OnSite® Overview

For the da Vinci Surgical System

Table of Contents

1. OnSite for the da Vinci Surgical System Overview

Indications for Use

OnSite is an accessory indicated for use by trained Intuitive 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

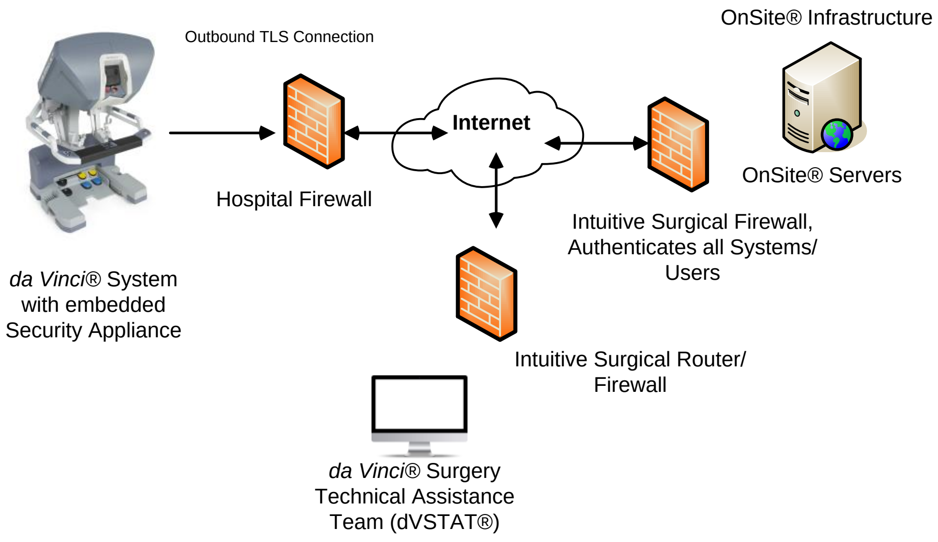
Introduction

OnSite provides connectivity that enables Intuitive service personnel to access the da Vinci Surgical System remotely 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 server
2. Remote system status monitoring
3. Remote diagnostics and servicing
4. Remote configuration changes
5. Enable/disable features
6. Remote software updates (da Vinci X and Xi only)

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

OnSite Network Diagram


OnSite® Infrastructure
Outbound TLS Connection
Internet
Hospital Firewall
OnSite® Servers
Intuitive Surgical Firewall, Authenticates all Systems/ Users
da Vinci® System with embedded Security Appliance
Intuitive Surgical Router/ Firewall
da Vinci® Surgery Technical Assistance Team (dVSTAT®)

Network Diagram Components

- Da Vinci System –
    - Operating Systems
        - da Vinci Si® and da Vinci X®, Xi: QNX real-time operating system
- Da Vinci Security Appliance – Enterprise grade security appliance (embedded inside the da Vinci System).
- Hospital Firewall – is assumed to be present as da Vinci System is typically deployed to the hospital Local Area Network. Outbound TLS (TCP/IP port 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 da Vinci Surgery Technical Assistance Team – Technical Support Engineer who provides pre, intra and post-operative technical assistance.
- OnSite Server Infrastructure - Intuitive infrastructure that supports OnSite.

** See Appendix 2 for Optional Wireless Network Diagram*

2. Requirements

Power Requirements

No additional power is required for OnSite.

Outgoing Internet Access

- (TLS) outbound access to:
  - Da Vinci Si systems- dvms-dv.intusurg.com (65.160.57.30)
  - Da Vinci X, Xi (or newer) systems- dvms-dv.davinci-onsite.com (199.87.79.30)

**Si and newer systems are restricted to use only TLS (1.2) cryptographic protocols.*
**All communication is initiated by the da Vinci system so there is no inbound firewall requirements*

Bandwidth Usage

- Status packets - ~ 4Kb (kilobit) every 10 seconds
- Log uploads – typically log sizes range from 1Kb to 10 MB (Megabytes) per hour based on system configuration and usage.
- Remote Access – typical usage when connected is ~ 1.5 Mb (Megabits) per second

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 system assigned IP and or gateway are not within 10.0.0.0/24 range. IPv6 is not currently supported.

