



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Remote User Access to Avaya one-X® Communicator SIP over VPN IPsec tunnel with Avaya VPN client using Avaya VPN Gateway 3050 with Avaya Aura® Session Manager R6.1 Issue – 1.0**

## **Abstract**

These Application Notes presents a configuration where a remote user with Avaya one-X® Communicator SIP soft client establishes and terminates a VPN IPsec Tunnel with Avaya VPN Client in the main office location, with an Avaya VPN Gateway 3050. Once the Avaya one-X® Communicator SIP soft client completes the VPN IPsec tunnel negotiation, it will register to Avaya Aura® Session Manager R6.1.

The validation test of the sample configuration was conducted at the Avaya Solution and Interoperability Test Lab at the request of the Avaya Solutions and Marketing Team.

# 1. Introduction

## 1.1. Avaya VPN Client Transparent Mode

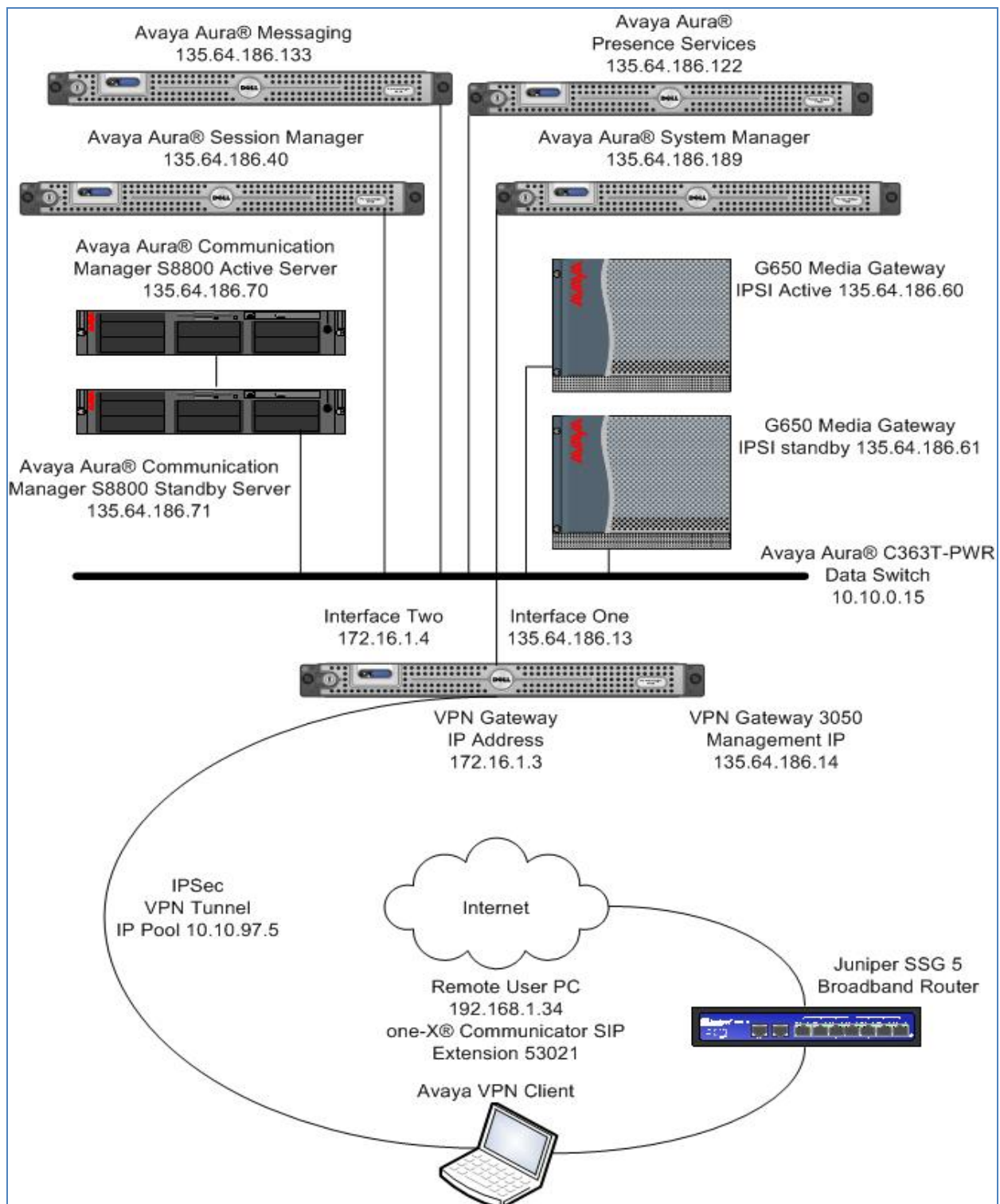
The term transparent mode is mainly relevant from a user perspective. It means that the remote user will experience network access as if actually sitting within the corporate intranet. No portal interaction is required. As opposed to clientless mode, transparent mode requires the user to install the VPN client on the remote user pc. Transparent mode supports access to the intranet through legacy TCP or UDP based client applications. Intranet web browsing without logging into a Portal and intranet mail server access through the remote users native email client server can be used. Access to a wide range of intranet services built on legacy client/server technologies, as well as telnet and SSH access to the intranet terminal servers through the remote users native telnet or SSH client software, is also possible.

## 1.2. Interoperability Compliance Testing

The objective of this interoperability test is to verify that the Avaya one-X® Communicator SIP soft client can interoperate with Avaya VPN Gateway 3050 over a VPN IPsec tunnel while registered to Avaya Aura® Session Manager. Another objective is to confirm that Avaya one-X® Communicator SIP can make a video call, integrate with Avaya Aura® Messaging and Avaya Aura® Presence Services, while the VPN IPsec tunnel is established to the Avaya VPN Gateway 3050.

## 1.3. Configuration

The configuration used in these Application Note is shown in **Figure 1**. The Avaya Aura® Session Manager software is installed and configured on Red Hat Linux 5.5 Operating System on a S8800 Media Server. The Avaya Aura® System Manager is installed on Avaya System Platform on a S8800 Media Server. The Avaya Aura® System Manager is a template running its own Red Hat Linux Operating System 5.5. The Avaya one-X® Communicator SIP soft client is configured to register to Avaya Aura® Session Manager and are administered as an OPS station on Avaya Aura® Communication Manager running as an Evolution Server. The Avaya G650 Media Gateway contains the IP server Interface card which is used to interface with the Avaya Aura® Communication Manager Evolution Server. The G650 Media Gateway also contains the CLAN and Medpro cards used for signaling and audio generation respectively. All inter-system calls are carried over a SIP trunk. The Avaya Aura® Presence Services Server is used to provide Presence information to one-X® Communicator SIP soft client. The Avaya Aura® Messaging server is used to provide voicemail functionality and message waiting indicator (mwi) to the one-X® Communicator SIP soft client. The diagram indicates logical signaling connections. All components are physically connected to a single Avaya C363T-PWR Converged Stackable Switch, and are administered into a subnet range, 135.64.186.x. The Avaya VPN Gateway 3050 is configured to establish a VPN IPsec tunnel between the remote users pc. The Juniper SSG 5 is used to simulate a broadband connection thus giving the remote user pc access to the internet.



**Figure 1: VPN IPsec tunnel with VPN Client using AvayaVPN Gateway 3050**

## 2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya Aura®	Software
Avaya Aura® System Manager on a S8800 Server	Avaya Aura® System Manager Release 6.1.0.0.7345-6.1.5.106 Update: Service Pack 2
Avaya Aura® Session Manager on a S8800 Server	Avaya Aura® Session Manager Release 6.1.2.0.612004 Update: Service Pack 2
Avaya Aura® Communication Manager on a S8800 Server	Avaya Aura® Communication Manager Release 6.0.1 R16x.00.1.510.0 Update: Service Pack 3
Avaya Media Gateway G650 IP Server Interface TN2312BP Clan TN799DP IPMedpro TN2602AP	Hardware 15 Firmware 54 Hardware 16 Firmware 40 Hardware 08 Firmware 59
Avaya Aura® C363T-PWR Converged Stackable Switch	Release 4.5.14
Avaya VPN Client	Release 10.05.012.0
Avaya VPN Gateway 3050	Release 8.0.7.1
Avaya one-X® Communicator SIP Soft client	Release 6.1.0.19-GA-31696
Juniper SSG 5 Router	Release 6.1.0r2.0

## 3. Configure Avaya Aura® System Manager

This section describes steps needed to configure System Manager. It will describe configuration of accessing System Manager, administering a Location and adding a SIP User in User Management of System Manager. For details of how to administer a SIP Entity between Session Manager and the Communication Manager Evolution Server in order to establish a SIP Entity link between Session Manager and the Communication Manager Evolution Server refer to **Application Notes for Configuring Avaya A175 Desktop Video Device to connect Avaya Aura® Session Manager with Avaya Aura® Communication Manager as an Evolution Server.**

### 3.1. Access Avaya Aura® Session Manager

Access the System Manager web interface, by entering **http://<ip-addr>/SMGR** as the URL in an Internet browser, where *<ip-addr>* is the IP address of the server running System Manager graphical user interface. Log in with the appropriate **User ID** and **Password** and press the **Log On** button to access System Manager.

System Manager - Windows Internet Explorer provided by Avaya IT

https://135.64.186.189/network-login/

AVAYA Avaya Aura® System Manager 6.1

Home / Log On

**Log On**

Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

User ID:

Password:

**Log On** Cancel

[Change Password](#)

The following screen is displayed upon login.

Users	Elements	Services
<b>Administrators</b> Manage Administrative Users	<b>Application Management</b> Manage applications and application certificates	<b>Backup and Restore</b> Backup and restore System Manager database
<b>Groups &amp; Roles</b> Manage groups, roles and assign roles to users	<b>Communication Manager</b> Manage Communication Manager objects	<b>Configurations</b> Manage system wide configurations
<b>Subscribers</b> Manage users and shared resources associated with CS1000, including LDAP/file import and export	<b>Conferencing</b> Conferencing	<b>Events</b> Manage alarms, view and harvest logs
<b>Synchronize and Import</b> Synchronize users with the enterprise directory, import users from file	<b>Inventory</b> Manage, discover, and navigate to elements, update element software	<b>Licenses</b> View and configure licenses
<b>UCM Roles</b> Manage UCM Roles, assign roles to users	<b>Messaging</b> Manage Messaging System objects	<b>Replication</b> Track data replication nodes, repair replication nodes
<b>User Management</b> Manage users, shared user resources and provision users	<b>Presence</b> Presence	<b>Scheduler</b> Schedule, track, cancel, update and delete jobs
	<b>Routing</b> Network Routing Policy	<b>Security</b> Manage Security Certificates
	<b>Session Manager</b> Session Manager Element Manager	<b>Templates</b> Manage Templates for Communication Manager and Messaging System objects
	<b>SIP AS 8.1</b> SIP AS 8.1	<b>UCM Services</b> Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

### 3.2. Administer Location

To add a new Location, click on **Routing** and access the **Locations** sub heading. The **New** button was selected to add a new location. Locations are used to identify logical and physical locations where SIP entities reside for the purposes of bandwidth management or location based routing.

The screenshot shows the Avaya Aura System Manager 6.1 interface. On the left, a navigation menu has 'Routing' and 'Locations' highlighted with red boxes. The main area shows a breadcrumb trail 'Home / Elements / Routing / Locations- Location'. Below this, the 'Location' section contains buttons for 'Edit', 'New' (highlighted with a red box), 'Duplicate', 'Delete', and 'More Actions'.

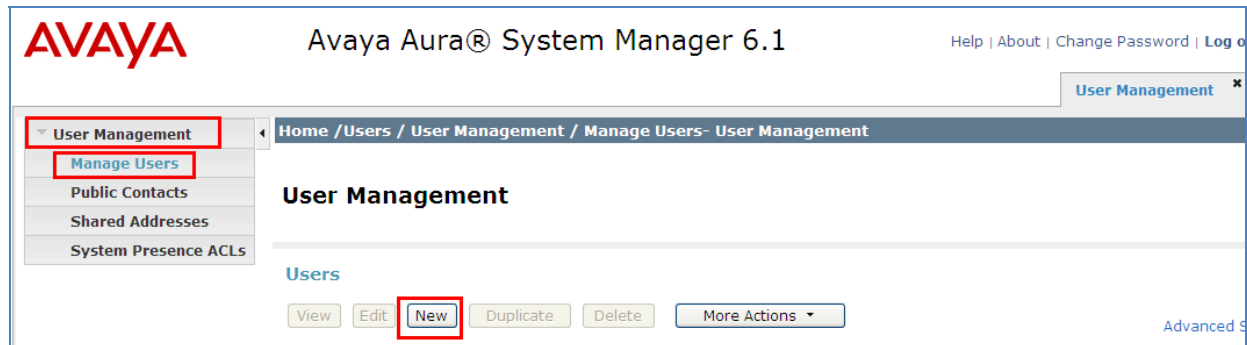
A location **Name** called **Galway Stack** was added to the Session Manager. The IP Address pattern **10.10.97.\*** and **135.64.186.\*** were added the **IP Address Pattern** table. The **Commit** button was selected to confirm changes.

The screenshot shows the 'New Location' form in Avaya Aura System Manager 6.1. The 'Name' field is filled with 'Galway Stack' and is highlighted with a red box. Below it is a 'Notes' field. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' set to 'Kbit/sec' and an empty 'Total Bandwidth' field. The 'Per-Call Bandwidth Parameters' section shows '\* Default Audio Bandwidth' set to '80 Kbit/sec'. The 'Location Pattern' section has 'Add' and 'Remove' buttons, with 'Add' highlighted by a red box. Below this is a table with 2 items, showing IP Address Patterns: '\* 10.10.97.\*' and '\* 135.64.186.\*', both highlighted with red boxes. At the bottom right, the 'Commit' button is highlighted with a red box, next to a 'Cancel' button. A '\* Input Required' message is visible at the bottom left.

