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.

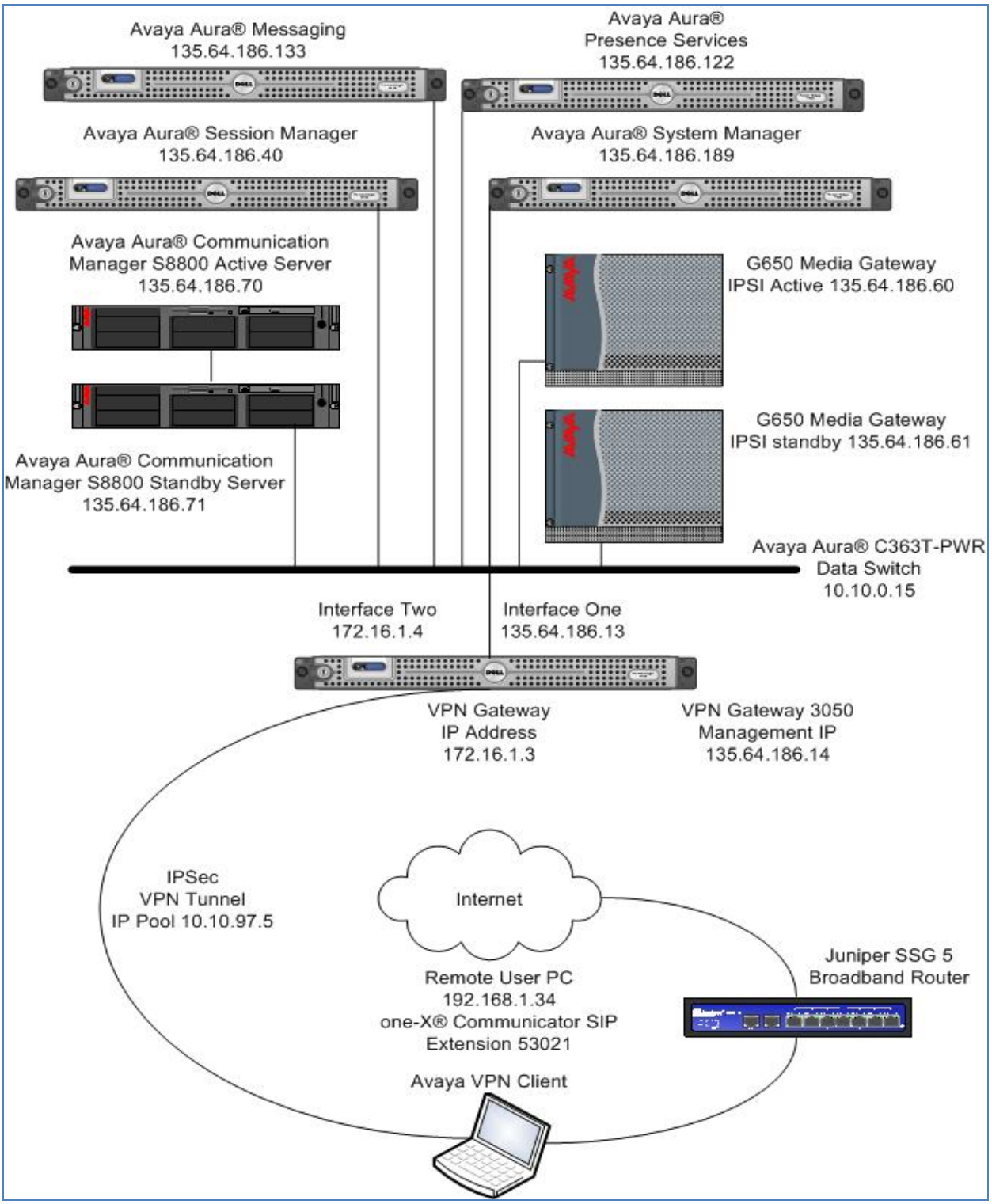


Figure 1: VPN IPSec tunnel with VPN Client using AvayaVPN Gateway 3050

2. Equipment and Software Validated

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

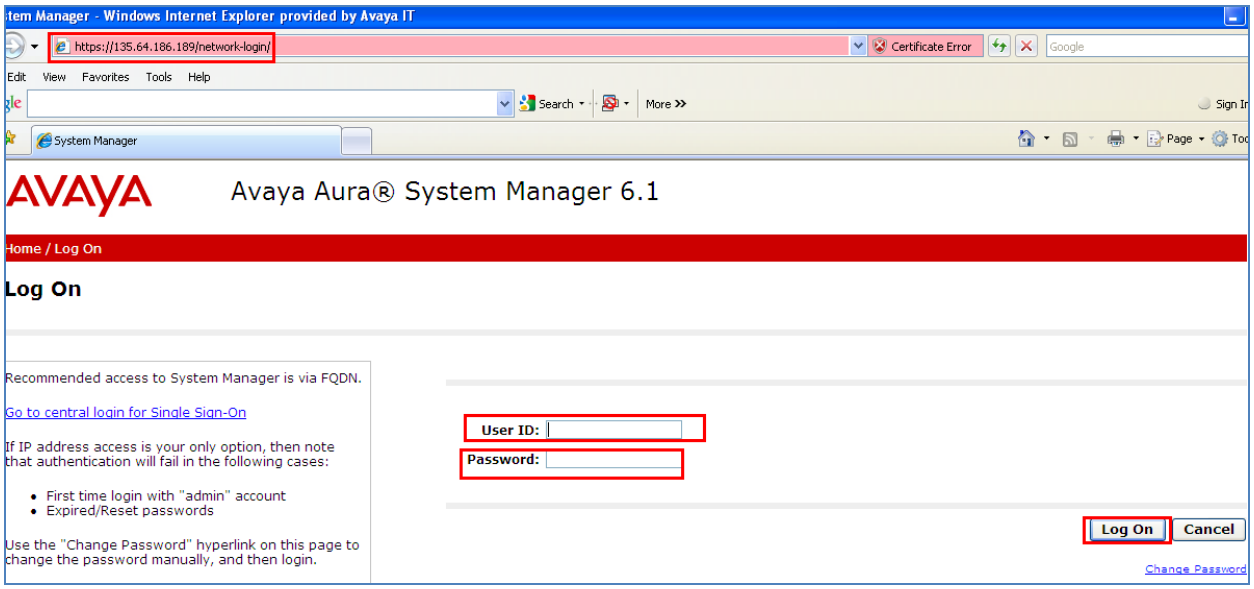
Avaya Aura®	Software
Avaya Aura® System Manager on a S8800 Server	Avaya Aura® System Manager Release 6.1.0.0.7345-6.1.5.106 Update: Service Pack 2
Avaya Aura® Session Manager on a S8800 Server	Avaya Aura® Session Manager Release 6.1.2.0.612004 Update: Service Pack 2
Avaya Aura® Communication Manager 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