Proxies

Simple HTTP Proxies, with no authentication, or simple (plaintext) authentication are supported. TLS Inspection Proxies (Blue Coat, etc.) are not currently supported and would require whitelisting the appropriate destination IP (based on system type) or alternate network topology to bypass this requirement.

Optional Wireless

OnSite can also support IEEE 802.11 wireless standards using either 802.11B, G, or N using 2.4 GHz frequency 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 the OnSite® connection is successfully installed, Intuitive field service personnel will conduct an end-to-end functional test to ensure that OnSite is functioning as expected.

Post-installation, Intuitive 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 milliseconds (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 (network address translation) 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, proprietary 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 access is designed to be both highly secure and firewall-friendly. The da Vinci System communicates with the OnSite Server Infrastructure via outgoing TLS connection on port 443. The embedded security appliance also communicates with public network time protocol (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 2048-bit RSA private keys and AES 256-bit encryption.

The da Vinci System is authenticated by the firewall using a self-signed Public Key Infrastructure (PKI) system certificate; each da Vinci System has a unique certificate installed by a da Vinci Field Service Engineer. The OnSite Server limits remote access through trusted/revoked certificates, Active Directory accounts and group membership.

4. Data Flow Process

OnSite uses "TLS 1.2 protocol" that is initiated by the da Vinci System.
Upon startup, the da Vinci System establishes an outgoing TLS 1.2 (transport layer security) connection to the OnSite Server.
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 da Vinci Field Service Engineer is required to retrieve data from the da Vinci System, a manual connection is established with the OnSite server. A request is then initiated to communicate with a specific da Vinci System.

a. Requests for data are transmitted from the Intuitive Surgical Technical Support Engineer to the OnSite server over the encrypted communication channel using a custom, proprietary 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. The Intuitive 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. Physical access to the da Vinci Surgery Technical Assistance Team PC is controlled by Intuitive. Physical access to the OnSite

Infrastructure is access is restricted to registered Intuitive employees and is hosted in a SOC2 compliant data center.

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. Intuitive does not initiate any connections into the hospital network.

Remote Access:

The da Vinci System configuration contains a unique client certificate to authenticate against the OnSite Infrastructure. The hospital 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 service support to disable OnSite features.

OnSite Infrastructure access control is restricted to Intuitive 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 proprietary 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.

User System Access:

The da Vinci system, by design, has no user "authentication" capability and does not require a surgeon or member of the OR staff to login to operate the surgical device. It has no ability to join a domain. The da Vinci has no keyboard or mouse, users have no means to access the OS and the device does interface or communicate with any hospital enterprise imaging or patient/record systems.

6. Security Patching Strategy

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

Intuitive technically does not provide da Vinci system patches per se but is responsible for all system software updates. The da Vinci's OS embedded software is updated as per the SLSA (typically 2x annually); however in the event we discover a critical vulnerability that is not mitigated we would address this as an embedded software update without due delay. Software updates are typically communicated and coordinated via the da Vinci coordinator; i.e. the person responsible for the da Vinci at the hospital.

7. Monitoring

The da Vinci OnSite Infrastructure Environment is monitored by the Intuitive Engineering Network Infrastructure & Operations group.

8. Third Party Audits and Certifications

The da Vinci OnSite infrastructure has no industry certification’s, 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.

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 or anti-malware software. To mitigate and to minimize any potential network threats, the da Vinci System sits 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. Da Vinci system service logs are backed up during the preventive maintenance service performed by a da Vinci field service engineer.

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. Onsite is not critical to the clinical operation and performance of the da Vinci Surgical System.

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.

