**Technical Requirements for Connecting the Stratus Video App**

**to the Stratus Video Network**

**Overview**

This document reviews the necessary technical requirements to connect to the Stratus Video Interpreting Network. The Stratus Video App is a PC, MAC, iOS, and Android based video application that allows any user running the software to make a video or audio call to the language interpreter of choice. The Stratus Video App can be downloaded from the Stratus Video website for PC and MAC, from the Apple App Store for iOS devices, or from the Google Play Store for Android devices. Here are the direct links to download the software for each type of device:

PC: <http://mcs.champvrs.com/MirialCarrierServer/download/latestVersion/ODI/Setup.exe>

Mac - <http://mcs.champvrs.com/MirialCarrierServer/download/latestVersionOSX/ODI/Setup.pkg>

iOS Device - [https://itunes.apple.com/us/app/on-demand-interpreting-odi/id519137581?mt=8#](https://itunes.apple.com/us/app/on-demand-interpreting-odi/id519137581?mt=8)

Android - <https://play.google.com/store/apps/details?id=com.odi.android&hl=en>

**Security – VPN and HIPAA**

To ensure HIPAA compliance, all connections to Stratus Video require an IPSEC or SSL VPN connection. This ensures both the call setup and media of the video and audio calls will be at minimum 128bit encrypted over the Internet. All calls to Stratus Video will leave the hospital network encrypted on VPNs going to both Stratus Video data centers and routed to an interpreter on the Status Video secure network Stratus Video currently uses Cisco ASA 5580 firewalls and will setup the VPN parameters based on the customers’ security requirements. Stratus Video supports site-to-site VPN’s to the customer’s firewall or VPN terminator, and device-based Cisco AnyConnect VPN’s. If the customer does not have a pre-defined set of VPN parameters then Stratus Video will provide a set of HIPAA compliant parameters to the customer. The customer also may purchase a direct MPLS connection to Stratus Video, so that no interpreted calls ever travel over the Internet.

**Approved Tablets and Smartphones**

**iOS Devices**

iPhone® 5S

iPhone® 5c

iPhone® 4S

iPhone® 4

iPod touch® 4th generation

iPad™ Air

iPad™ 2

iPad™Mini

iPad™ (iPad™ has no video camera, so only remote-party video is shown if available)

iPhone® 3GS (iPhone® 3GS uses the only available back camera)

**Android**™ **Devices**

HTC EVO™, Desire™ HD, Incredible, Sensation, myTouch® 4G, Droid Incredible II, ThunderBolt,

Flyer P512, Evo 3D, One X, One S

Samsung Epic™, Galaxy S, Galaxy S II, Galaxy Tab, Galaxy Tab 10.1, Captivate™, Fascinate™, Vibrant™, Galaxy Nexus, Sidekick 4G, Droid Charge, Conquer, Note

Google Nexus One, Nexus S

Dell Streak 5, Streak 7

Motorola Atrix 4G, Xoom, Droid Bionic

Acer Iconia Tab A500

**Note**: This list includes only the certified devices; other Android devices may work.

**PC and MAC Requirements**

**Minimum Requirements**

Operating System:

* Windows XP / 2003 / Vista / 7 / 8 / 8.1 (including 64 bit versions), DirectX 9.0c or higher
* Mac OS X 10.5 Leopard or higher
* Any x86 CPU with SSE2 instructions (audio/high-res video calls)
* Core 2 Duo class, 2.33 GHz (H.264 calls)
* 1GB Ram (2GB recommended on Vista)
* 30Mb unused hard-disk space

**Recommended Requirements**

Operating System:

* Windows 7 (including 64 bit versions), DirectX 9.0c or higher
* Mac OS X 10.5 Leopard or higher
* Core 2 Duo class, 3 GHz
* 4GB Ram (2GB recommended on Vista)
* 250Mb unused hard-disk space

**Recommended Peripheral Webcams**

Logitech HD Pro C910

Logitech HD Pro C920

Logitech HD Pro C930

Logitech HD Pro C510

Microsoft Life Cam Studio

**Application Requirements**

1. The required “Outbound Only” (See Below) ports for each used product must be opened on the hospital’s firewall.
2. Each concurrent video interpreted call requires a minimum bandwidth of 384K.
3. Each concurrent audio call for spoken language requires a minimum of 64K.

4. Stratus Video requires the customer to have a non-saturated Internet connection.

5. For the Stratus Video App software, the customer must provide a wireless network with enough coverage, capacity and security for connectivity over the hospital network. The network should be designed and structured to provide 384k of bandwidth for each simultaneous video call.

6. If possible, QOS should be used on the entire session from the video device to the customers firewall.

**Port Requirements for the Stratus Video App**

The Stratus Video App is a SIP based video software application. They require the following ports to be opened on the hospital firewall to allow the software to communicate with Stratus Video’s servers and for the SIP signaling and media to pass through the firewall. Only OUTBOUND ports are required to be opened because the Stratus Video App uses stateful HTTPS, SIP and RTP ports. The Stratus Video App also works with source NATing of internal IPs and do not require a 1 to 1 NAT or a globally routed IP address.

