Support

The Enterprise solution can be configured to send out automated emails—using built-in or user-defined email templates—to users for calendar scheduling, task assignments and reminders. The Enterprise Administrator can also create email templates as desired.

The system needs to be configured with the SMTP/POP3 server information and a user account (if not the domain system account). This information is provided by the client as part of the IT planning phase of the project and documented in the project documents.

8.3. System Account

As referenced in **Section 3.1 - Domain Name Space** on page 15, the solution requires a domain account that is used by the system to communicate and transfer files between different computers. The account is configured with administrator rights on the EMS systems and is used to impersonate file access for any user request. **IMPORTANT!** If an account is not specified, none of the AV functions will work as desired.

9. Third-Party Integration Requirements

9.2. AV Controller

EMS uses industry standard Audio-Video Control systems from Crestron Electronics Inc. (www.crestron.com) and AMX LLC (www.amx.com) to provide reliable communication and control between applications and AV hardware. The control systems are IP enabled and thus require network access. **Static IP** addresses are required for these devices and are requested by EMS project manager at the time of project design and documentation.

9.3. Simulator Integration

The Enterprise solution interfaces with all commonly used medical simulators (e.g. Laerdal, Gaumard, CAE and Simulaids) as well as with medical task trainers. These interfaces depend on the feature/functions available on the simulators. In order to provide seamless automation to these interfaces, the simulator's instructor and/or vital monitor computer needs to be part of the same network as EMS solutions. **IMPORTANT!** Simulators may be on a different VLAN or Subnet but must on the same network. This also includes any telemetry display system used with the simulator. **Static IP addresses are required** for these devices and are requested by the EMS project manager at the time of project design and documentation.

9.4. Simulator Instructor Laptop Specifications

- Intel® i5
- 8 GB RAM
- 250 GB Hard Drive
- Minimum 802.11g Wireless Network Card
- Windows 7 Professional or higher
- 17" or higher screen size