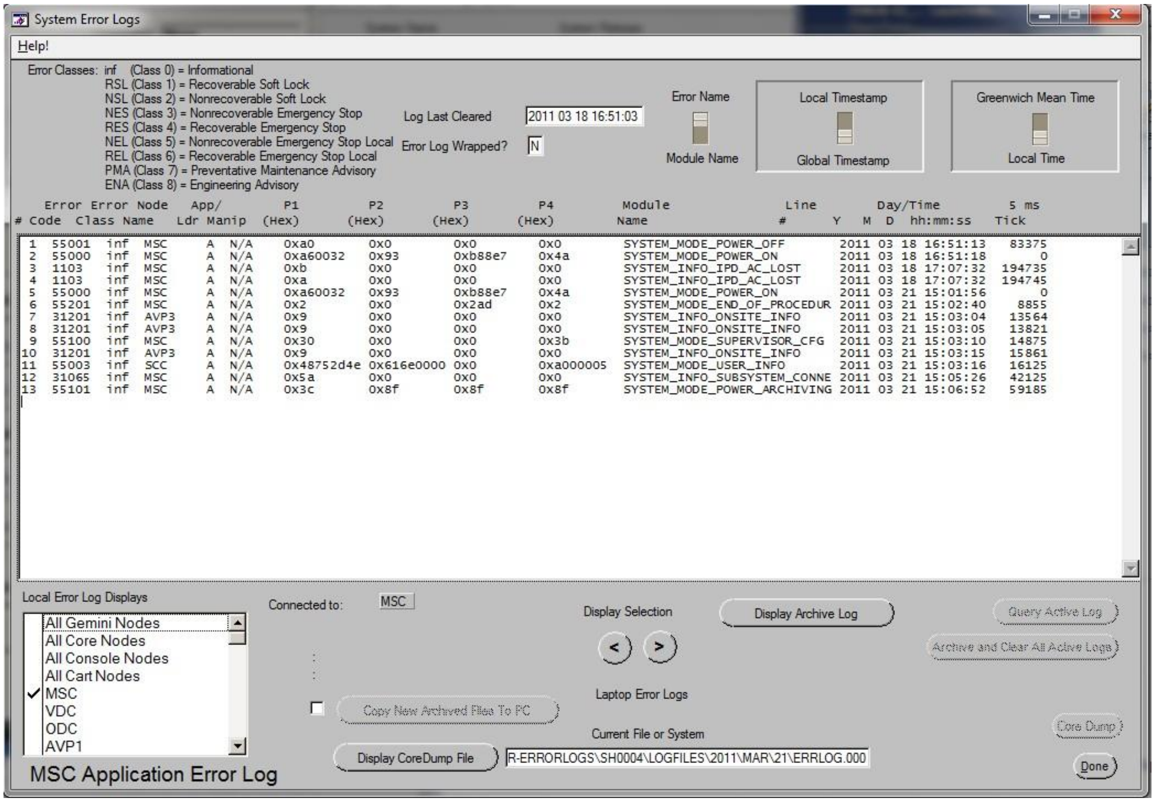
15. Patient Privacy

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 electronic Patient Health Information (ePHI), nor does the system interface with any of the Hospital’s internal resources’ such as Hospital Information System (HIS), Radiology Information System (RIS) or Picture Archiving and Communication System (PACS) systems to obtain such information.

Appendix 1 – System Log

The da Vinci stores binary formatted machine data that broadly consists of; time stamped systems events, system identifier, various component data (serial numbers, voltages and firmware), instrument data, software versions and checksums, system internal network communication data, ergonomic profile settings, system configuration and feature enabled data and other machine / service information. Advance logging (if enabled) collects spatial manipulator / arm data and UI information, typically used in conjunction with a research study or advance service troubleshooting. The da Vinci does not store, access, or transmit any patient or contain any hospital sensitive information.

Below is a screen capture of a parsed log file, using our proprietary service application. Logs do not contain any patient sensitive information.



System Error Logs

Help!