IP Address Pattern	Notes
* 10.10.97.*	
* 135.64.186.*	

### 3.3. Administer SIP User

To add a SIP User to Session Manager, access the **User Management** heading on the left hand side of the System Manager GUI. Access the **Manage Users** sub heading. The **New** button was selected.



For the SIP User being added the **Last Name** was **1XC** and the **First Name** was **User**. The **Login Name** was **53021@silstack.com** and the **Password** was set to the password of the System Manager upon login.

The screenshot shows the 'Identity' form for adding a new user. The form includes the following fields: 'Last Name' (value: 1XC), 'First Name' (value: User), 'Middle Name' (empty), 'Description' (empty), 'Login Name' (value: 53021@silstack.com), 'Authentication Type' (dropdown: Basic), 'Password' (masked with dots), 'Confirm Password' (masked with dots), 'Localized Display Name' (empty), 'Endpoint Display Name' (empty), 'Honorific' (empty), 'Language Preference' (dropdown), and 'Time Zone' (empty). The fields for 'Last Name', 'First Name', 'Login Name', 'Password', and 'Confirm Password' are highlighted with red boxes, indicating the required information for the user.

Access the **Communication Address** heading. In the Communication Address the **Type** was set to **Avaya E.164**. The **Fully Qualified Address** was set as **+35391453021@silstack.com**. Select the **Add** button to save the changes.

**Communication Address** ▼

New Edit Delete

<input checked="" type="checkbox"/>	Type	Handle	Domain
<input type="checkbox"/>	Avaya SIP	53021	silstack.com
<input type="checkbox"/>	Jabber	53021@pres.silstack.com	

Select : All, None

Type: Avaya E.164 ▼

\* Fully Qualified Address: +35391453021 @ silstack.com ▼

Add Cancel

Access the **Session Manager Profile**. The **Primary Session Manager** was set to **Session Manager One** as shown below. This equates to the Session Manager SIP entity. The **Origination and Termination Application Sequence** was set to **CMES**. This is the Communication Manager Evolution Server Application Sequence name. The **Home Location** was set to **Galway Stack**.

☒ **Session Manager Profile** ▼

\* Primary Session Manager Session Manager One ▼

Secondary Session Manager (None) ▼

Origination Application Sequence CMES ▼

Termination Application Sequence CMES ▼

Survivability Server (None) ▼

\* Home Location Galway Stack ▼

Primary	Secondary	Maximum
17	0	17

Primary	Secondary	Maximum

In order for the Station Profile template information to be pushed from the Session Manager down to the Communication Manager Evolution Server, **enable** the **Endpoint Profile** box. The **System** was set to **CMES60**. This is the Communication Manager Evolution Server Element Name. The **Extension** was set to **53021** and the **Template** was set to **DEFAULT\_9630SIP\_CM\_6\_0**. The **Port** was set to **IP**. The **Voice mail Number** was set to **80960**.



☒ **Endpoint Profile** ▼

\* **System** CMES60 ▼

\* **Profile Type** Endpoint ▼

Use Existing Endpoints ☐

\* **Extension** 53021 Endpoint Editor

\* **Template** DEFAULT\_9630SIP\_CM\_6\_0 ▼

**Set Type** 9630SIP

**Security Code**

\* **Port** IP

**Voice Mail Number** 80960

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☐

Click on **Endpoint Editor**, and under **Feature Options** enable **IP softphone** and **IP Video Softphone**.

General Options (G) *	<b>Feature Options (F)</b>	Site Data (S)	Abbreviated Call Dialing (A)																
Enhanced Call Fwd (E)	Button Assignment (B)	Group Membership (M)																	
<b>Active Station Ringing</b> single ▼ <b>MWI Served User Type</b> Select ▼ <b>Per Station CPN - Send Calling Number</b> Select ▼ <b>IP Phone Group ID</b> <input type="text"/> <b>Remote Soft Phone Emergency Calls</b> as-on-local ▼ <b>LWC Reception</b> spe ▼ <b>AUDIX Name</b> <input type="text"/> <b>Speakerphone</b> 2-way ▼ <b>Short/Prefixed Registration Allowed</b> Select ▼	<b>Auto Answer</b> none ▼ <b>Coverage After Forwarding</b> system ▼ <b>Display Language</b> english ▼ <b>Hunt-to Station</b> <input type="text"/> <b>Loss Group</b> 19 <b>Survivable COR</b> internal ▼ <b>Time of Day Lock Table</b> Select ▼ <b>Voice Mail Number</b> <input type="text"/>																		
<b>Features</b> <table border="0"> <tr> <td><input type="checkbox"/> Always Use</td> <td><input type="checkbox"/> Idle Appearance Preference</td> </tr> <tr> <td><input type="checkbox"/> IP Audio Hairpinning</td> <td><input checked="" type="checkbox"/> <b>IP SoftPhone</b></td> </tr> <tr> <td><input type="checkbox"/> Bridged Call Alerting</td> <td><input checked="" type="checkbox"/> LWC Activation</td> </tr> <tr> <td><input type="checkbox"/> Bridged Idle Line Preference</td> <td><input type="checkbox"/> CDR Privacy</td> </tr> <tr> <td><input checked="" type="checkbox"/> Coverage Message Retrieval</td> <td><input checked="" type="checkbox"/> Direct IP-IP Auto Connection</td> </tr> <tr> <td><input type="checkbox"/> Data Restriction</td> <td><input type="checkbox"/> H.320 Conversion</td> </tr> <tr> <td><input checked="" type="checkbox"/> Survivable Trunk Dest</td> <td><input checked="" type="checkbox"/> <b>IP Video Softphone</b></td> </tr> <tr> <td><input type="checkbox"/> Bridged Appearance Origination Restriction</td> <td></td> </tr> </table>				<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference	<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> <b>IP SoftPhone</b>	<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation	<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy	<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Direct IP-IP Auto Connection	<input type="checkbox"/> Data Restriction	<input type="checkbox"/> H.320 Conversion	<input checked="" type="checkbox"/> Survivable Trunk Dest	<input checked="" type="checkbox"/> <b>IP Video Softphone</b>	<input type="checkbox"/> Bridged Appearance Origination Restriction	
<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference																		
<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> <b>IP SoftPhone</b>																		
<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation																		
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy																		
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Direct IP-IP Auto Connection																		
<input type="checkbox"/> Data Restriction	<input type="checkbox"/> H.320 Conversion																		
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input checked="" type="checkbox"/> <b>IP Video Softphone</b>																		
<input type="checkbox"/> Bridged Appearance Origination Restriction																			

For a video call to work correctly from the one-X Communicator SIP endpoint, **6 call-app** buttons were set via the **Button Assignments** tab. The **Done** button was selected.

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)	<b>Button Assignment (B)</b>	Group Membership (M)	

Main Buttons	Feature Buttons	Button Modules		
1 call-appr ▼				
2 call-appr ▼				
3 call-appr ▼				
4 call-appr ▼				
5 call-appr ▼				
6 call-appr ▼				
7 Select ▼				
8 Select ▼				

\*Required

Select **Commit** to save the changes.

**Delete Endpoint on Unassign of Endpoint from User or on Delete User.** ☐

☐ **Messaging Profile** ▶

## 4. Administer Avaya Aura® Communication Manager

This section describes steps needed to configure Communication Manager. It will describe configuration of ip codec, ip network region, ip network map and configuring Avaya one-X Communicator SIP as a station for a remote user to make a video call. These instructions assume that Communication Manager has been installed, configured, licensed and provided with a functional dial plan. For details of configuring an Off-PBX Station (OPS) and administering a SIP Trunk to carry calls between a SIP endpoint in Communication Manager Evolution Server refer to **Application Notes for Configuring Avaya A175 Desktop Video Device to connect Avaya Aura® Session Manager with Avaya Aura® Communication Manager as an Evolution Server Issue – 0.2.**

## 4.1. Administer Signaling Group

This section describes the **Signaling Group** screen. The **Group Type** was set to **sip** and the **Transport Method** was set to **tls**. Since the one-X Communicator endpoint is using a Communication Manager Feature Server for Off Pbx Station Mapping, the **IMS Enabled** setting must be set to **no**. Since the sip trunk is between the Communication Manager Evolution Server and Session Manager, the **Near-end Node Name** is the node name of the “procr” of the Communication Manager Evolution Server. The **Far-end Node Name** is the node name of the Session Manager Server. This is **SessionManager1**. The **Near-end Listen Port** and **Far-end Listen Port** are both set to port number **5061**. The **Far-end Network-Region** was set to **1**.

```
display signaling-group 120

SIGNALING GROUP

Group Number: 120          Group Type: sip
IMS Enabled? n            Transport Method: tls
Q-SIP? n                  SIP Enabled LSP? n
IP Video? y               Priority Video? n   Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM

Near-end Node Name: procr      Far-end Node Name: SessionManager1
Near-end Listen Port: 5061     Far-end Listen Port: 5061
Far-end Network Region: 1

Far-end Domain:

Incoming Dialog Loopbacks: eliminate      Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                  RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3         Direct IP-IP Audio Connections? y
Enable Layer 3 Test? n                     IP Audio Hairpinning? n
Direct IP-IP Early Media? n
```

## 4.2. Administer IP Network Map

This section describes the **IP Network Map** screen. The IP Address range will be the same range as the IP Pool address range defined on the Avaya VPN Gateway 3050. The **FROM** range was **10.10.97.0** and the **TO** range was **10.10.97.255**. The **Network Region** was **1** and **Subnet Bits** was **24**.

```
display ip-network-map                                     Page 1 of 63

IP ADDRESS MAPPING

IP Address          Subnet Bits  Network Region  VLAN  Emergency Location Ext
-----
FROM: 10.10.97.0    /24         1              n
TO: 10.10.97.255
```

### 4.3. Administer IP Network Region

This section describes the **IP Network Region** screen. It was decided to place the one-X Communicator SIP soft client on the remote user pc into network region **1**. The **Authoritative Domain** must mirror the domain name of Session Manager. This was **silstack.com**. The codecs used on the SIP endpoints were placed in **Codec Set 1**. IP Shuffling was turned on so both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** were set to **y** (yes).

```
display ip-network-region 1                                     Page 1 of 19

                                IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: silstack.com
Name:
MEDIA PARAMETERS                      Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                    Inter-region IP-IP Direct Audio: yes
      UDP Port Min: 2048                IP Audio Hairpinning? n
      UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                RTCP Reporting Enabled? y
Call Control PHB Value: 46            RTCP MONITOR SERVER PARAMETERS
      Audio PHB Value: 46                Use Default Server Parameters? y
      Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
      Audio 802.1p Priority: 6
      Video 802.1p Priority: 5          AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                      RSVP Enabled? n
      H.323 Link Bounce Recovery? y
      Idle Traffic Interval (sec): 20
      Keep-Alive Interval (sec): 5
      Keep-Alive Count: 5
```

### 4.4. Administer IP Codec Set

This section describes the **IP Codec Set** screen. IP Codec **G.711MU**, **G.711A** and **G.729** were used for testing purposes with the One X Communicator SIP endpoint on the remote user pc.

```
display ip-codec-set 1                                         Page 1 of 2

                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt   Size(ms)
1: G.711MU      n           2         20
2: G.711A      n           2         20
3: G.729       n           2         20
4:
```

On **Page 2** set **Allow Direct-IP Multimedia** to **y** (yes). For this configuration a **Maximum Call Rate** of **768 Kbits** was set to prevent video from oversubscribing.

display ip-codec-set 1		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? y		
Maximum Call Rate for Direct-IP Multimedia:		768:Kbits
Maximum Call Rate for Priority Direct-IP Multimedia:		768:Kbits
	Mode	Redundancy
FAX	relay	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

## 4.5. Save Translations

Use the **save translations** command to save these changes.