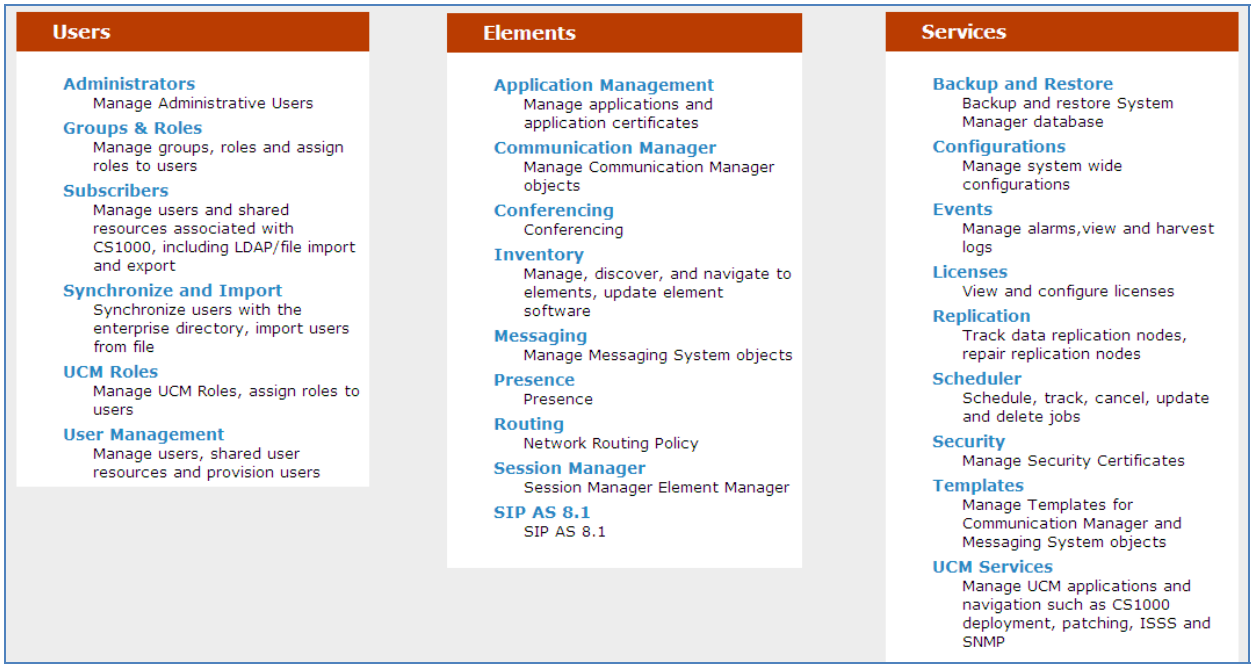
This section describes steps needed to configure System Manager. It will describe configuration of accessing System Manager, administering a Location and adding a SIP User in User Management of System Manager. For details of how to administer a SIP Entity between Session Manager and the Communication 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.

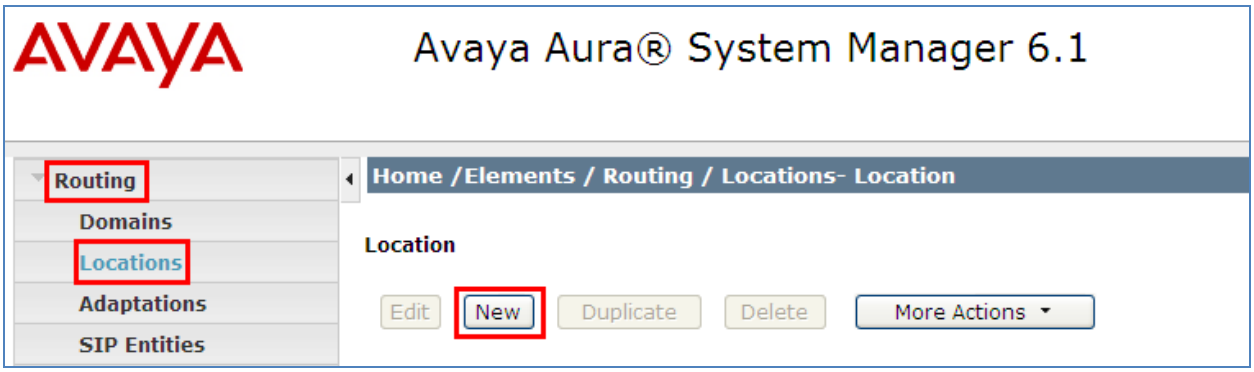


The following screen is displayed upon login.