Error Classes: inf (Class 0) = Informational
RSL (Class 1) = Recoverable Soft Lock
NSL (Class 2) = Nonrecoverable Soft Lock
NES (Class 3) = Nonrecoverable Emergency Stop
RES (Class 4) = Recoverable Emergency Stop
NEL (Class 5) = Nonrecoverable Emergency Stop Local
REL (Class 6) = Recoverable Emergency Stop Local
PMA (Class 7) = Preventative Maintenance Advisory
ENA (Class 8) = Engineering Advisory

Log Last Cleared: 2011 03 18 16:51:03

Error Log Wrapped? N

```
   Error Error Node   App/       P1         P2         P3         P4         Module               Line       Day/Time       5 ms
# Code  Class Name  Ldr Manip   (Hex)      (Hex)      (Hex)      (Hex)      Name                 #     Y  M  D  hh:mm:ss   Tick
 1  55001  inf  MSC    A  N/A   0xa0       0x0        0x0        0x0        SYSTEM_MODE_POWER_OFF       2011 03 18 16:51:13   83375
 2  55000  inf  MSC    A  N/A   0xa60032   0x93       0xb88e7    0x4a       SYSTEM_MODE_POWER_ON        2011 03 18 16:51:18       0
 3  1103   inf  MSC    A  N/A   0xb        0x0        0x0        0x0        SYSTEM_INFO_IPD_AC_LOST     2011 03 18 17:07:32  194735
 4  1103   inf  MSC    A  N/A   0xa        0x0        0x0        0x0        SYSTEM_INFO_IPD_AC_LOST     2011 03 18 17:07:32  194745
 5  55000  inf  MSC    A  N/A   0xa60032   0x93       0xb88e7    0x4a       SYSTEM_MODE_POWER_ON        2011 03 21 15:01:56       0
 6  55201  inf  MSC    A  N/A   0x2        0x0        0x2ad      0x2        SYSTEM_MODE_END_OF_PROCEDUR 2011 03 21 15:02:40    8855
 7  31201  inf  AVP3   A  N/A   0x9        0x0        0x0        0x0        SYSTEM_INFO_ONSITE_INFO     2011 03 21 15:03:04   13564
 8  31201  inf  AVP3   A  N/A   0x9        0x0        0x0        0x0        SYSTEM_INFO_ONSITE_INFO     2011 03 21 15:03:05   13821
 9  55100  inf  MSC    A  N/A   0x30       0x0        0x0        0x3b       SYSTEM_MODE_SUPERVISOR_CFG  2011 03 21 15:03:10   14875
10  31201  inf  AVP3   A  N/A   0x9        0x0        0x0        0x0        SYSTEM_INFO_ONSITE_INFO     2011 03 21 15:03:15   15861
11  55003  inf  SCC    A  N/A   0x48752d4e 0x616e0000 0x0        0xa000005  SYSTEM_MODE_USER_INFO       2011 03 21 15:03:16   16125
12  31065  inf  MSC    A  N/A   0x5a       0x0        0x0        0x0        SYSTEM_INFO_SUBSYSTEM_CONNE 2011 03 21 15:05:26   42125
13  55101  inf  MSC    A  N/A   0x3c       0x8f       0x8f       0x8f       SYSTEM_MODE_POWER_ARCHIVING 2011 03 21 15:06:52   59185
```