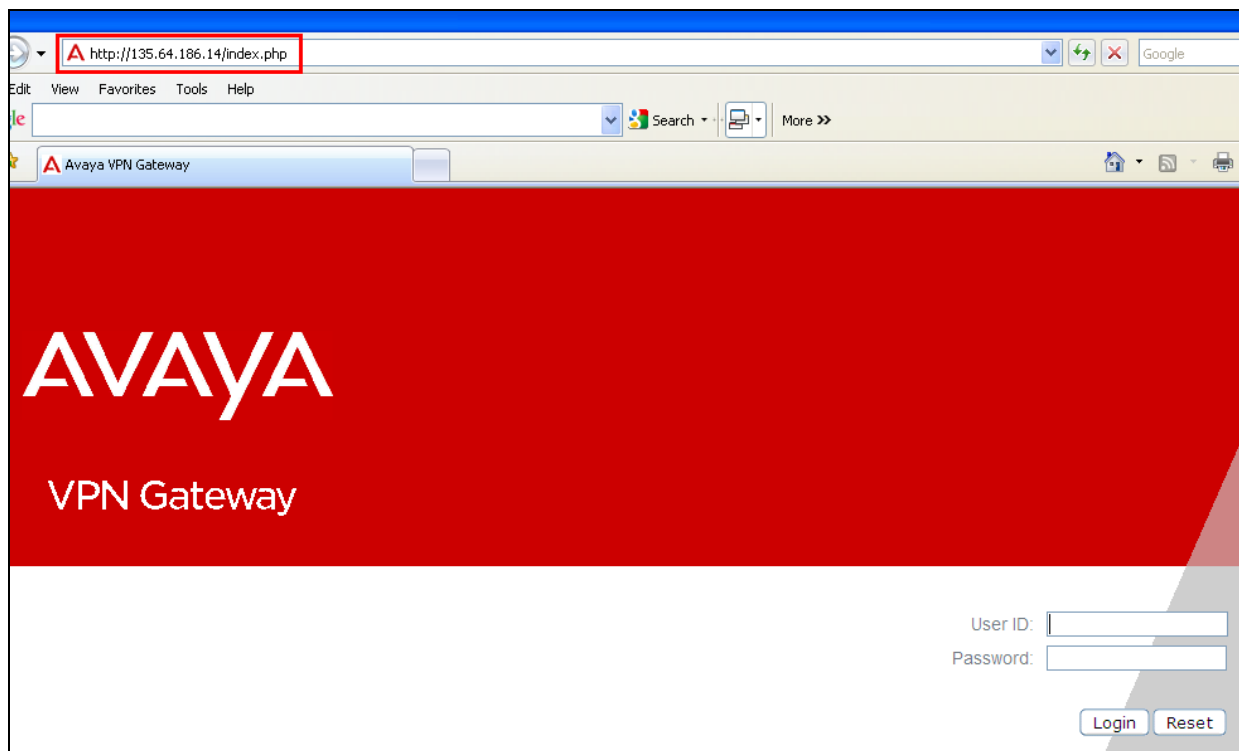
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

## 5. Administer Avaya VPN Gateway 3050

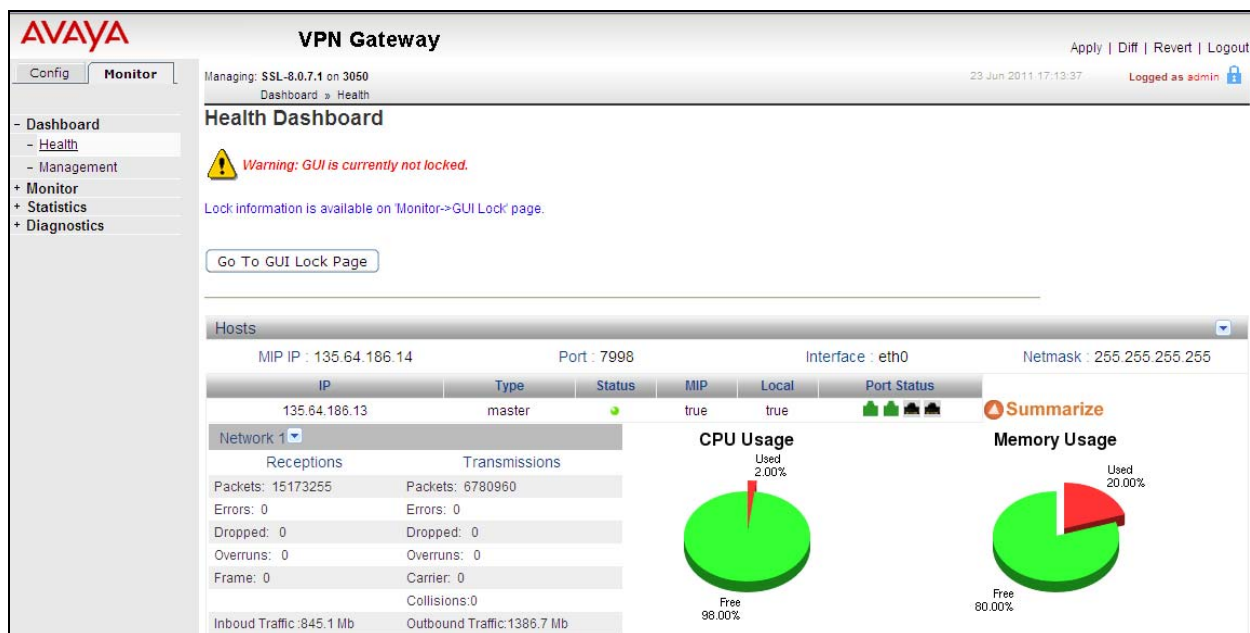
The following steps describe configuration of the VPN Gateway 3050. This section will describe the server configuration needed to establish a VPN IPSec tunnel between the remote user pc and VPN Gateway 3050. It will describe configuring an IP Pool, adding a User Tunnel Profile, administering an IKE Profile and configuring Split Tunneling to establish the VPN IPSec tunnel. For configuring the VPN Gateway in a two arm configuration, where interface One will be configured to handle the private traffic and interface Two will be configured to handle public traffic and setting up static routes, please refer to **Application Note for Configuring Remote User Access to one-X® Communicator H323 over a VPN SSL Net Direct Tunnel using the Avaya VPN Gateway 3050 Issue – 0.1**. It will also detail the creation of the IPSec VPN Gateway. It will also describe creating a Trusted Group and assigning the IP Pool to that Group. Administering of User Accounts is also discussed.

### 5.1. Access the Avaya VPN Gateway 3050

To access the VPN Gateway 3050 browse to the management IP Address. This was **<http://135.64.186.14>**. Input the User ID and password for the VPN Gateway 3050.



Upon login the following screen is displayed.



## 5.2. Administer IPsec Avaya VPN Gateway

To create the IPsec VPN Gateway select **Config → VPN Gateway** on the graphical user interface. Select the **Quick VPN** button.



AVAYA VPN Gateway

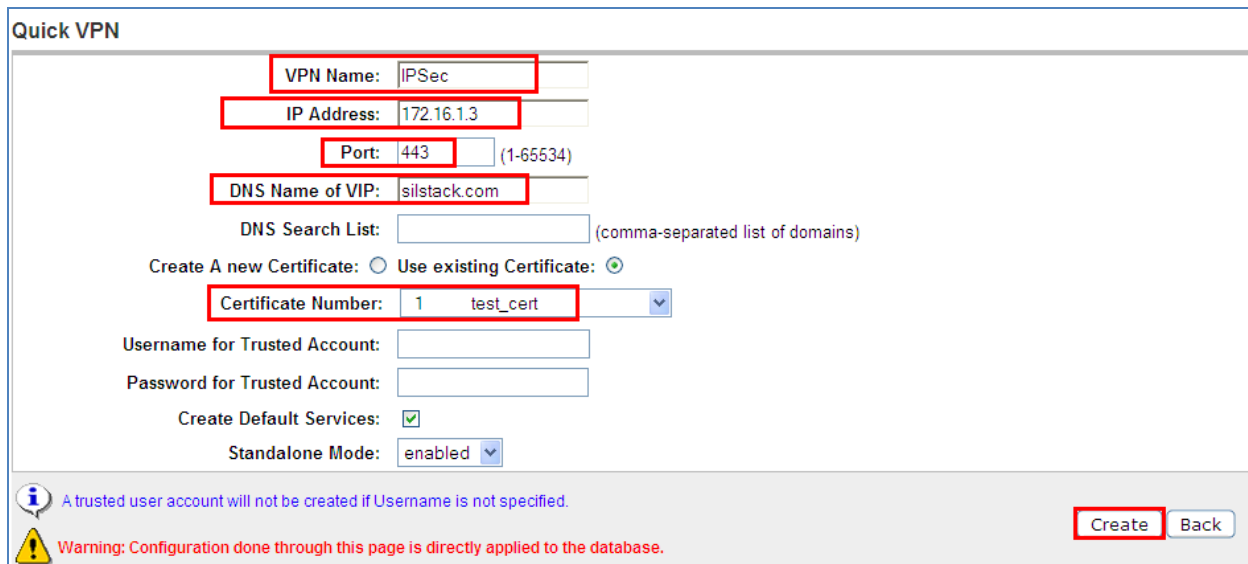
Managing: SSL-8.0.7.1 on 3050 28 Jun 2011 13:44:30

**VPN Gateways**

Lists the configured VPN(s) and also allows you to add, edit and delete VPN(s).

ID	Name	IP Address(es)	Port	SSL	IPsec
<input type="checkbox"/> 1	IPSec	172.16.1.3	443	Enabled	Enabled
<input type="checkbox"/> 2	SSL	172.16.1.6	443	Enabled	Disabled

The **VPN Name** was **IPSec**. The **IPsec VPN IP Address** was set to **172.16.1.3**. This is the IP Address the remote user will use to access the IPsec VPN tunnel with Avaya VPN client. The default **Port** number was **443**. The **DNS Name of VIP** was set to **silstack.com**. The **Certificate Number** was set to **test\_cert**. This is not crucial to the set up of the IPsec tunnel but needs to be assigned to the IPsec VPN Gateway to complete the changes. The **Create** button was selected to save the changes.



**Quick VPN**

VPN Name:

IP Address:

Port:  (1-65534)

DNS Name of VIP:

DNS Search List:  (comma-separated list of domains)

Create A new Certificate: ☐ Use existing Certificate: ☒


Certificate Number:

Username for Trusted Account:

Password for Trusted Account:

Create Default Services: ☒

Standalone Mode:

 Warning: Configuration done through this page is directly applied to the database.

Upon completion, the following screen is displayed.

The screenshot shows the AVAYA VPN Gateway configuration interface. The left sidebar contains a navigation menu with options like Wizards, Cluster Manager, Host(s), Certificates, SSL Offload Servers, Bandwidth Management, VPN Gateways, and Administration. The main content area is titled 'VPN Gateway' and shows a table of configured VPNs.

ID	Name	IP Address(es)	Port	SSL	IPsec
1	IPSec	172.16.1.3	443	Enabled	Enabled
2	SSL	172.16.1.6	443	Enabled	Disabled

### 5.3. Administer IP Pool

To administer the IP Pool select **Config** → **VPN Gateway** → **VPN 1**. Then under **Settings** select **IP Pool** on the graphical user interface.

The screenshot shows the AVAYA VPN Gateway configuration interface, specifically the 'VPN Summary' page for 'VPN-1'. The left sidebar is the same as the previous screenshot. The main content area shows the 'VPN Summary' for 'VPN-1' with various settings.

Settings	Configuration
General	VPN Name : IPSec, Standalone Mode is enabled, WholeSecurity is off.
SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is SILStackCA.....
Traffic Trace	Lets you traceroute or ping a host.
IP Pool	Default IP Pool is 1, The configured IP Pools are Stack
Host IP Pool	Host IP Pool is disabled

Under the IP Pool list select the **ADD** button.

The screenshot shows the AVAYA VPN Gateway configuration interface, specifically the 'IP Pool' configuration page for 'VPN-1'. The left sidebar is the same as the previous screenshots. The main content area shows the 'IP Pool' configuration.

Default IP Pool: 1 Stack (None indicates that no IP Pool will be used by default)

The IP Pool menu is used to configure the desired method for assigning IP address and network attributes to VPN clients. The IP pool comes into play when a user attempts to access a host using an IPsec VPN client (formerly the Nortel VPN client) or Net Direct client connection. The IP address is used as a new source IP for the VPN Gateway and the destination host, once the remote user is authenticated and the VPN tunnel is set up.

**IP Pool List**

ID	Name	Type	Proxy ARP	Status
1	Stack	local	on	on



For the IPsec VPN Gateway **VPN 1**. The IP Pool **Name** was set to **Stack**. The **Status** was **enabled**. The **Type** was set to **local** and **Proxy ARP** was set to **on**. The **Update** button was selected to save the changes.

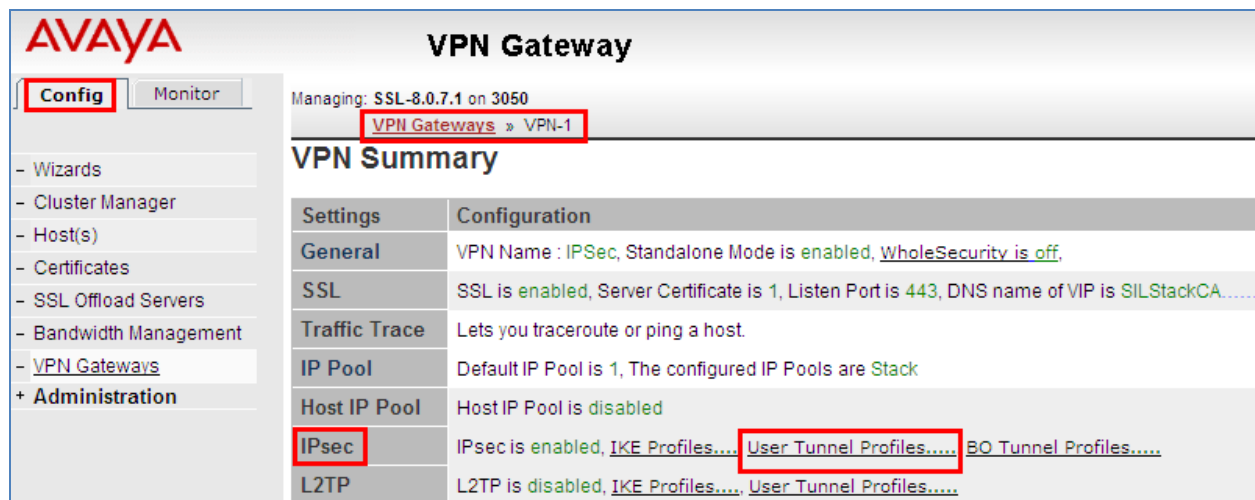
The screenshot shows the Avaya VPN Gateway configuration interface. The left sidebar contains a navigation menu with options like Wizards, Cluster Manager, Host(s), Certificates, SSL Offload Servers, Bandwidth Management, VPN Gateways, and Administration. The main content area is titled 'VPN Gateway' and shows the breadcrumb path: 'Managing: SSL-8.0.7.1 on 3050' > 'VPN Gateways' > 'VPN-1' > 'IP Pool-'. The 'Add/Modify' button is visible. The 'IP Pool Configuration' section is active, showing 'Add new IP Address Pool'. The configuration fields are: VPN: 1, IP Pool ID: 2, Name: Stack, Status: enabled, Type: local, and Proxy ARP: on. The 'Update' and 'Back' buttons are at the bottom right.