From:   Any IP address, subnet, or host address

To:  208.94.16.21, 208.94.16.49, 208.94.16.203, 208.94.16.204, 208.94.16.205, 208.95.32.21, 208.95.32.49, 208.95.32.203, 208.95.32.204, and 208.95.32.205

Ports: 443 TCP, 5060 TCP and 10000-16000 UDP

From:   Any IP address, subnet, or host address

To:  208.94.16.114 and 208.95.32.114

Ports: 80 TCP, 443 TCP

**Port Requirements for Stratus Video-Provided SOTI MDM (if applicable)**

From:   Any IP address, subnet, or host address

To:  208.94.16.200 and 208.95.32.200

Ports: 80 TCP, 443 TCP, 5494 TCP

**Important:** Any SIP packet inspection or SIP ALG of the Stratus Video data on the firewall must be disabled for the Stratus Video App data. Inspection policies or ALGs are typically included in the firewall’s global policy, and can cause problems with the Stratus Video App application logging in, placing calls, and/or dropping calls. Create a service policy for the Stratus Video App data with port TCP 5060 pointing to 208.94.16.21, 208.94.16.49, 208.94.16.203, 208.94.16.204, 208.94.16.205, 208.95.32.21, 208.95.32.49, 208.95.32.203, 208.95.32.204, and 208.95.32.205

Also, proxy servers or web content appliances can adversely affect the Stratus Video App. The App must be bypass these entirely, or exceptions or white lists must be created on these devices for 208.94.16.21, 208.94.16.49, 208.94.16.114, 208.94.16.203, 208.94.16.204, 208.94.16.205, 208.95.32.21, 208.95.32.49, 208.95.32.114, 208.95.32.203, 208.95.32.204, 208.95.32.205, mcs.csdvrs.com, lb.mcs.csdvrs.com, mcs1.mcs.csdvrs.com, mcs2.mcs.csdvrs.com, mcs3.mcs.csdvrs.com, mcs4.mcs.csdvrs.com, and zdial.champvrs.com.

For DNS resolution, the Stratus Video App uses mcs.csdvrs.com, lb.mcs.csdvrs.com, mcs1.mcs.csdvrs.com, mcs2.mcs.csdvrs.com, mcs3.mcs.csdvrs.com, mcs4.mcs.csdvrs.com, and zdial.champvrs.com. This requires customer’s DNS server and/or firewall must be able to reach TCP and UDP ports 53 on Stratus Video Name Servers 208.94.16.61, 208.94.16.62, 208.95.32.61, and 208.95.32.62.

Please complete the VPN Information Form on the next page and return to the Stratus Video Support Contact specified on the form, if a site-to-site VPN is required for encryption of the Stratus Video App data. It is highly recommended that a single public IP address is specified for the encryption domain on the VPN tunnels, and that PAT (port address translation) is used to mask all hosts that will be used for the Stratus Video App behind the single IP address. PAT allows up to 65,535 private IP addresses to be masked behind a single public IP address

**Stratus Video VPN Information Form**

*If your gateway doesn’t support a particular configuration parameter, please indicate so by entering ‘not supported’ in the field.*

|  |  |
| --- | --- |
| **VPN END PEER INFORMATION** |  |
| Company Name | **Stratus** |
| Remote Firewall Peer Address | 74.119.12.20 Tunnel A - 74.119.14.20 Tunnel B |
| Remote Firewall Type/Brand/Version | Cisco ASA 5580 |
| Remote Support Contact Name/Number | Customer Support 855-663-1231  Email –VPN@stratusvideo.com |
| Customer Company Name |  |
| Customer VPN Peer Address |  |
| Customer Firewall Type |  |
| Customer Firewall Contact Name/Company/Number |  |
| Support/Help Desk Number |  |

For security purposes the following security requirements are enforced

|  |  |  |  |
| --- | --- | --- | --- |
| **IPSEC PHASE 1** | |  | |
| Exchange Mode | | Main Mode | |
| Authentication Method – Pre-Shared Secret | | To be exchanged via phone | |
| Encryption Method | | 3DES, AES128, AES192, AES256 (circle choice) | |
| Hash Algorithm | | MD5, SHA (circle choice) | |
| Security association (SA) Lifetime | | 86400 seconds, unless otherwise specified | |
| Diffie-Hillman Group | | 1, 2, 5, 7 (circle choice) | |
| **IPSEC PHASE 2** | |  | |
| Security Protocol | | ESP | |
| Encapsulation Mode | | Tunnel | |
| Encryption Method | | 3DES, AES128, AES192, AES256 (circle choice) | |
| Hash Algorithm | | MD5, SHA (circle choice) | |
| Security association (SA) Lifetime | | 28800 seconds, unless otherwise specified | |
| Compression Method | | None | |
| Perfect Forward Secrecy | | On Off (circle choice) | |
| **ENCRYPTION DOMAIN (HOST IP, IP RANGE, OR SUBNET, NOT GREATER THAN A /24)** | | | |
| From Host(s) | To Hosts | | TCP/UDP Ports |
| (Use of single IP and PAT all hosts behind it preferred) | Tunnel A – 208.94.16.21, 208.94.16.49, 208.94.16.114, 208.94.16.203, 208.94.16.204, 208.94.16.205 | | 80 TCP, 443 TCP, 5060 TCP, 10000 – 16000 UDP |
| Tunnel B - 208.95.32.21, 208.95.32.49, 208.95.32.114, 208.95.32.203, 208.95.32.204, 208.95.32.205 | | 80 TCP, 443 TCP, 5060 TCP, 10000 – 16000 UDP |