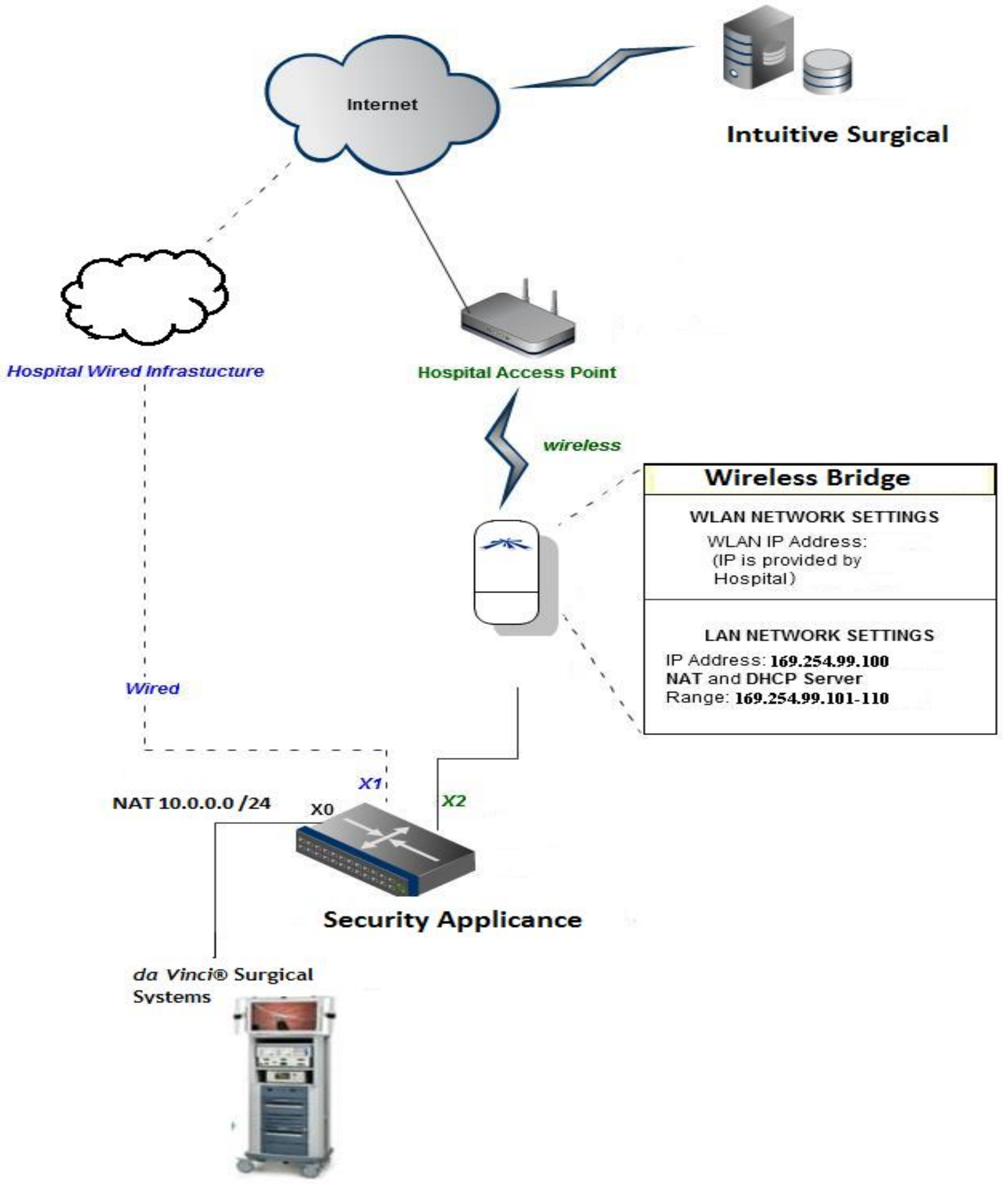
Connected to: MSC

Current File or System: R-ERRORLOGS\SH0004\LOGFILES\2011\MAR\21\ERRLOG.000

Appendix 2 – Optional Wireless Connectivity Kit

The wireless bridge is configured to only operate as a wireless supplicant. The bridge supports 802.11 B, G, and N using 2.4GHz frequency. 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 Bridge

WLAN NETWORK SETTINGS

WLAN IP Address:
(IP is provided by
Hospital)

LAN NETWORK SETTINGS

IP Address: **169.254.99.100**
NAT and DHCP Server
Range: **169.254.99.101-110**

Wireless Security

The Wireless Connectivity Option currently supports the following security configurations:

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

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.