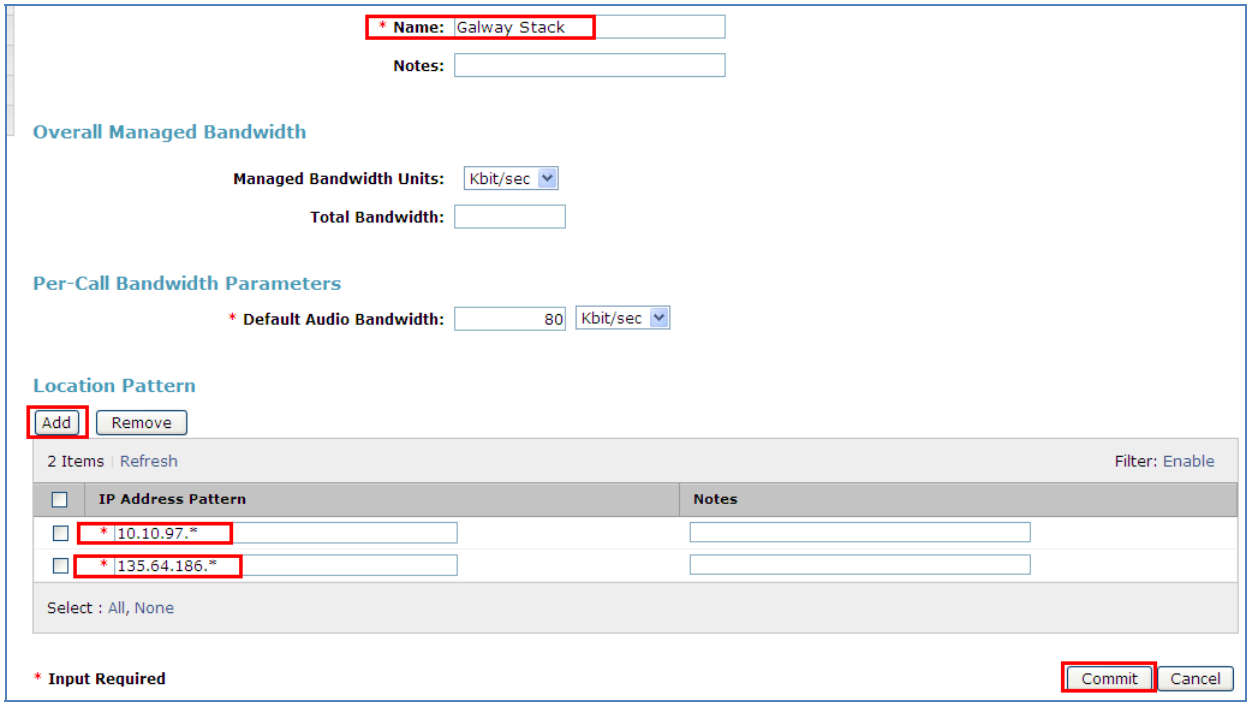


3.2. Administer Location

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.

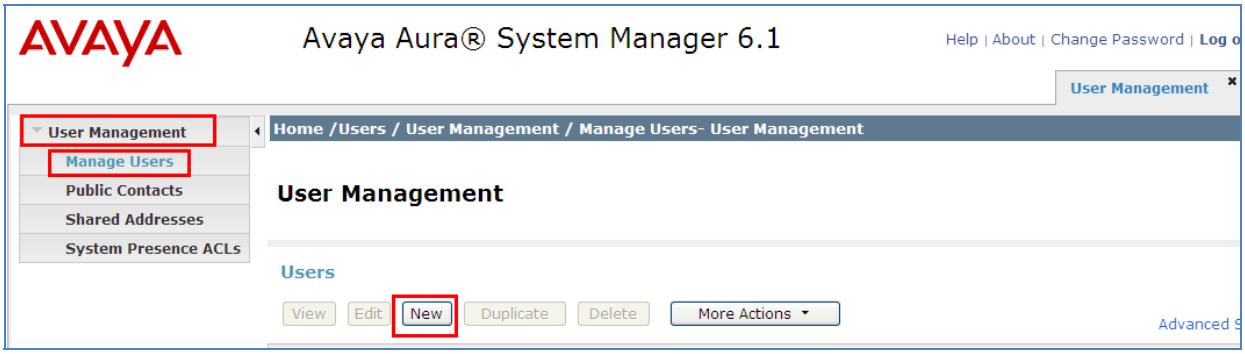


A location **Name** called **Galway Stack** was added to the Session Manager. The IP Address pattern **10.10.97.*** and **135.64.186.*** were added the **IP Address Pattern** table. The **Commit** button was selected to confirm changes.