Under the **General Settings** of the IP Pool named **Stack**. The **Lower IP** address was set to **10.10.97.2** and the **Upper IP** address was set to **10.10.97.20**. The **Update** button was selected to save the changes.

The screenshot shows the 'Modify IP Address Pool' page for the IP Pool named 'Stack'. The 'General' tab is selected, and the 'General Settings' section is highlighted. The configuration fields are: Name: Stack, Status: enabled, Type: local, Proxy ARP: on, Lower IP: 10.10.97.2, and Upper IP: 10.10.97.20. The 'Update' and 'Back' buttons are at the bottom right.

## 5.4. Add User Tunnel Profile

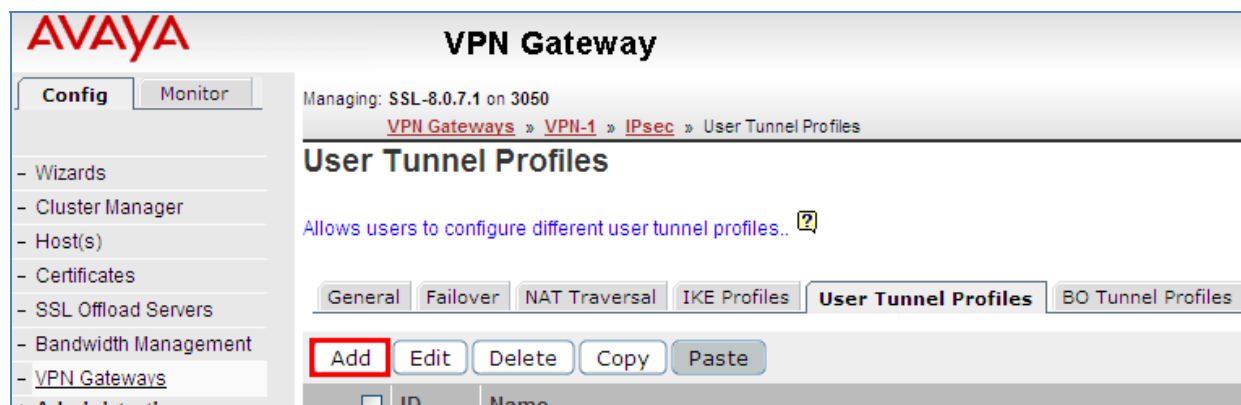
Under the **Config** → **VPN Gateway** → **VPN 1** then under **Settings** for **IPSec** choose **User Tunnel Profile** option.



The screenshot shows the Avaya VPN Gateway configuration interface. The left sidebar contains a menu with options like Wizards, Cluster Manager, Host(s), Certificates, SSL Offload Servers, Bandwidth Management, VPN Gateways, and Administration. The main area is titled 'VPN Gateway' and shows the configuration for 'VPN-1'. A table titled 'VPN Summary' lists various settings and their configurations. The 'IPsec' row is highlighted with a red box, and the 'User Tunnel Profiles....' link within that row is also highlighted with a red box.

Settings	Configuration
General	VPN Name : IPSec, Standalone Mode is <b>enabled</b> , <b>WholeSecurity</b> is <b>off</b> ,
SSL	SSL is <b>enabled</b> , Server Certificate is 1, Listen Port is 443, DNS name of VIP is SILStackCA.....
Traffic Trace	Lets you traceroute or ping a host.
IP Pool	Default IP Pool is 1, The configured IP Pools are Stack
Host IP Pool	Host IP Pool is <b>disabled</b>
<b>IPsec</b>	IPsec is <b>enabled</b> , IKE Profiles.... <b>User Tunnel Profiles....</b> BO Tunnel Profiles....
L2TP	L2TP is <b>disabled</b> , IKE Profiles.... User Tunnel Profiles....

Under User Tunnel Profiles select the **ADD** button.



The screenshot shows the Avaya VPN Gateway configuration interface, specifically the 'User Tunnel Profiles' section. The left sidebar is the same as in the previous screenshot. The main area is titled 'User Tunnel Profiles' and includes a description: 'Allows users to configure different user tunnel profiles..'. Below this, there are tabs for General, Failover, NAT Traversal, IKE Profiles, User Tunnel Profiles, and BO Tunnel Profiles. The 'User Tunnel Profiles' tab is selected. Below the tabs, there are buttons for Add, Edit, Delete, Copy, and Paste. The 'Add' button is highlighted with a red box.

Under **User Tunnel Profile Configuration** for **VPN 1** the User Tunnel Profile called **Stack** was added. The **Update** button was selected to save the changes.

**AVAYA VPN Gateway**

Managing: SSL-8.0.7.1 on 3050

28 Jun 2011 15:17:34 Logged as admin

**User Tunnel Profile Configuration**

General user tunnel configuration for specific user tunnel profile.. [?]

User Tunnel Profiles List **General** Auto Connection Client PC Control Split Tunnels Client Policy Rules Mobility

**Add New User Tunnel Profile**

VPN: 1  
Id: 2  
Name: Stack

**Update** Back

Upon completion, the following screenshot is displayed.

**AVAYA VPN Gateway**

Managing: SSL-8.0.7.1 on 3050

VPN Gateways » VPN-1 » IPsec » User Tunnel Profiles

**User Tunnel Profiles**

Allows users to configure different user tunnel profiles.. [?]

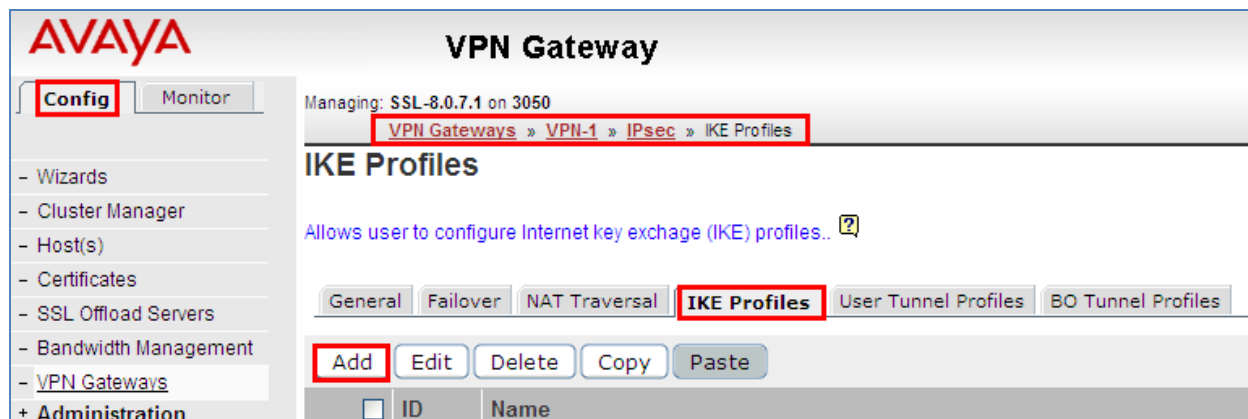
General Failover NAT Traversal IKE Profiles **User Tunnel Profiles** BO Tunnel Profiles

Add Edit Delete Copy Paste

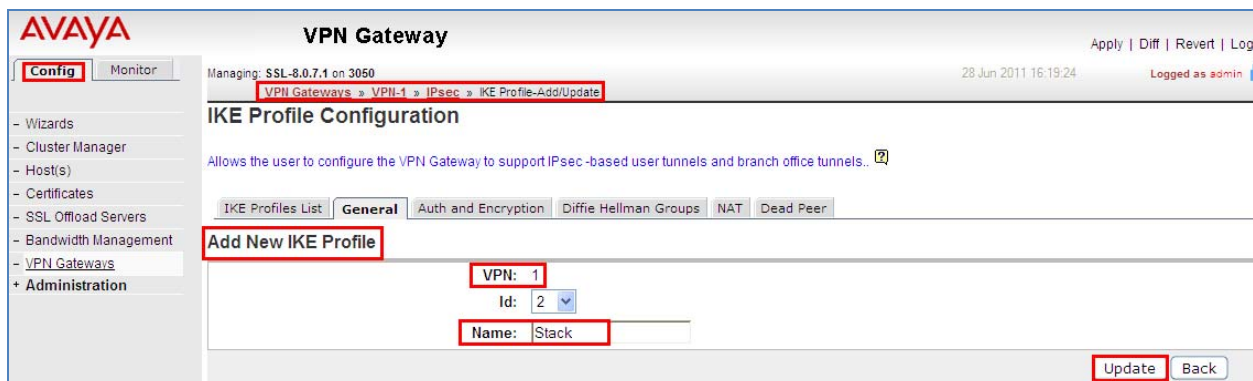
<input type="checkbox"/>	ID	Name
<input type="checkbox"/>	1	Stack

## 5.5. Administer IKE Profiles

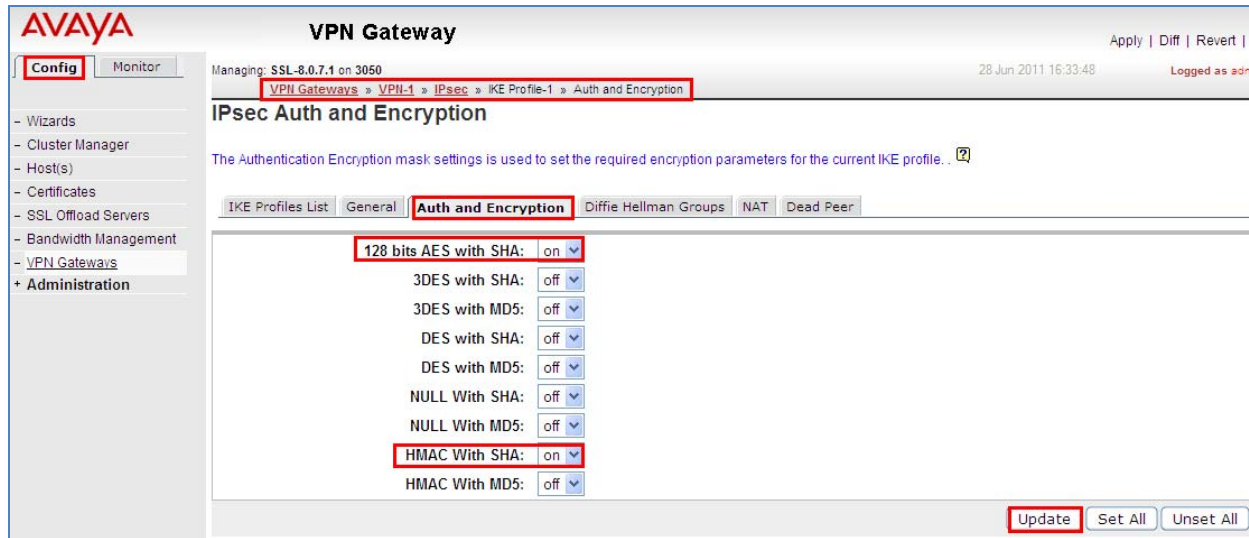
To administer an IKE Profile select **Config** → **VPN Gateways** → **VPN 1** → **IPSec**. Then select **IKE Profile**. To add a new IKE Profile select the **ADD** button.



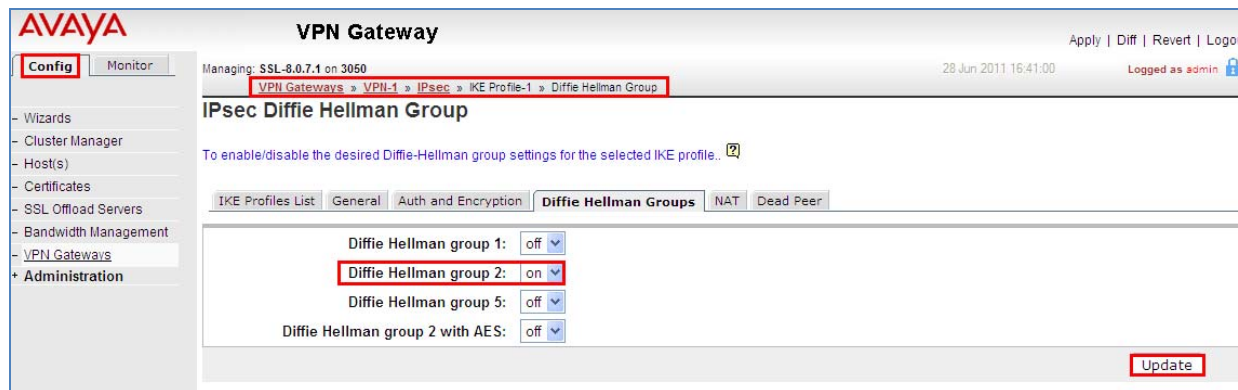
A new **IKE Profile** called **Stack** was added for **VPN 1**. The **Update** button was selected to save the changes.



To administer **Auth and Encryption** select **Config → VPN Gateways → VPN 1 → IPsec → IKE Profile 1 → Auth and Encryption**. The **128 bits AES with SHA** was set to **on** and **HMAC with SHA** was set to **on**. The **Update** button was selected to save the changes.



