OnSite™

for the *da Vinci*® Surgical System

Overview

Table of Contents

1. *OnSite™* for the *da Vinci* System Overview

Indications for Use

OnSite™ is an accessory indicated for use by trained Intuitive Surgical Field Service personnel to: (1) obtain system information for the purpose of diagnosing faults, (2) remotely enable/disable features including configuration updates through either a wired or wireless Ethernet connection between the da Vinci Surgical System and the hospital's Internet Protocol (IP) infrastructure

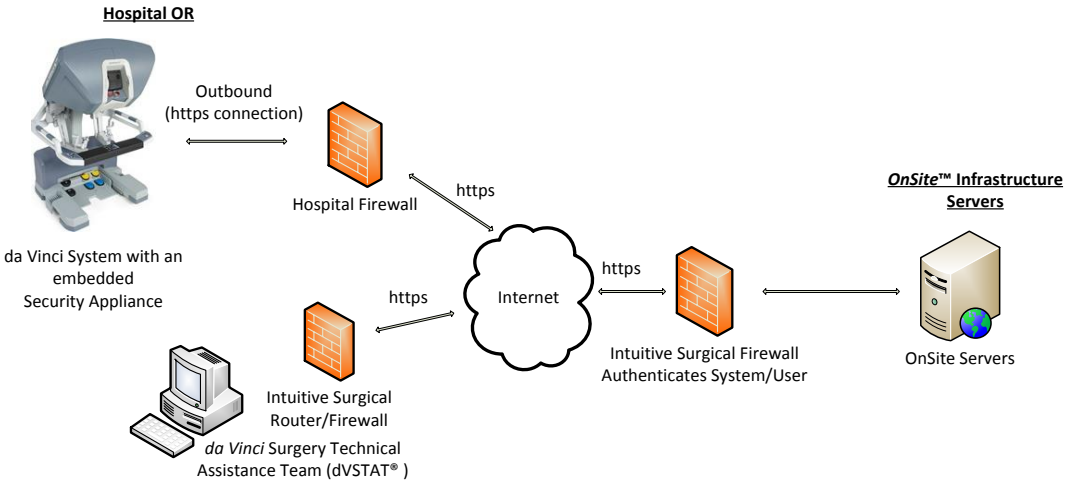
Introduction

OnSite provides connectivity that enables Intuitive Surgical service personnel to remotely service the da Vinci Surgical System pre-operatively and intra-operatively. It enables the following capabilities.

1. Automated log retrieval, when idle the da Vinci Surgical System uploads logs to an Intuitive Surgical server
2. Remote system status monitoring
3. Remote diagnostics and servicing
4. Remote configuration changes
5. Enable/disable features

To implement OnSite remote service capabilities, the da Vinci Surgical System must have access to the Internet. *OnSite* is designed to accomplish this using existing hospital networks.

OnSite™ Network Diagram



Network Diagram Components

- ***da Vinci* System** – *da Vinci S™ or newer* system.
  - Operating Systems
    - *da Vinci* Si™ and Xi™: QNX real-time operating system
    - *da Vinci S*: RTOS for embedded processors
- ***da Vinci Security Appliance*** – Dell Sonicwall security appliance (embedded inside the *da Vinci* System).
- ***da Vinci* Wireless Bridge* -** Wireless Bridge installed inside the *da Vinci*
- **Hospital Firewall –** assumed to be present as *da Vinci* System is typically deployed to the hospital Local Area Network. Outbound TLS (TCP:443) to the OnSite Server infrastructure is required.
- **Internet –** *OnSite*™ works over the hospitals existing Internet connection, and does not require a VPN connection.
- **Intuitive Surgical *da Vinci* Surgery Technical Assistance Team –** Technical Support Engineer who provides intra-operative technical assistance and can initiate a remote troubleshooting session with the customer's system.
- ***OnSite* Server Infrastructure –** the infrastructure that supports *OnSite*™ and brokers communication between *dVSTAT* and the *da Vinci* System.

** See Appendix 2 for Optional Wireless Network Diagram*

2. Requirements

Power Requirements
No additional power is required for *OnSite™*.