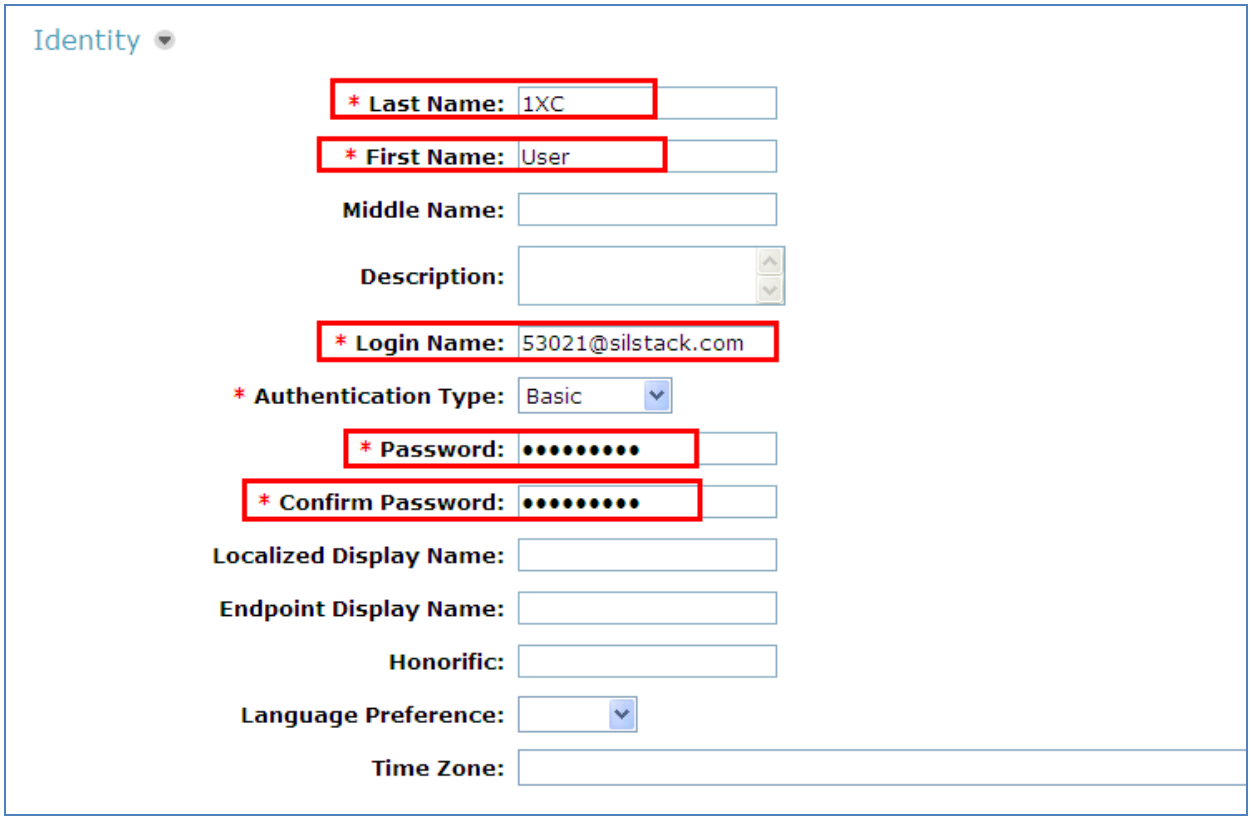


3.3. Administer SIP User

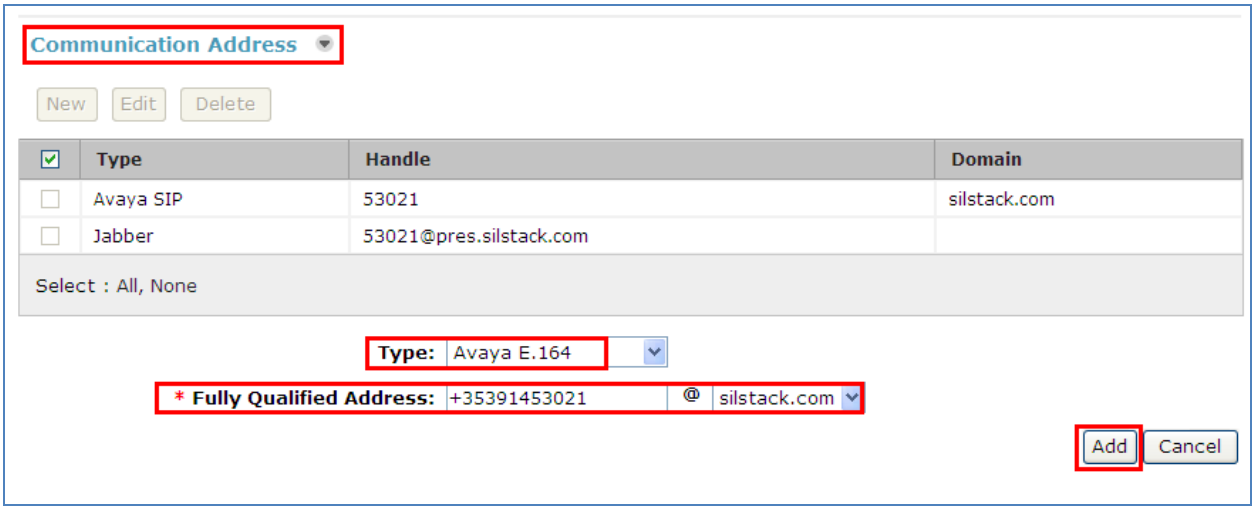
To add a SIP User to Session Manager, access the **User Management** heading on the left hand side of the System Manager GUI. Access the **Manage Users** sub heading. The **New** button was selected.



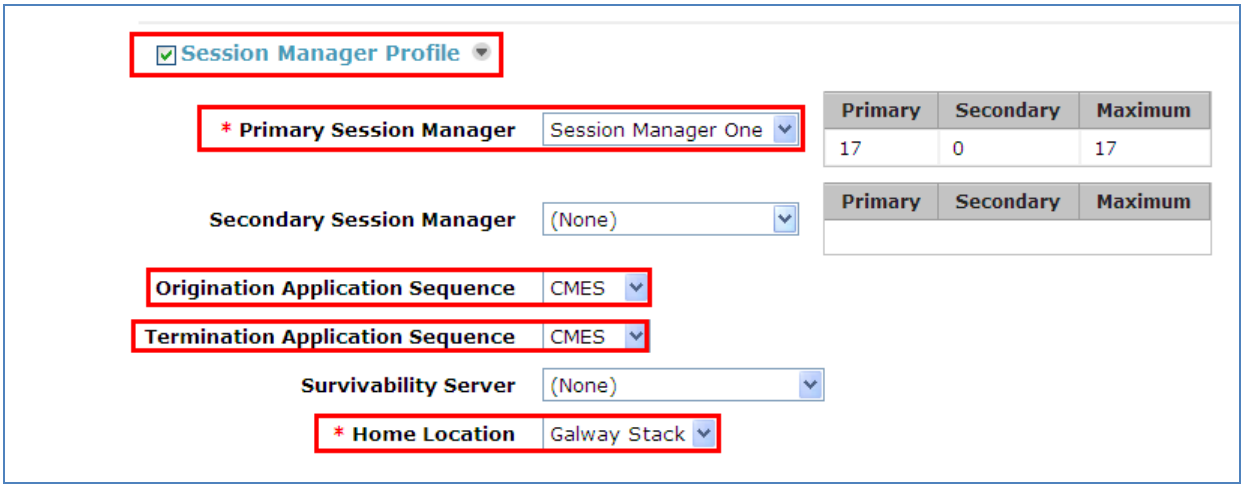
For the SIP User being added the **Last Name** was **1XC** and the **First Name** was **User.** The **Login Name** was **53021@silstack.com** and the **Password** was set to the password of the System Manager upon login.



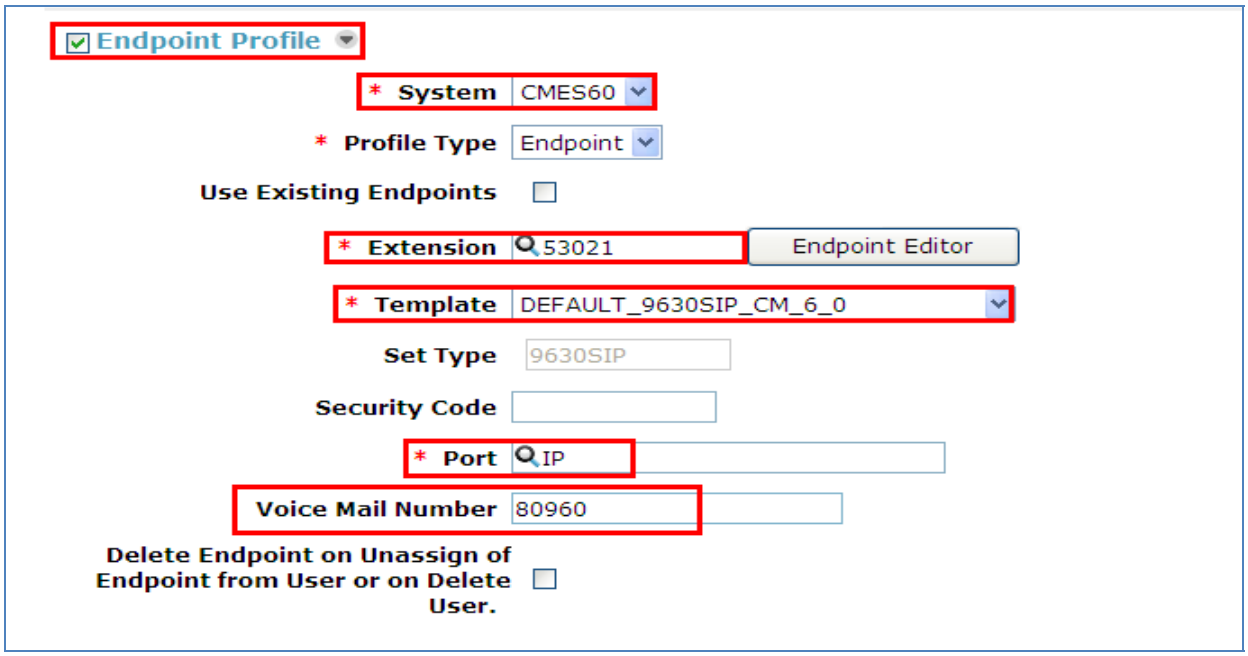
Access the **Communication Address** heading. In the Communication Address the **Type** was set to **Avaya E.164**. The **Fully Qualified Address** was set as **+35391453021@silstack.com.** Select the **Add** button to save the changes.