To administer Diffie Hellman group 2 select **Config → VPN Gateways → VPN 1 → IPsec → IKE Profile 1 → Diffie Hellman Group**. The **Diffie Hellman group 2** was set to **on**. The **Update** button was selected to save the changes.



To disable NAT select **Config → VPN Gateways → VPN 1 → IPSec → NAT Traversal**. The **NAT Traversal Status** was **disabled**. The **Update** button was selected to save the changes.

The screenshot shows the Avaya VPN Gateway configuration interface. The left sidebar contains a menu with options like Wizards, Cluster Manager, Host(s), Certificates, SSL Offload Servers, Bandwidth Management, VPN Gateways, and Administration. The main content area is titled 'VPN Gateway' and shows the configuration path: 'VPN Gateways > VPN-1 > IPsec > NAT Traversal'. The 'NAT Traversal' tab is selected, and the 'NAT Traversal Status' is set to 'disabled'. Other settings include 'UDP Port: 10001' and 'Client IKE Source Port Switching: disabled'. An 'Update' button is located at the bottom right of the configuration area.

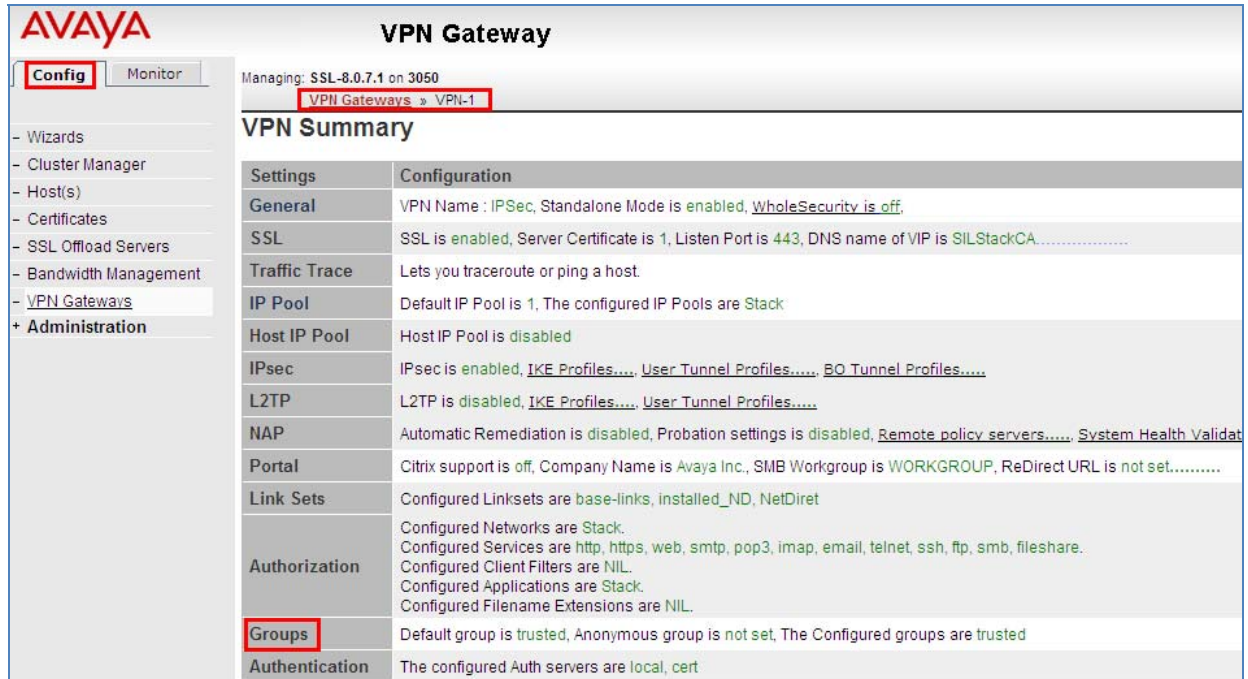
## 5.6. Administer Split Tunnel

To administer Split Tunnel Mode select **Config → VPN Gateways → VPN 1 → IPSec → User Tunnel Profile 1 → Split Tunnels**. The **Split Tunnel Mode** was **disabled**. The **Update** button was selected to save the changes.

The screenshot shows the Avaya VPN Gateway configuration interface for Split Tunnels. The left sidebar is the same as the previous screenshot. The main content area is titled 'VPN Gateway' and shows the configuration path: 'VPN Gateways > VPN-1 > IPsec > User Tunnel Profile-1 > Split Tunnels'. The 'Split Tunnels' tab is selected, and the 'Split Tunnel Mode' is set to 'disabled'. An 'Update' button is located at the bottom right of the configuration area. Below the configuration area, there is a section titled 'Split Tunnel Network List'.

## 5.7. Administer Trusted Group

To administer a Trusted Group select **Config** → **VPN Gateway** → **VPN 1**. Then under settings select **Groups** on the graphical user interface.



**AVAYA** **VPN Gateway**

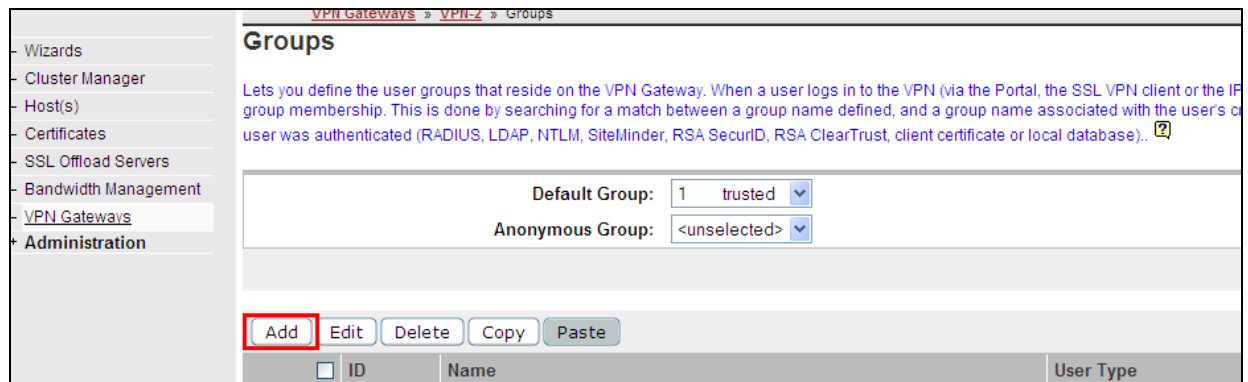
Managing: SSL-8.0.7.1 on 3050

**VPN Gateways** » **VPN-1**

**VPN Summary**

Settings	Configuration
General	VPN Name : IPSec, Standalone Mode is <b>enabled</b> , WholeSecurity is <b>off</b> .
SSL	SSL is <b>enabled</b> , Server Certificate is 1, Listen Port is 443, DNS name of VIP is SILStackCA.....
Traffic Trace	Lets you traceroute or ping a host.
IP Pool	Default IP Pool is 1, The configured IP Pools are Stack
Host IP Pool	Host IP Pool is disabled
IPsec	IPsec is <b>enabled</b> , IKE Profiles..., User Tunnel Profiles..., BO Tunnel Profiles....
L2TP	L2TP is <b>disabled</b> , IKE Profiles..., User Tunnel Profiles....
NAP	Automatic Remediation is <b>disabled</b> , Probation settings is <b>disabled</b> , Remote policy servers..., System Health Validat
Portal	Citrix support is <b>off</b> , Company Name is Avaya Inc., SMB Workgroup is WORKGROUP, ReDirect URL is not set.....
Link Sets	Configured Linksets are base-links, installed_ND, NetDirect
Authorization	Configured Networks are Stack. Configured Services are http, https, web, smtp, pop3, imap, email, telnet, ssh, ftp, smb, fileshare. Configured Client Filters are NIL. Configured Applications are Stack. Configured Filename Extensions are NIL.
<b>Groups</b>	Default group is <b>trusted</b> , Anonymous group is <b>not set</b> , The Configured groups are <b>trusted</b>
Authentication	The configured Auth servers are local, cert

Select the **Add** button under Groups



**VPN Gateways** » **VPN-1** » **Groups**

**Groups**

Lets you define the user groups that reside on the VPN Gateway. When a user logs in to the VPN (via the Portal, the SSL VPN client or the IP group membership. This is done by searching for a match between a group name defined, and a group name associated with the user's c user was authenticated (RADIUS, LDAP, NTLM, SiteMinder, RSA SecurID, RSA ClearTrust, client certificate or local database).. ?

Default Group: 1 trusted

Anonymous Group: <unselected>

**Add** Edit Delete Copy Paste

ID	Name	User Type
----	------	-----------



Under the **Add a Group** the Group **Name** was set to **trusted**. The **User Type** was set to **advanced**. The **Update** button was selected.

The screenshot shows the 'Add a Group' form for VPN 2. The form includes fields for 'Name' (set to 'trusted'), 'User Type' (set to 'advanced'), and 'Comment'. The 'Update' button is highlighted in red.

VPN Gateways » VPN-2 » Groups » Add

**Add a Group**

Add New Group to VPN 2

VPN: 2  
Id: 2  
Name: trusted  
User Type: advanced  
Comment:

Update Back

The following **trusted** group was added.

The screenshot shows a table with columns: ID, Name, User Type, and Comment. The first row is highlighted with a red box, showing ID 1, Name 'trusted', and User Type 'advanced'.

ID	Name	User Type	Comment
1	trusted	advanced	

After selecting the group named **trusted** the following page is displayed. The **IP Pool** called **Stack** created in **Section 5.3** was assigned to the group named **trusted**. The **Update** button was selected to save the changes.

The screenshot shows the configuration page for the 'trusted' group. The 'IP Pool' is set to 'Stack'. The 'Update' button is highlighted in red.

General Access Lists Linksets EACA IPsec L2tp VPN Admin Net Direct Mobility Extended Profiles SPO

Name: trusted  
User Type: advanced  
Bandwidth policy: <None>  
Net Direct Windows Admin User Name:  
Net Direct Windows Admin Password:  
Net Direct Windows Admin Password (again):  
IP Pool: 1 Stack  
Host IP Pool: <None>  
Maximum Sessions: 0 (0 is unlimited)  
Session Idle Time: 0 (seconds)  
Maximum Session Length: 0 (seconds)  
Comment:

Update



## 5.8. Administer User Authentication

To administer an Authentication Account select **Config** → **VPN Gateway** → **VPN 1**. Then under **Settings**, select **Authentication** on the graphical user interface.

The screenshot shows the Avaya VPN Gateway configuration interface. The left sidebar contains a navigation menu with options like Wizards, Cluster Manager, Host(s), Certificates, SSL Offload Servers, Bandwidth Management, VPN Gateways, and Administration. The main area is titled 'VPN Gateway' and shows the configuration for 'VPN-1'. The 'Authentication' tab is selected, displaying a table of authentication settings.

Settings	Configuration
General	VPN Name : IPSec, Standalone Mode is enabled, <u>WholeSecurity is off</u> .
SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is SILStackCA.....
Traffic Trace	Lets you traceroute or ping a host
IP Pool	Default IP Pool is 1, The configured IP Pools are Stack
Host IP Pool	Host IP Pool is disabled
IPsec	IPsec is enabled, <u>IKE Profiles.....</u> , <u>User Tunnel Profiles.....</u> , <u>BO Tunnel Profiles.....</u>
L2TP	L2TP is disabled, <u>IKE Profiles.....</u> , <u>User Tunnel Profiles.....</u>
NAP	Automatic Remediation is disabled, Probation settings is disabled, <u>Remote policy servers.....</u> , <u>System Health Validator.....</u>
Portal	Citrix support is off, Company Name is Avaya Inc., SMB Workgroup is WORKGROUP, ReDirect URL is not set.....
Link Sets	Configured Linksets are base-links, installed_ND, NetDiret
Authorization	Configured Networks are Stack. Configured Services are http, https, web, smtp, pop3, imap, email, telnet, ssh, ftp, smb, fileshare. Configured Client Filters are NIL. Configured Applications are Stack. Configured Filename Extensions are NIL.
Groups	Default group is trusted, Anonymous group is not set, The Configured groups are trusted
Authentication	The configured Auth servers are local, cert

Select the Authentication Server called **local** that was defined on the Avaya VPN Gateway 3050 after installation.

The screenshot shows the 'Authentication Servers' configuration page. It includes a table with columns for ID, Name, Display Name, and Domain Name. The 'local' server is highlighted with a red box.

<input type="checkbox"/>	ID	Name	Display Name	Domain Name
<input type="checkbox"/>	1	local		
<input type="checkbox"/>	2	cert	Not applicable	ssl.silstack.com

Select the **Add** option under **Config → VPN Gateways → VPN 1 → Auth Server 1(Local) → User**.

The screenshot shows the Avaya VPN Gateway configuration interface. The top navigation bar includes 'Config' and 'Monitor' tabs. The left sidebar lists various configuration options, with 'VPN Gateways' and 'Administration' highlighted. The main content area is titled 'VPN Gateway' and shows the breadcrumb path: 'VPN Gateways > VPN-1 > Auth Server-1 [Local] > Users'. The 'Users' section is active, displaying a list of users and an 'Add' button. The 'Add' button is highlighted with a red box.

The User Name called **Stack** was added and the **Password** for the user. The **trusted** Group was selected. The **Save User** button was selected to save the changes.