Outgoing Internet Access

- HTTPS (TLS) outbound access to dvms-dv.intusurg.com (65.160.57.30) and dvms-dv.davinci-onsite.com (199.87.79.30)
    - Si and newer systems are restricted to use only TLS (1.2) cryptographic protocols. *da Vinci* S systems can communicate using both SSL 3.0 and TLS protocols.
    - All communication is initiated by the *da Vinci* so there is no inbound firewall requirements

Bandwidth Usage

- Status packets - ~ 2Kb every 10 seconds
- Log uploads – typically log sizes range from 1Kb to 100Kb but may burst to 1000Kb every 15 to 30 minutes based on system configuration and usage.
- Remote Access – typical usage when connected is ~ 100Kb/s - 500Kb/s

Wired Ethernet
The *da Vinci™* System requires a 10/100/1000bT Ethernet link in OR.

IP Addressing
IPv4 DHCP and static addressing are supported provided the *da Vinci's* assigned IP and or gateway are not within 10.0.0.0/24 range. IPv6 is currently not supported.

Proxies
Simple HTTP Proxies, with no authentication, or simple (plaintext) authentication are supported. SSL Inspection Proxies (Blue Coat, etc.) are not currently supported.

Optional Wireless
OnSite can also support IEEE 802.11 wireless standards using either 802.11B, G and N by means of an optional wireless upgrade. Wireless communication is facilitated by installing a wireless bridge in the *da Vinci* System vision cart which acts as a client to the hospital Wireless Access Point transmitting data back and forth between the hospital network and the *OnSite* enabled *da Vinci* System.

Wireless Connectivity Requirements:

- Wireless Access Point located within 75 feet of the *da Vinci* System
- Maximum latency of 50 ms between the Wireless Bridge and the hospital supplied Wireless Access Point
- Wireless Channel that has 20% or less utilization

Overall Network Requirements

- Maximum end-to-end packet loss of less than 10%
- Network latency should not exceed 300 ms

Note: Once OnSite™ is *successfully installed, Intuitive Surgical field service personnel will conduct an end-to-end functional test to ensure that OnSite is functioning as expected.*

Post-installation, Intuitive Surgical recommends that the hospital routinely monitor to ensure that the Wireless Channel does not exceed 20% utilization, and the latency between the Wireless Access Point and the Wireless Bridge does not exceed 50 ms. If either of these exceeds the specified levels, please contact Intuitive Surgical Customer Service. 1 800 876 1310 Option 2, 2

3. Detailed Hardware, Software and Features

***da Vinci®* System**

The *da Vinci* System is configured with off-the-shelf embedded commercial network/security appliance not accessible to the user. This network/security appliance is preconfigured with a template configured to block all inbound ports and NAT enabled. In addition to the security appliance, several Cat5e or greater Ethernet cables are used. The *da Vinci* System also requires a version of embedded software that is configured to support *OnSite* functionality.

OnSite Server Infrastructure

While providing highly secure network communication with user authentication and logging, the OnSite Server infrastructure provides back-end functionality to collect event logs, manage remote connectivity and track status of *OnSite*-equipped *da Vinci* Systems in the field,

Network Infrastructure and Connection

OnSite is designed to be both highly secure and firewall-friendly. The *da Vinci* System communicates with the *OnSite* Server Infrastructure via outgoing HTTPS connection on port 443. The embedded security appliance also communicates with public NTP servers to update the firewall system clock. (On request, NTP can be disabled on this device)

The *da Vinci* System communicates with the *OnSite* server over a secure TLS protocol. Minimum cipher/key requirements include 1024-bit RSA private keys and 128-bit encryption.

The *da Vinci* System is authenticated by the firewall using a pki system certificate; each *da Vinci* System has a unique certificate installed by a *da Vinci* Technical Field Specialist.

The *OnSite™* Server limits remote access through trusted/revoked certificates, Active Directory accounts and group membership.

4. Data Flow Process

Upon startup, the *da Vinci®* System establishes an outgoing TLS connection to the OnSite Server. *OnSite* uses "request-response (https) protocol" that is initiated by the *da Vinci* System.

The *da Vinci* System presents its TLS client certificate to the *OnSite* server and negotiates a TLS encrypted communications session. The TLS session remains active until the *da Vinci* System is powered off or the network connection is no longer available.