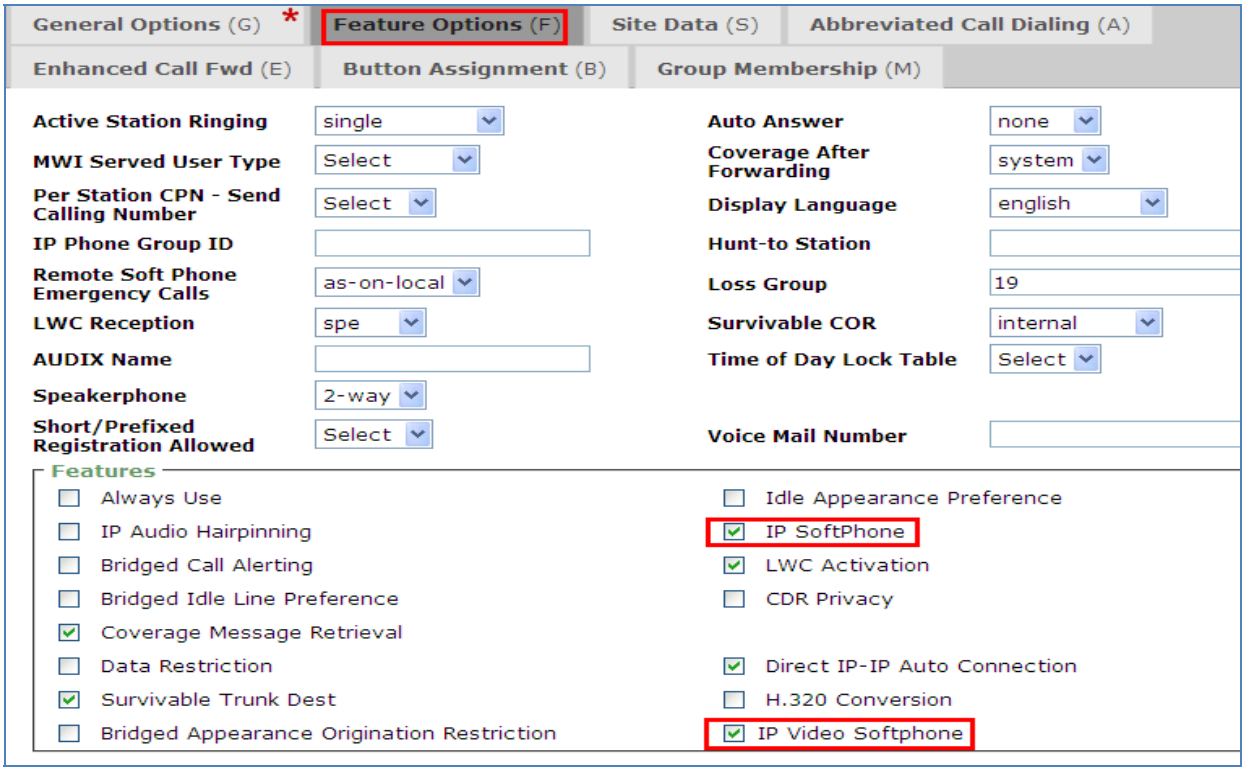
Access the **Session Manager Profile.** The **Primary Session Manager** was set to **Session Manager One** as shown below. This equates to the Session Manager SIP entity. The **Origination and Termination Application Sequence** was set to **CMES.** This is the Communication Manager Evolution Server Application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



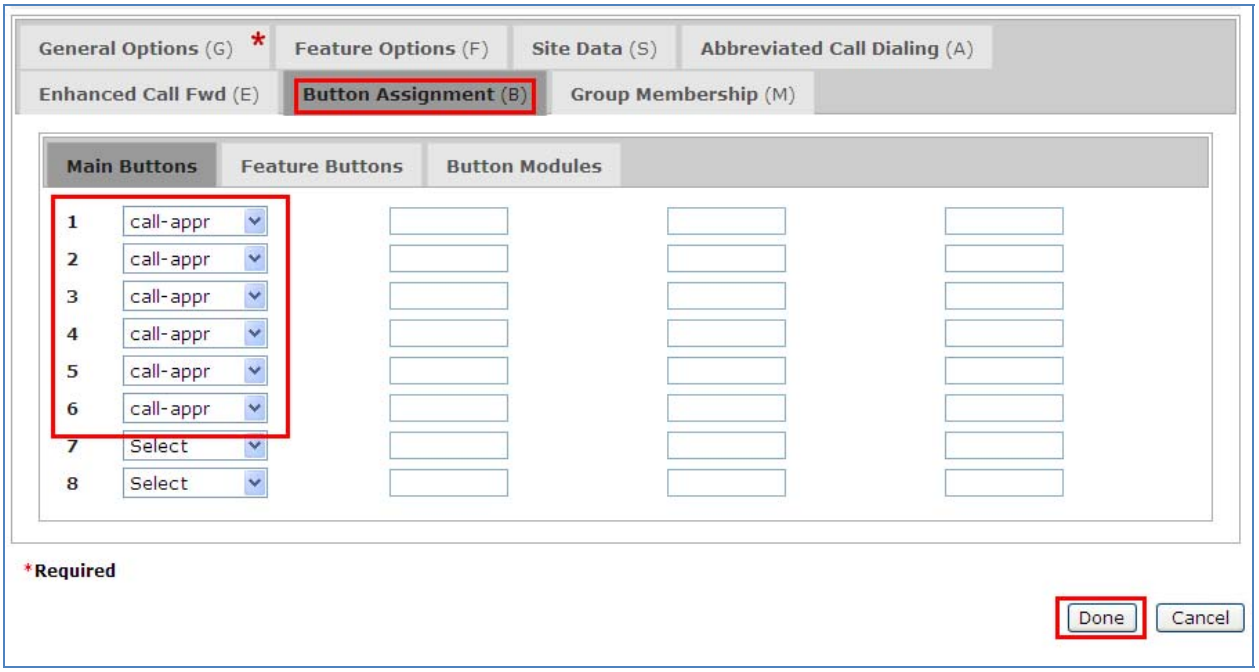
In order for the Station Profile template information to be pushed from the Session Manager down to the Communication Manager Evolution Server, **enable** the **Endpoint Profile** box. The **System** was set to **CMES60.** This is the Communication Manager Evolution Server Element Name. The **Extension** 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.**