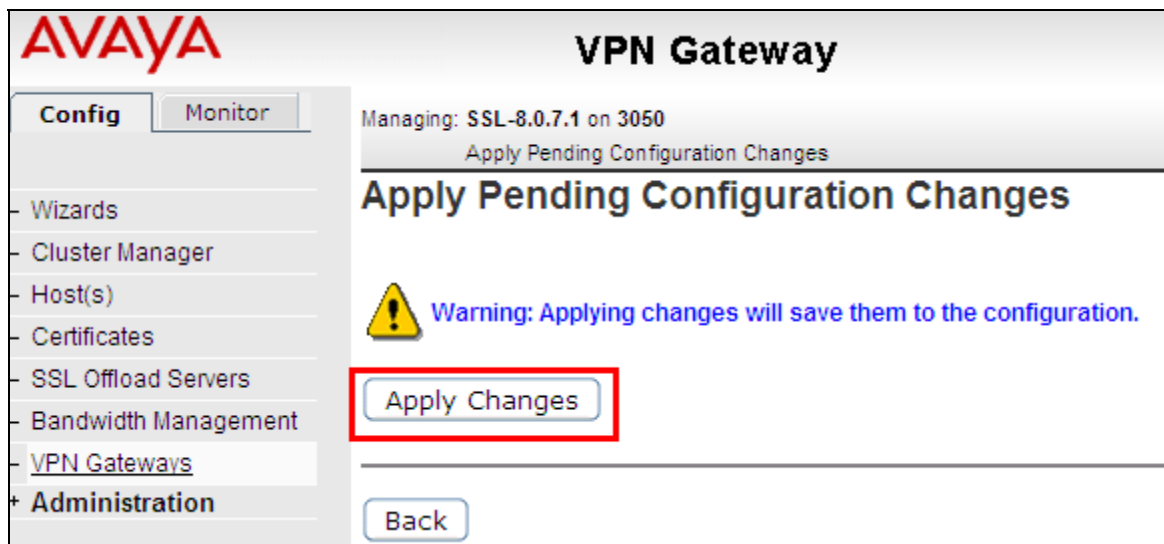
The screenshot shows the 'Add Single User' form in the Avaya VPN Gateway configuration interface. The form includes fields for 'Name' (Stack), 'Password' (masked with dots), and 'Password (again)' (masked with dots). Below these fields is a 'Groups' section with a list of available groups. The 'trusted' group is selected and highlighted with a red box. At the bottom of the form, there is a 'Save User' button, which is also highlighted with a red box. A warning message at the bottom states: 'Warning: Users are added immediately to the database. No apply is required.'

## 5.9. Apply Changes

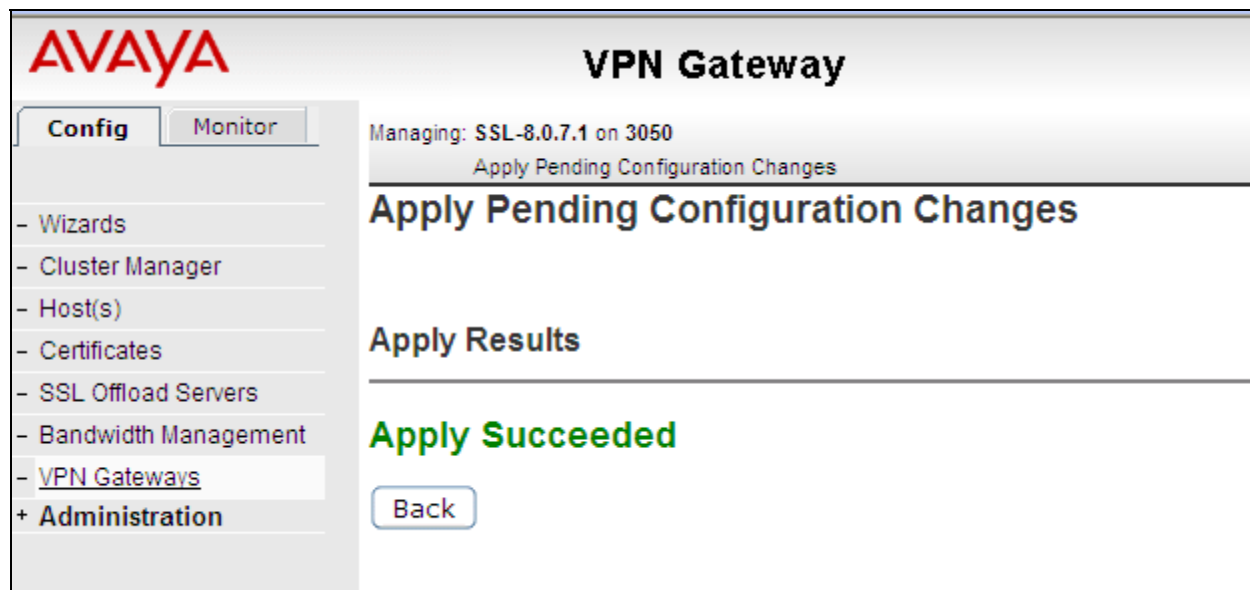
For the changes to take effect on the Avaya VPN Gateway 3050 select the **Apply** button on the top right hand side of the graphical user interface.



Select the **Apply Changes** button.



The following screenshot shows the changes were successful.

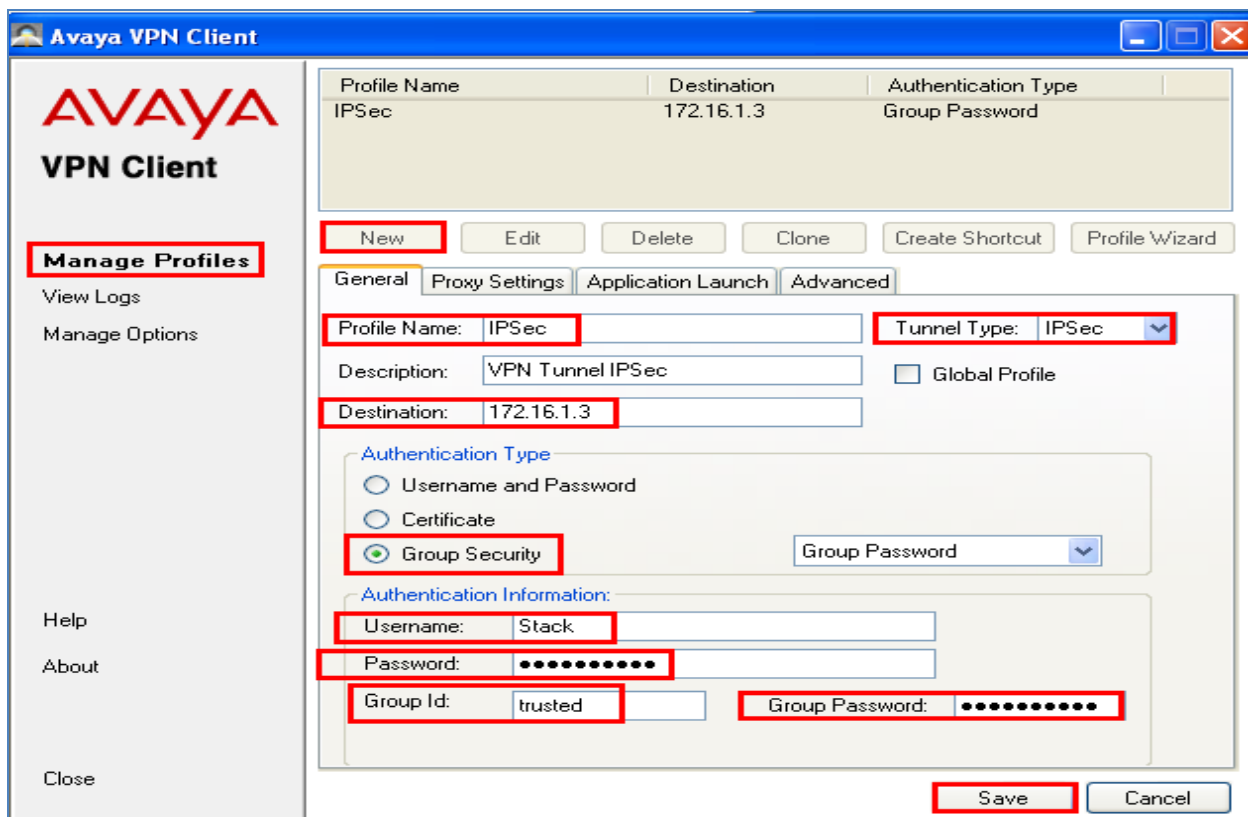


## 6. Avaya VPN Client Settings

The following section describes the setting needed to administer the VPN Client. Open the VPN Client and select the **Edit the profile** heading.

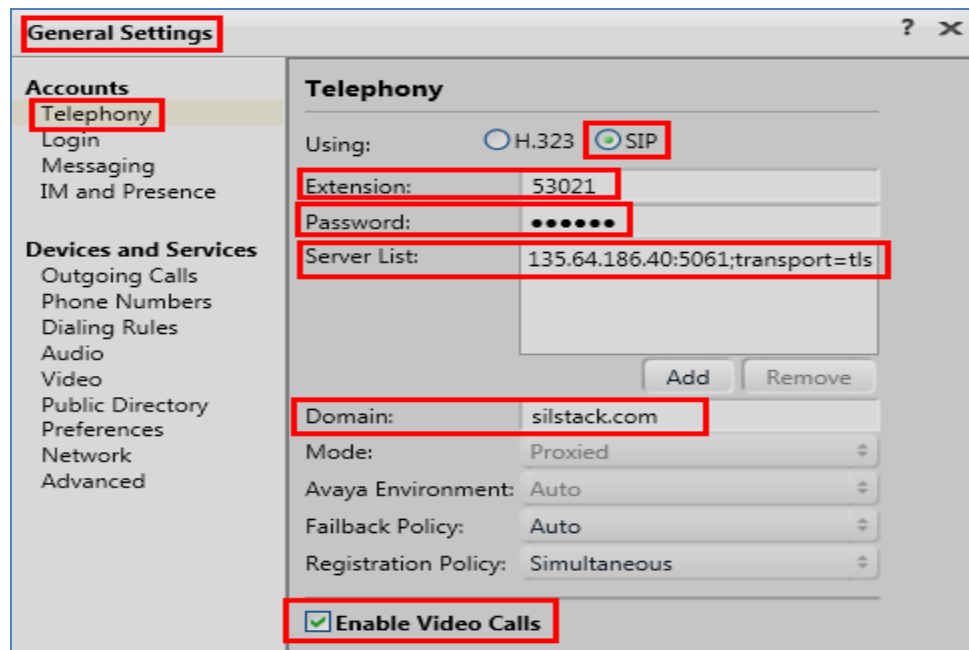


The following screen is displayed. The **Manage Profiles** heading was selected. The **New** button was selected. The **Profile Name** was set to **IPSec**. The **Tunnel Type** was set to **IPSec**. The **Destination** was set to **172.16.1.3** (the IPSec VPN Gateway IP Address administered in **Section 5.2**). In **Authentication Type** the **Group Security** option was enabled. Under **Authentication Information** the **Username** was set to **Stack** and the **Password** was set to match the User Authentication administered in **Section 5.8**. The **Group Id** was set to **trusted** to match the Group trusted name administered in **Section 5.7**. Since the User Authentication was assigned to the Trusted Group, the **Group Password** was the same as the User Authentication password administered in **Section 5.8**. The **Save** button was selected.

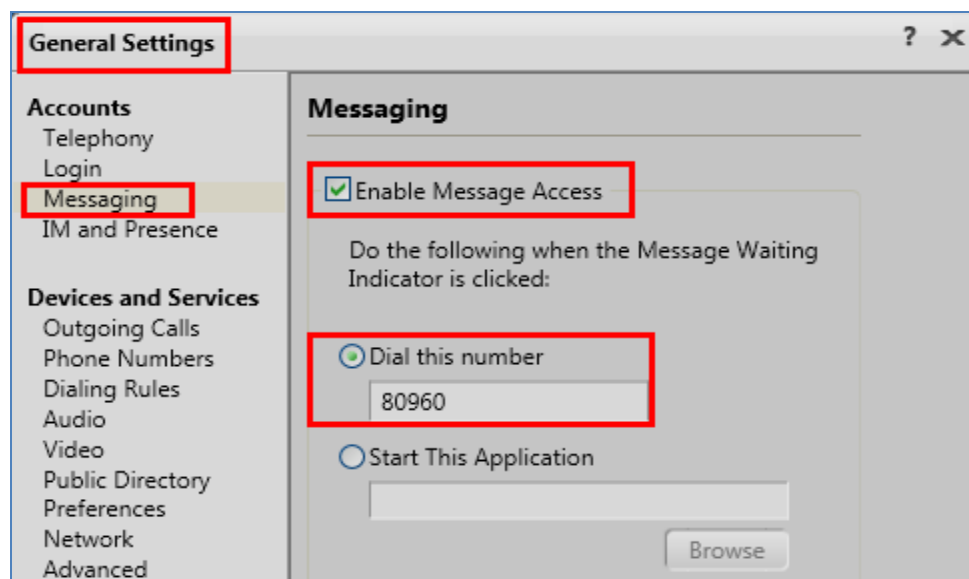


## 7. Avaya one-X® Communicator SIP Settings

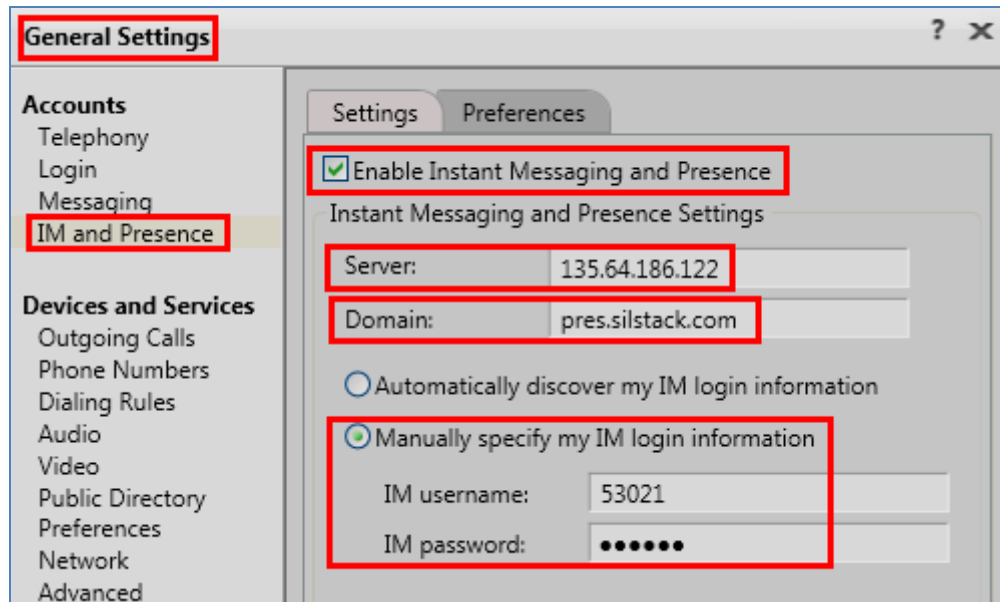
The following section describes the settings needed to administer one-X Communicator SIP soft client. On the one-X Communicator SIP soft client select **General Settings**. Under **Telephony** the **SIP** option was enabled. The **Extension** was set to **53021**. The **Password** was set and the **Server list** was set to **135.64.186.40**. This is the IP Address of the SIP Signalling Server. The **port** was set to **5061** using **TLS**. The **Domain** was set to **silstack.com**. The **Enable Video Calls** was also selected