If an Intuitive Surgical *da Vinci* Technical Field Specialist is required to retrieve data from the *da Vinci* System a manual connection is established with the *OnSite* server, and a request is initiated to communicate with a specific *da Vinci* System.

a. Requests for data are transmitted from Intuitive Surgical Technical Support Engineer to the *OnSite* server over the encrypted communication channel using a custom communication protocol
b. The *da Vinci* System retrieves the request, confirms that the request is valid, and then retrieves the requested data
    (Any unknown request retrieved from the server will be ignored, after three (3) consecutive unknown requests the *da Vinci* System disables the *da Vinci's* network interface until the system is powered off.)
c. The *da Vinci* System transmits the information to the OnSite server
d. Intuitive Surgical's service application collects the data and presents the results to a Technical Support Engineer.

5. Security and Access Control

Physical Access

Physical access to the *da Vinci* System is controlled by the hospital OR. Physical access to the da Vinci Surgery Technical Assistance Team PC is controlled by Intuitive Surgical. Physical access to the *OnSite* Infrastructure is access is restricted to registered Intuitive Surgical employees and is hosted in a SOC2 compliant data center. Access to the data center requires an issued proximity badge with a photo ID.

Logical (Network) Access
Network access to the *da Vinci®* System is limited to remote diagnostics traffic from the *OnSite™* Server over the existing (outbound) TLS connection originating from the *da Vinci* System in the OR.

Access Control:
The *da Vinci* System configuration contains a unique client certificate to authenticate against the *OnSite* Infrastructure. The hospital's OR or IT department may restrict or disable the outgoing TLS tunnel by their firewall policy, physical link interaction, or by written request to Intuitive Surgical Service Support to disable *OnSite* features.

OnSite Infrastructure access control is restricted to Intuitive Surgical personnel and several layers of access control:

- To access the *OnSite* server a client certificate based on an Active Directory (AD) account is issued to *dVSTAT®* (*da Vinci* Surgery Technical Assistance Team). If a member of the *dVSTAT* team changes roles or leaves the company the certificate is revoked and AD account is disabled.
- The service application that interacts with the *da Vinci* System is password protected and has a security file that expires after a period of time or a controlled number of uses and must be re-activated by Intuitive Surgical Technical Support.

6. Security Patching Strategy

The *da Vinci OnSite* Infrastructure incorporates industry standard IT hardware and software. The infrastructure will be patched regularly following OEM guidelines.

7. Monitoring

The *da Vinci OnSite* Infrastructure Environment is monitored by Intuitive Surgical's Engineering Network Infrastructure & Operations group.

8. Third Party Audits and Certifications

The *da Vinci OnSite* infrastructure has no industry certifications, however as a part of software development life cycle we perform periodic cyber security audits and engage with 3rd party security consultants to perform various levels of security/penetration audits.

9. Security Administration Roles and Responsibilities

All portions of the *OnSite™* Infrastructure are managed by Intuitive Surgical.

10. Antivirus and Malware

All portions of the *da Vinci® OnSite* Infrastructure running Windows based operating systems have Anti-Virus and Anti-Malware installed and are updated regularly.

The *da Vinci* Surgical System operating software is an embedded proprietary RTOS and QNX which does not support any commercially available antivirus and malware software. We further attempt to minimize any potential network threats by placing the *da Vinci* System behind a NAT'ed Sonicwall security appliance that is configured to block all inbound ports.

11. Backup and Recovery

The *OnSite* infrastructure is backed up regularly, Stored Logs on the *da Vinci* system are backed up during preventive maintenance service by a da Vinic Technical Field Specialist.

12. Storage Management

The *da Vinci OnSite* Infrastructure currently utilizes both SAN hardware and physical servers utilizing direct attached storage.

13. Disaster Recovery

OnSite infrastructure hardware will be handled per SLAs with our vendors. The SLA for site localized failures is One (1) business day or less. A complete site failure of the data center will result in extended downtime.