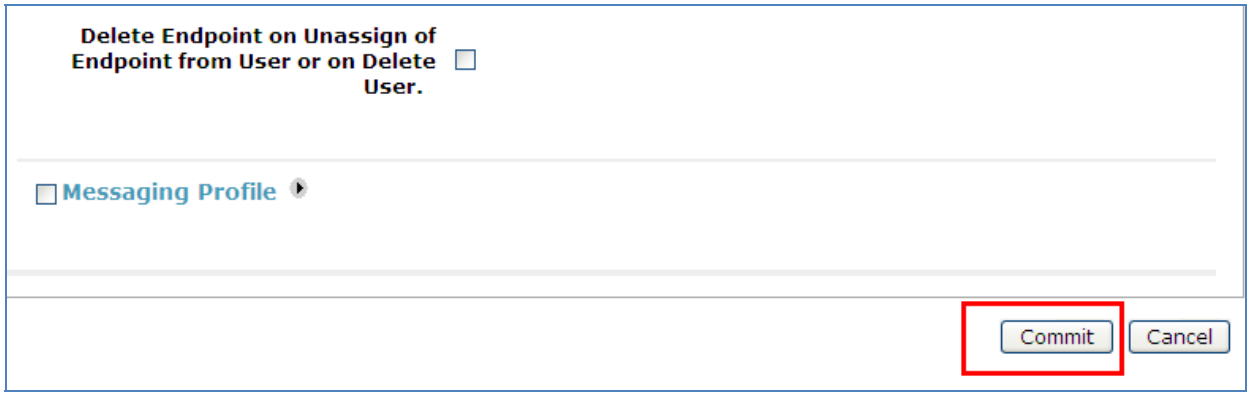
Click on **Endpoint Editor,** and under **Feature Options** enable **IP softphone** and **IP Video Softphone.**



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



Select **Commit** to save the changes.



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:

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

                                                 Subnet Network     Emergency
 IP Address                                      Bits   Region VLAN 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.

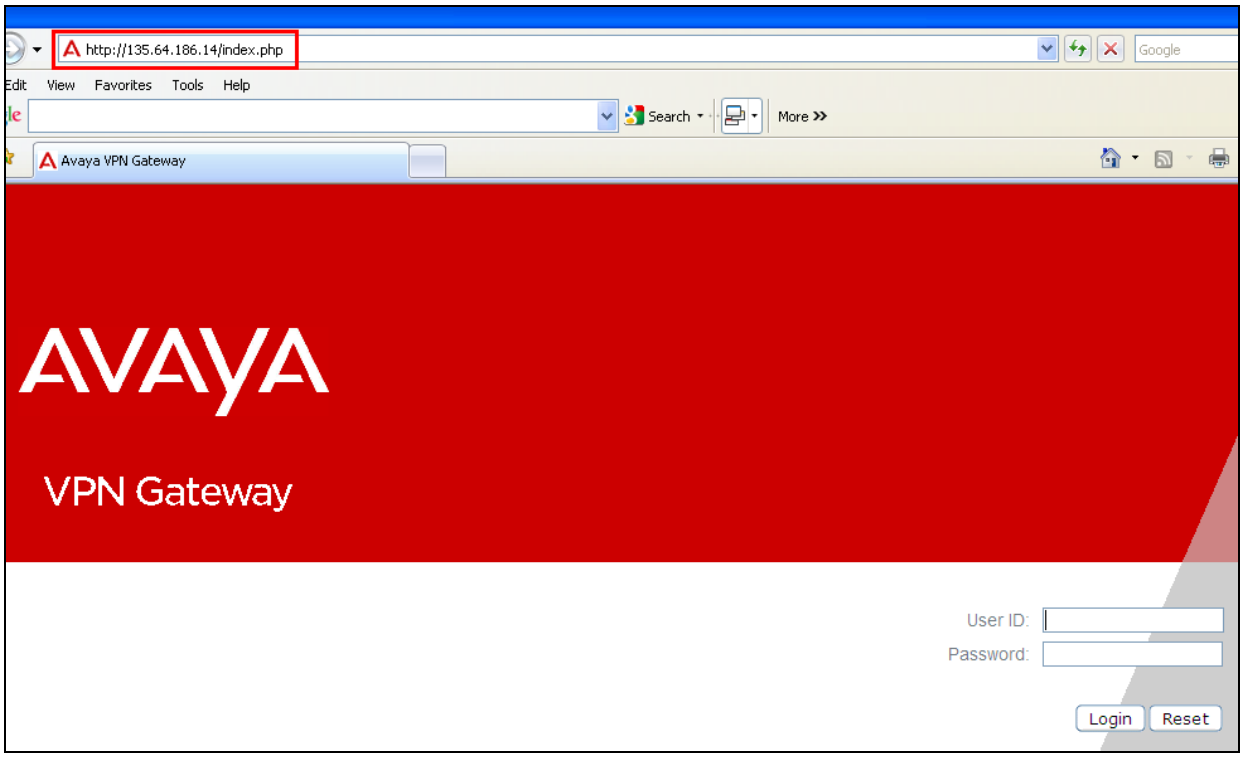
```
                              SAVE TRANSLATION

           Command Completion Status                              Error Code
           Success                                                    0
```