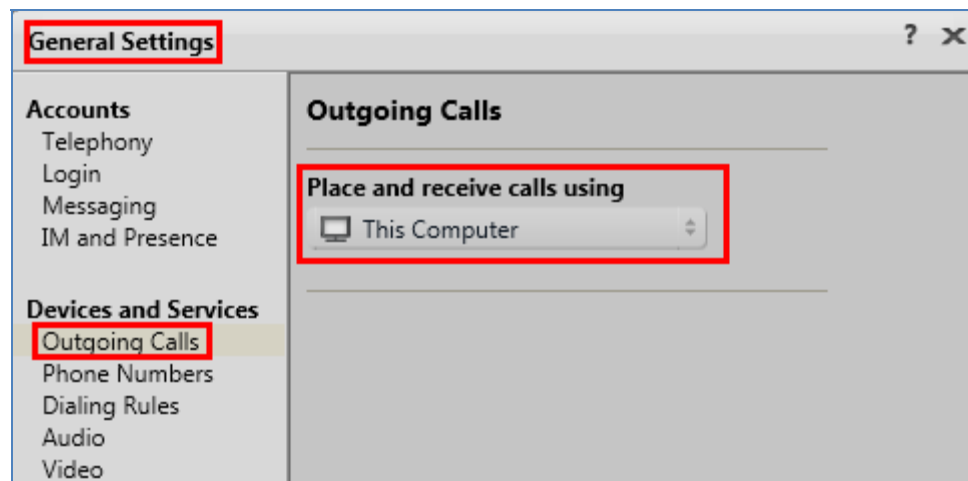
Under **General Settings** the **Messaging** option was selected. The **Enable Message Access** was selected and the **Dial this number** was set to **80960** the hunt group number of the voicemail.



Under **General Settings** the **IM and Presence** option was selected. The **Enable Instant Messaging and Presence** was selected. The **Server** was set to **135.64.186.122**, the IP Address of the Presence Server and the **Domain** was set to **pres.silstack.com**. The **Manually specify my IM login information** was enabled. The **IM username** was set to **53021** and **IM password** was set.



Under **General Settings** the **Outgoing Calls** option was selected. The **Place and receive calls using** option was set to **This Computer**.



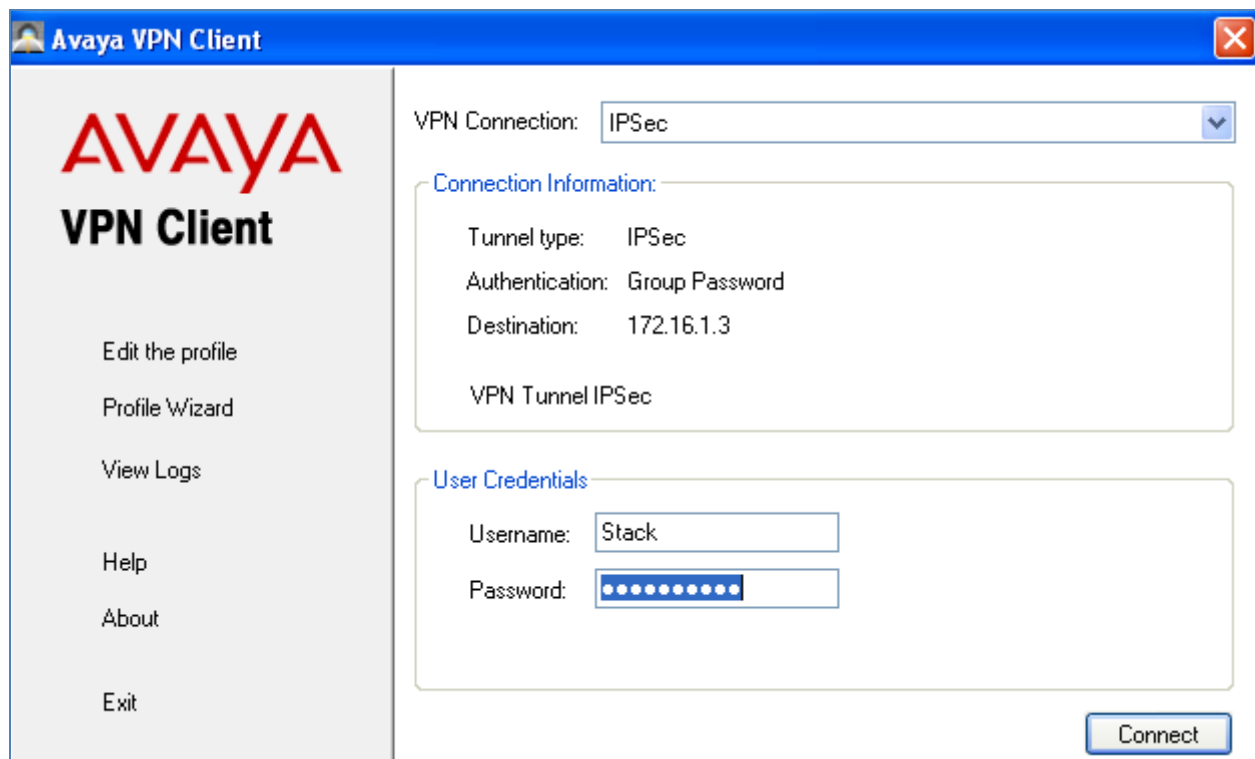
## 8. Verification Steps

The following six verification steps were tested using the sample configuration. The following steps can be used to verify installation in the field.

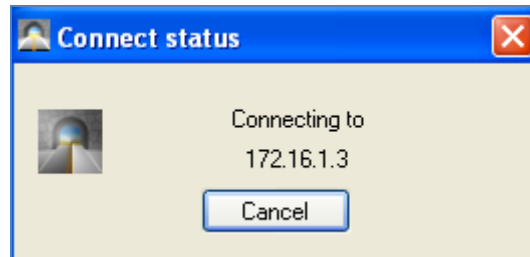
1. Verified the IPsec VPN Tunnel is connected from the remote user pc to the VPN Gateway 3050.
2. Verified one-X Communicator SIP extension 53021 is registered to Session Manager while the IPsec VPN Tunnel is connected.
3. Verified one-X Communicator SIP extension 53021 is able to make a Video Call while the IPsec VPN Tunnel is connected.
4. Verified that a message could be left for one-X Communicator SIP extension 53021 and that the message waiting indicator turned on while the IPsec VPN Tunnel is connected.
5. Verified that Presence information is seen on one-X Communicator SIP extension 53021 while the IPsec VPN Tunnel is connected.
6. Verified that an Instant Messaging is sent from one-X Communicator SIP extension 53021 while the IPsec VPN Tunnel is connected

### 8.1. Verify Access and Connection to IPsec VPN Tunnel

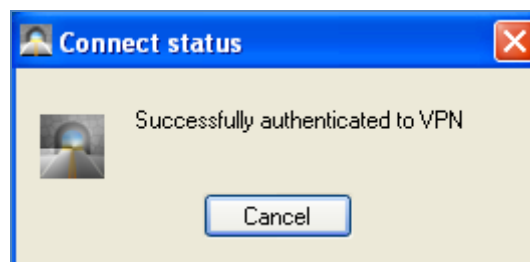
The remote user accesses the IPsec VPN Tunnel by connecting to the IPsec Gateway 172.16.1.3, configured in **Section 5.2**, with VPN client software. The remote user enters the Authentication User account administered in **Section 5.8** and selects the **Connect** button.



The following screenshot shows the remote user attempting to connect to the IPsec VPN Tunnel.



The following screenshot shows the remote user successfully authenticated to the IPsec VPN Tunnel





The following screenshot shows a Status of the IPSec VPN Tunnel while connected.



The ipconfig command was run from the command line of DOS on the remote user pc.

```
C:\ Command Prompt

C:\Documents and Settings\administrator.SILSTACK.000>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : SSG5-Serial-WLAN
    IP Address. . . . . : 192.168.1.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter {E84D4957-93C9-40A0-8AFD-9C5A7B7451BD}:

    Connection-specific DNS Suffix  . : silstack.com
    IP Address. . . . . : 10.10.97.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.97.5

Ethernet adapter {030DB429-4FC2-4839-92EE-3971162EADA}:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\administrator.SILSTACK.000>
```

An additional status of the IPSec VPN Tunnel is completed from the VPN Gateway 3050. Under the heading **Monitor** select the subheading **IPSecUser**

Managing: SSL-8.0.7.1 on 3050  
29 Jun 2011 11:19:43  
Logged as admin

**Monitor** | Monitor » Ipssec Sessions

### IPsec Users

Provides information about the current IPsec sessions. [Refresh](#)

VPN:   
Prefix:

[List](#)

**IPsec Users**

Number of Active IPsec Sessions: 2

VPN	User:TunnelProfile	IP Inner/Outer	Encrypted	Decrypted	Time
1	Stack:Stack	10.10.97.5/172.16.1.10	138	80	00:07:23
1	Stack:Stack	10.10.97.7/172.16.1.10	2	2	6 days

## 8.2. Verify Avaya one-X® Communicator SIP Registered to Avaya Aura® Session Manager

Select **Session Manager** → **System Status** → **User Reaistration**. The following screenshot shows one-X Communicator SIP extension 53021 registered to Session Manager..