14. Support Requirements

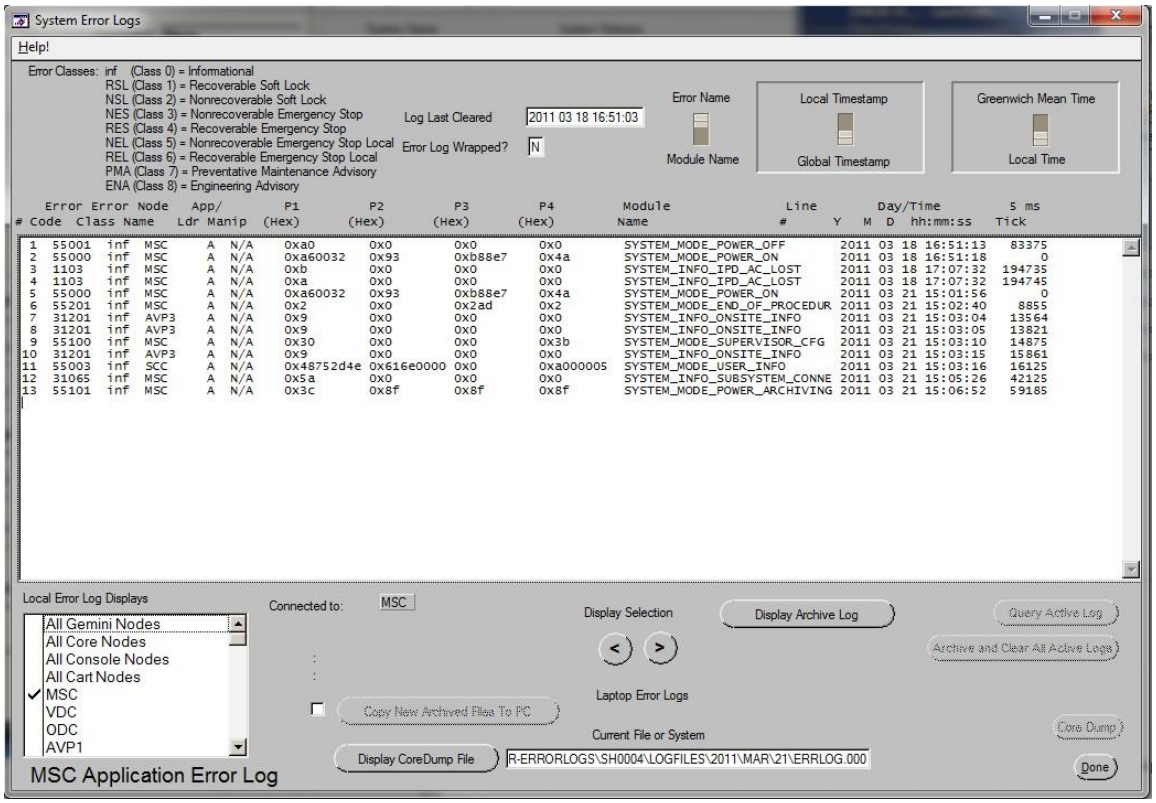
The *OnSite™* installation requires the hospital to provide IP connectivity in the OR, an appropriate bandwidth and necessary network configuration(s) as required for the ports/protocols listed under Section 2 Requirements.

15. Patient Privacy

The *da Vinci™* Surgical System with *OnSite* does not have access to or store any patient health or sensitive data. There is no interface on the *da Vinci* System to enter any ePHI, nor does the system interface with any of the hospital's internal resources' such as HIS, RIS or PACS systems to obtain such information.