5. Administer Avaya VPN Gateway 3050

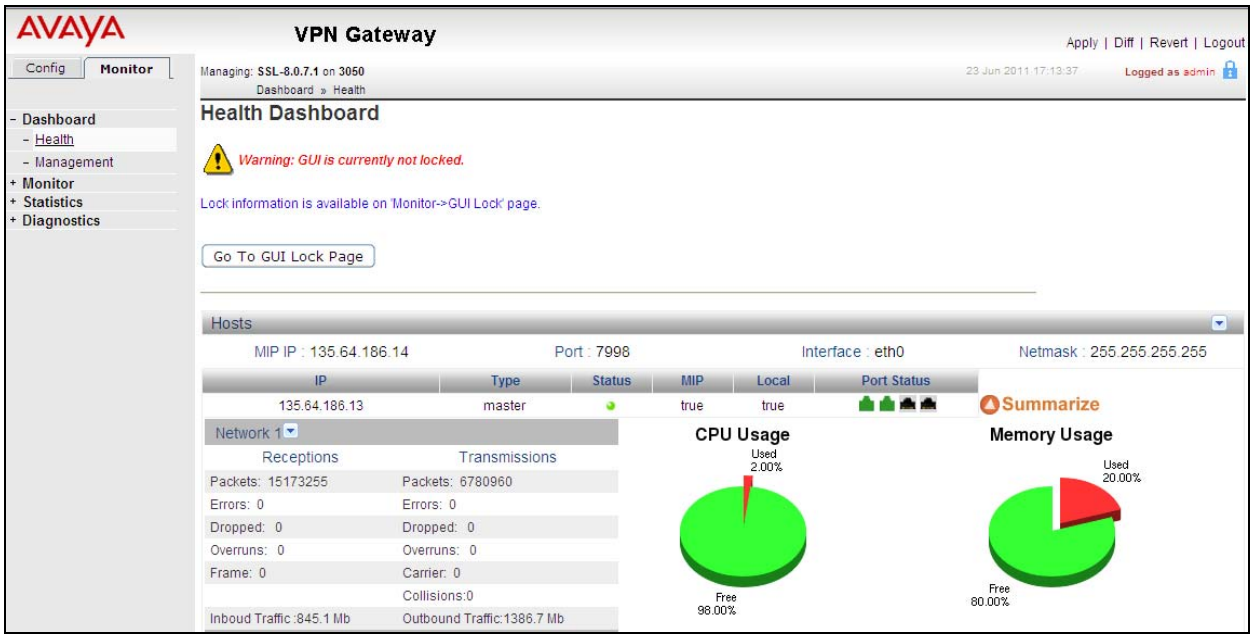
The following steps describe configuration of the VPN Gateway 3050. This section will describe the server configuration needed to establish a VPN IPSec tunnel between the remote user pc and VPN Gateway 3050. It will describe configuring an IP Pool, adding a User Tunnel Profile, administering an IKE Profile 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.

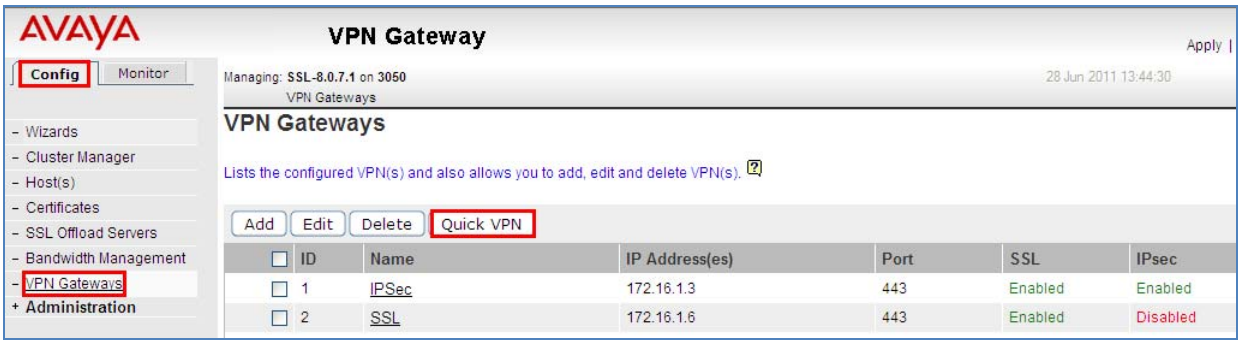


Upon login the following screen is displayed.

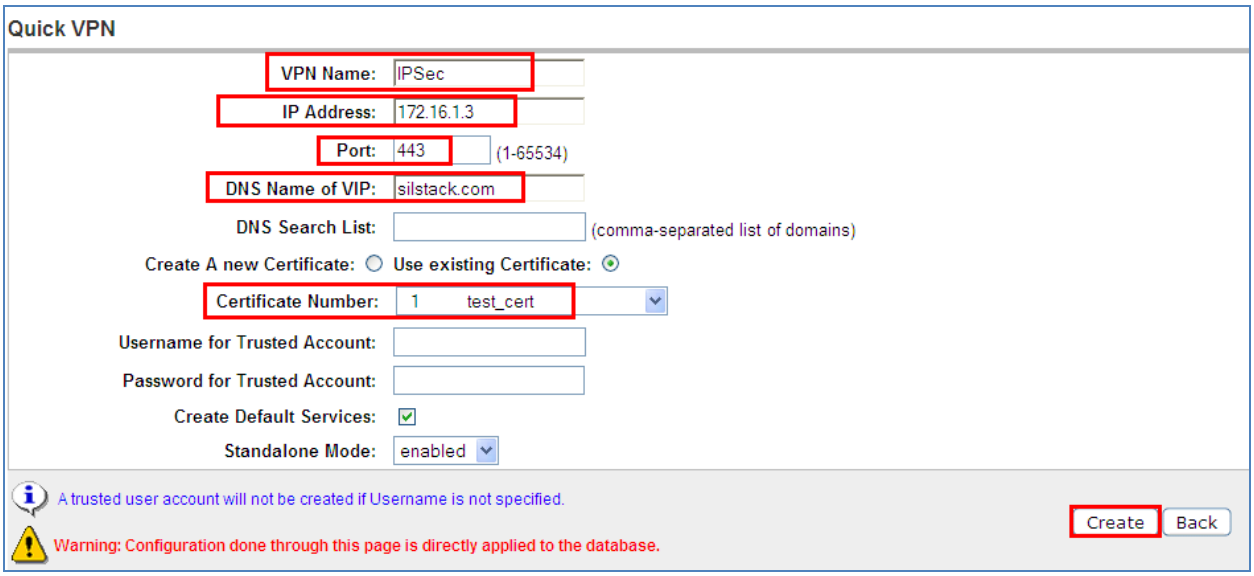


5.2. Administer IPSec Avaya VPN Gateway

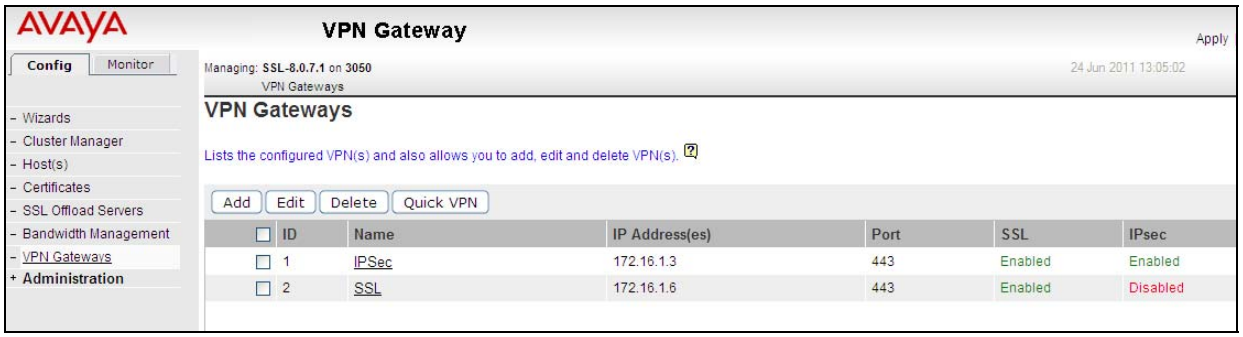
To create the IPSec VPN Gateway select **Config → VPN Gateway** on the graphical user interface. Select the **Quick VPN** button.