Device and Location Configuration

Application Configuration

System Status

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

Registration Summary

User Registrations

SIP Performance

System Performance

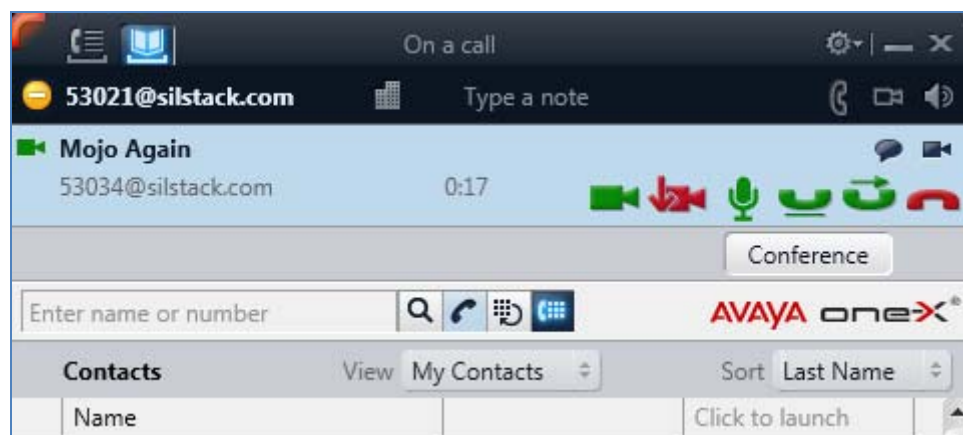
System Tools

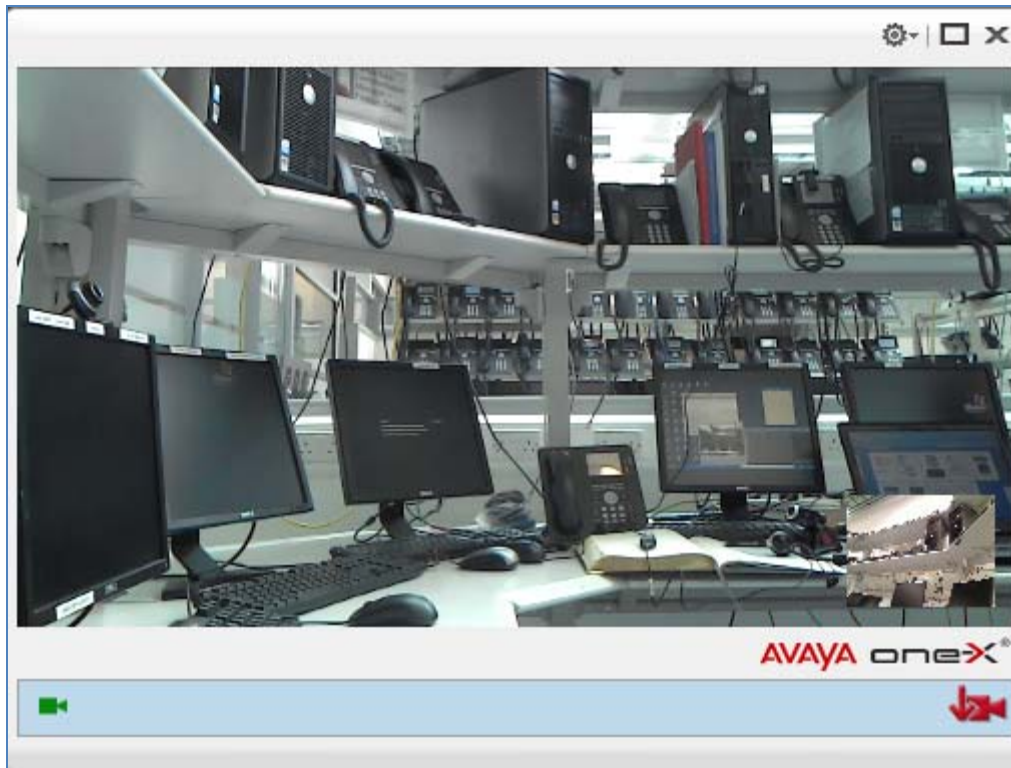
16 Items Refresh Show 15 Filter: Enable

<input type="checkbox"/>	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered		
									Prim	Sec	Sup
<input type="checkbox"/>	➤ Show	53012@silstack.com	53012@silstack.com	phone	sip	Galway Stack	135.64.186.204:5060	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	➤ Show	---	53011@silstack.com	phone	sip	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	➤ Show	---	53040@silstack.com	mojo	wireless CHES	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	➤ Show	---	53099@silstack.com	Mojo	Wireless	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	➤ Show	34007@silstack.com	34007@silstack.com	another	try	Galway Stack	135.64.186.254:5061	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	➤ Show	---	53015@silstack.com	sip	9608	VPN	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	➤ Show	53014@silstack.com	53014@silstack.com	9608	sip	Galway Stack	10.10.99.26:5060	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	➤ Show	53034@silstack.com	53034@silstack.com	Mojo	Again	Galway Stack	135.64.186.252:5061	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	➤ Show	---	34009@silstack.com	CMFS	9641	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	➤ Show	---	34003@silstack.com	sip	oneXportal	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	➤ Show	34010@silstack.com	34010@silstack.com	CMFS	34010	Galway Stack	10.10.99.39:5061	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	➤ Show	---	34002@silstack.com	onexPortal	onexces	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	➤ Show	---	34008@silstack.com	CMFS	try	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	➤ Show	---	53019@silstack.com	IPSec	VPN	VPN	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	➤ Show	53021@silstack.com	53021@silstack.com	User	1XC	Galway Stack	10.10.97.5:5061	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## 8.3. Verify Video using Avaya one-X® Communicator SIP

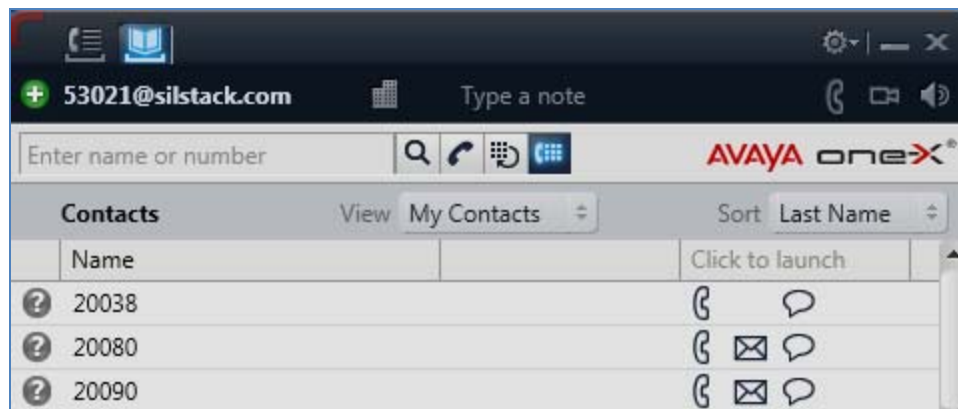
The following screenshots show a successful **Video Call** made from **one-X Communicator SIP** extension **53021** to another video endpoint, while the IPSec VPN Tunnel is connected.



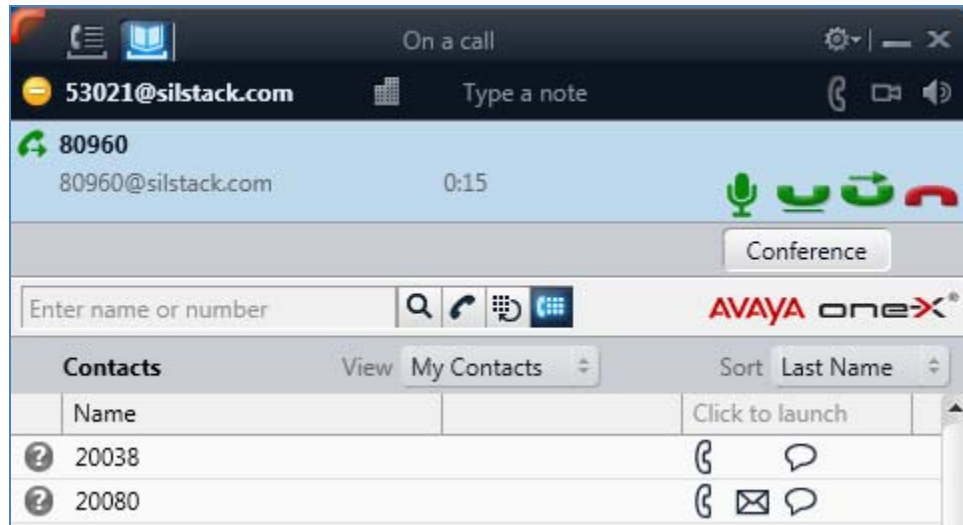


#### 8.4. Verify MWI using Avaya one-X®Communicator SIP

The following screenshot shows the one-X Communicator SIP extension 53021 message waiting indicator off while the IPsec VPN Tunnel is connected.

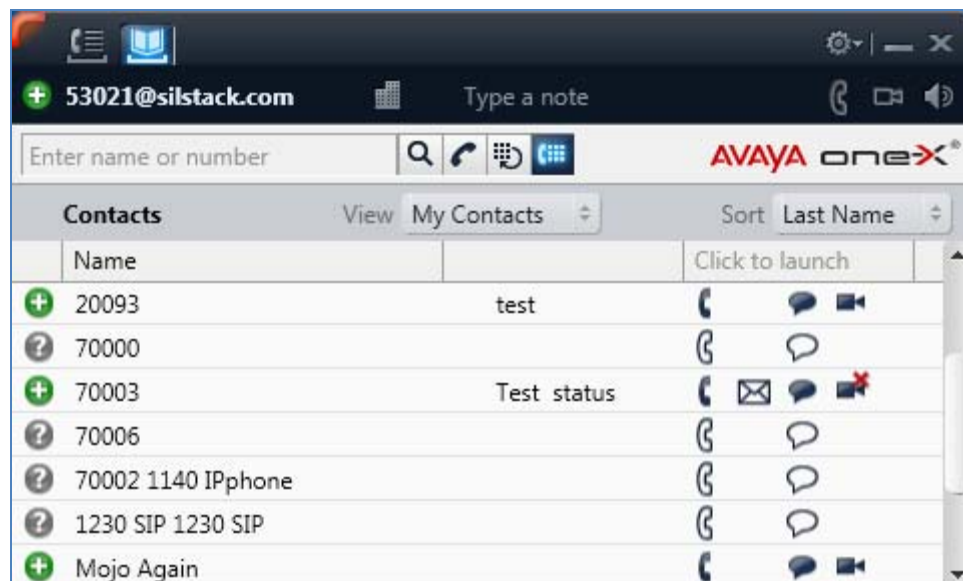


The following screenshot shows that a message can be left with the one-X Communicator SIP extension 53021 and that the message waiting indicator was turned on while the IPSecVPN Tunnel is connected.

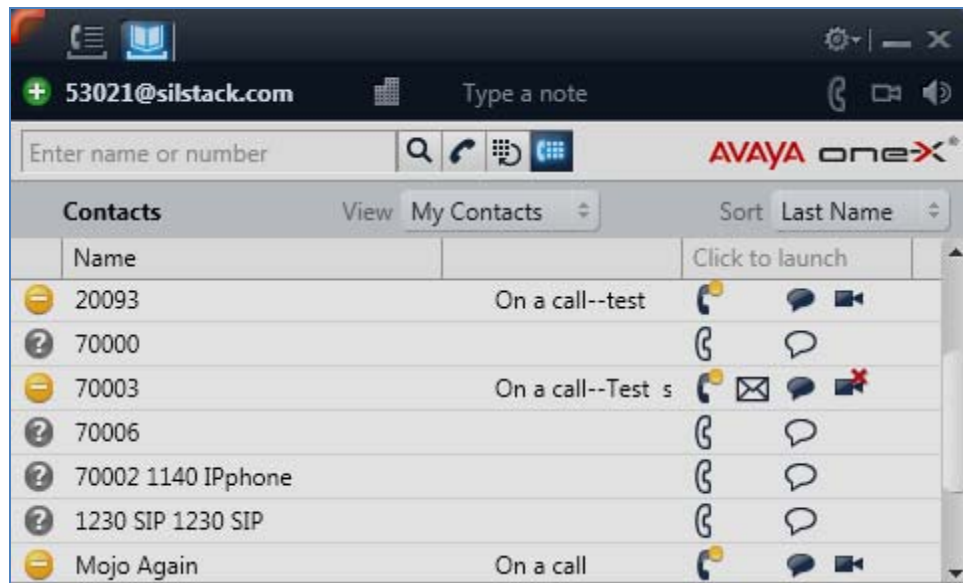


## 8.5. Verify Presence using Avaya one-X® Communicator SIP

The following screenshot shows Presence information for the one-X communicator SIP extension 53021 while the IPSec VPN Tunnel is connected.

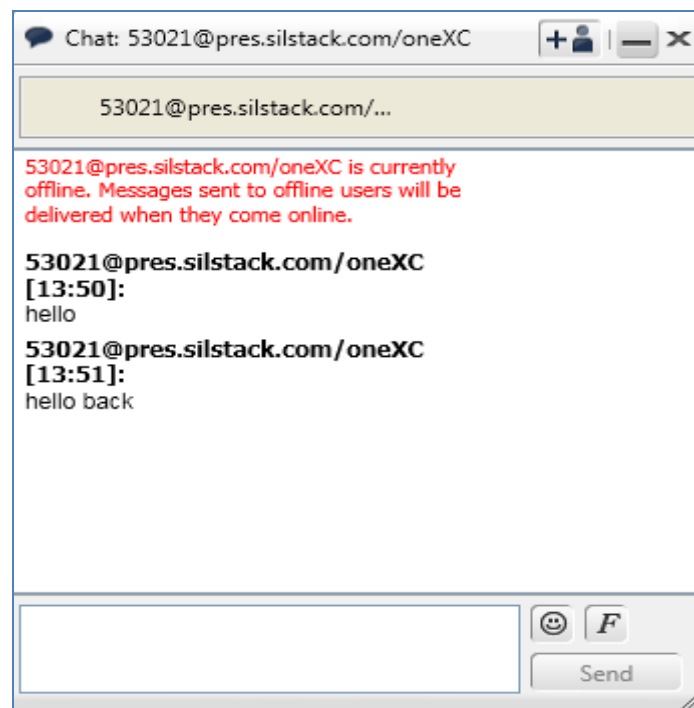


The following screenshot shows Presence busy information for the Contacts of one-X Communicator SIP extension 53021 while the IPSecVPN Tunnel is connected.



## 8.6. Verify Instant Messaging using Avaya one-X® Communicator SIP

The following screenshot You may want to highlight this indicator shows Instant Messaging information for the one-X Communicator SIP extension 53021 while the IPSec VPN Tunnel is connected.



## 9. Conclusion

These Application Notes have described the administration steps required so that Avaya one-X® Communicator SIP soft client can interoperate with Avaya VPN Gateway 3050, over a VPN IPSec tunnel, while registered to Avaya Aura® Session Manager. It has also confirmed that Avaya one-X® Communicator SIP can make a video call, interoperate with Avaya Aura® Messaging and Avaya Aura® Presence Services, while the VPN IPSec tunnel is established to the Avaya VPN Gateway 3050.

## 10. Additional References

This section references Avaya documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] Administrator Guide Avaya VPN Gateway, December 2010 Document Number NN46120-105
- [2] User Guide Avaya VPN Gateway, December 2010 Document Number NN46120-104.
- [3] Administering Avaya Aura® Session Manager, August 2010 Document Number 03-603-324.
- [4] Installing Avaya Aura® Session Manager, January 2010 Document Number 03-603473
- [5] Administering Avaya Aura® Communication Manager Server Options, June 2010, Document Number 03-603479.
- [6] Administering Avaya Aura® Presence Services 6.0 , September 2010.
- [7] Administering Avaya Aura® Presence Services 6.0 XCP Controller, August 2010.



---

**©2011 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com)