Appendix 1 – System Log

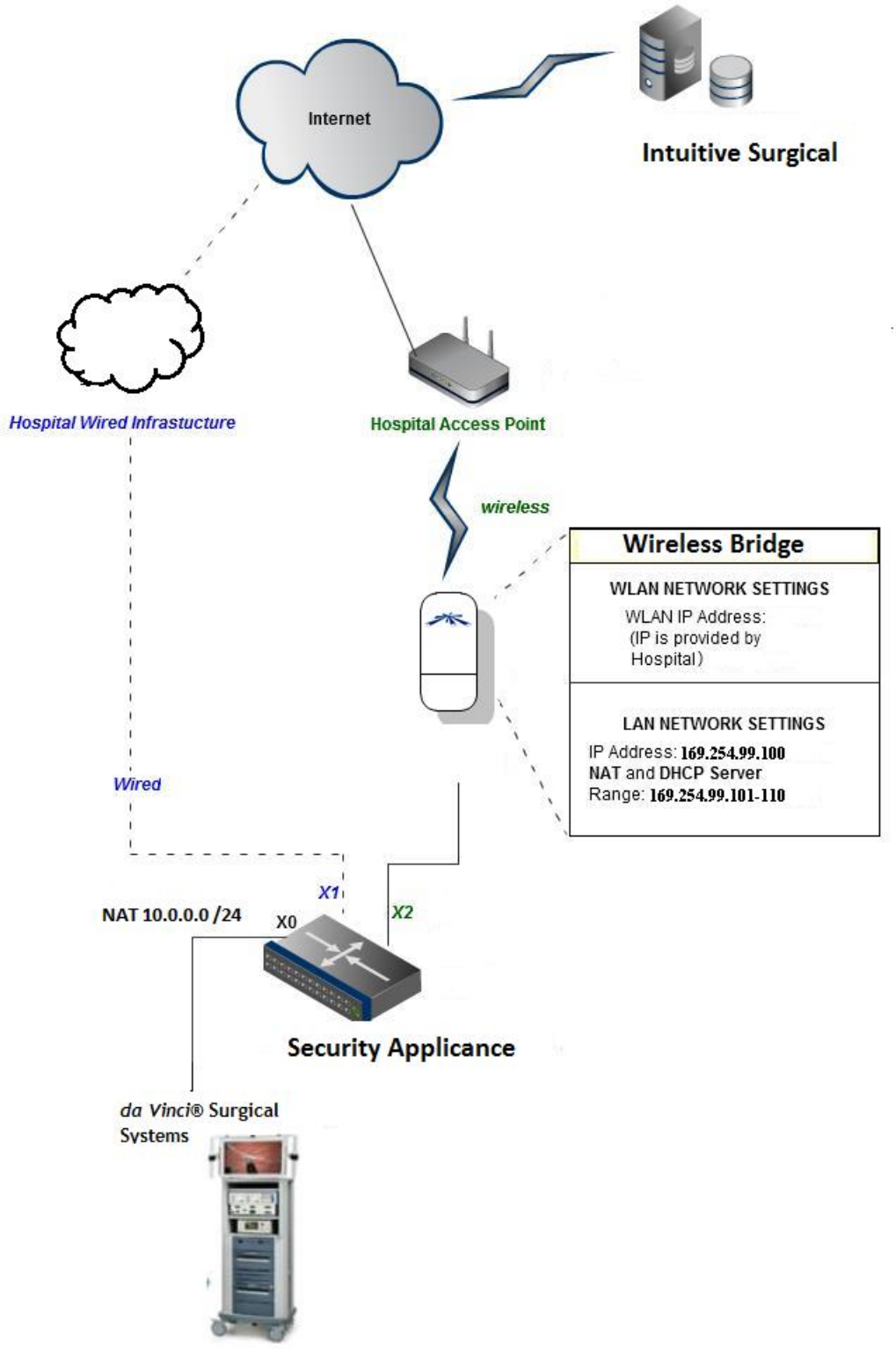
System log files are binary formatted files that contain time stamped system events, instrument and component data, and system/software configuration information. Shown below is a screen capture of a log file parsed using our proprietary service application. Logs do not contain any patient sensitive information.



Appendix 2 – Optional Wireless Connectivity Kit

The wireless bridge is configured to only operate as a wireless supplicant. The bridge supports both 802.11 B, G and N signals. The *da Vinci® OnSite*™ firewall is configured to work with both a wired and wireless connection. If both wired and wireless options are enabled the device is configured to failover to the firewall's X1 (wired) or X2 (wireless) ports using the X1 as a priority when both are showing a valid connection (see below).

Wireless Connectivity Option Network Diagram



Wireless Security

The Wireless Connectivity Option currently supports the following security configurations:

WEP
WPA
WPA – TKIP
WPA – AES
WPA2
WPA2 – TKIP
WPA2 - AES

WEP Authentication: WEP authentication supports either HEX or ASCII character formats.

Open Authentication – station is authenticated automatically by AP (selected by default).
Shared Authentication – station is authenticated after the challenge, generated by AP.

WEP Key:

64-bit** – specify WEP key as 10 HEX (0-9, A-F or a-f) characters (e.g. 00112233AA) or 5 ASCII characters.
128-bit – specify WEP key as 26 HEX (0-9, A-F or a-f) characters (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

WPA Authentication:

PSK – WPA™ or WPA2™ with Pre-shared Key method (selected by default).

WPA Pre-shared Key: The pre-shared key may be entered as a passphrase of 8 to 63 printable ASCII characters.

*Currently 64 character ASCII WPA pre-shared keys and client-side digital certificate or secure smartcard is not supported.