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.

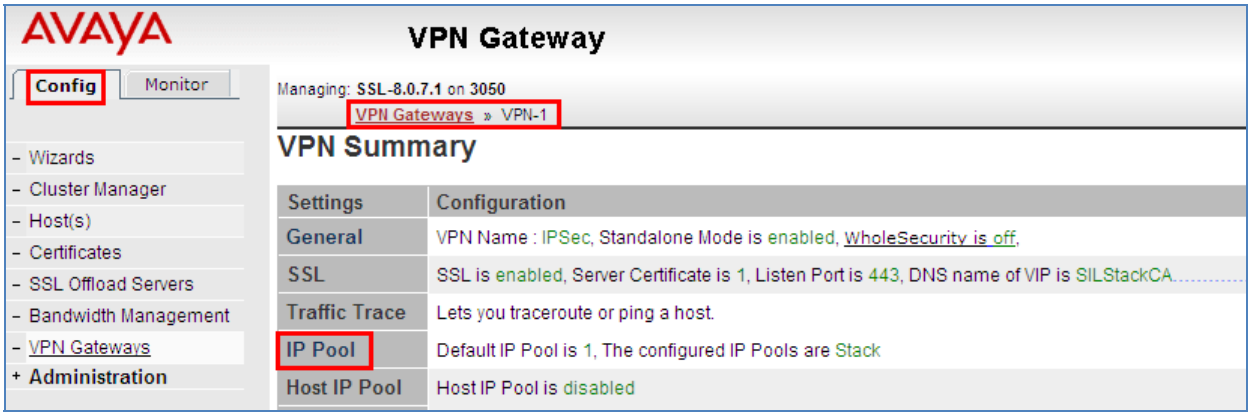


Upon completion, the following screen is displayed.

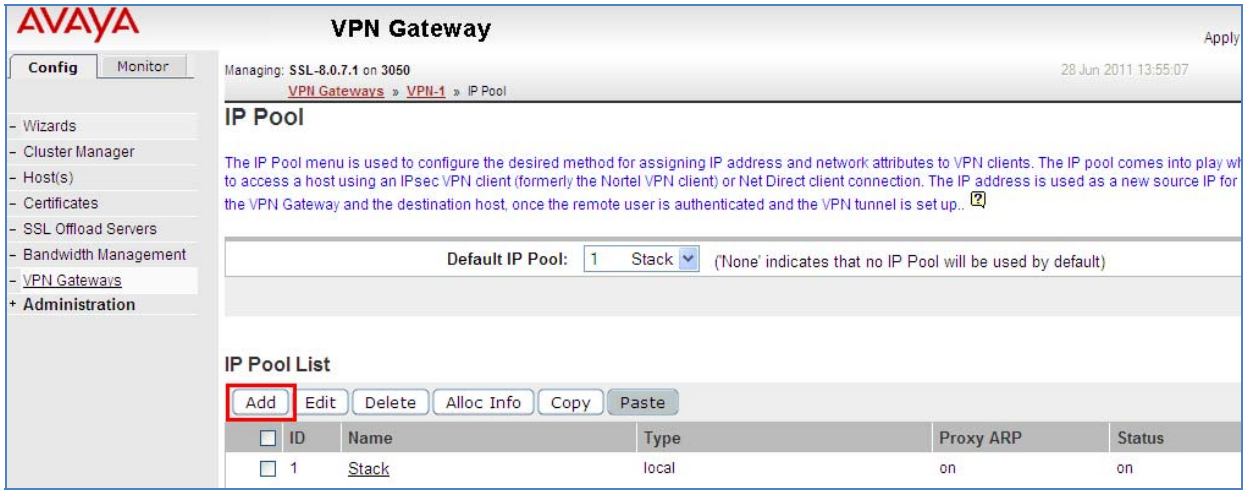


5.3. Administer IP Pool

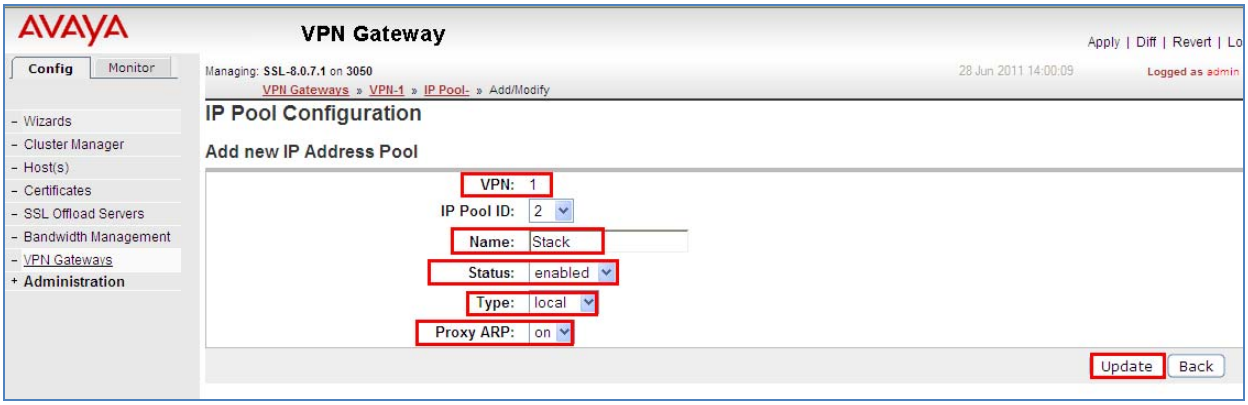
To administer the IP Pool select **Config → VPN Gateway → VPN 1**. Then under **Settings** select **IP Pool** on the graphical user interface.



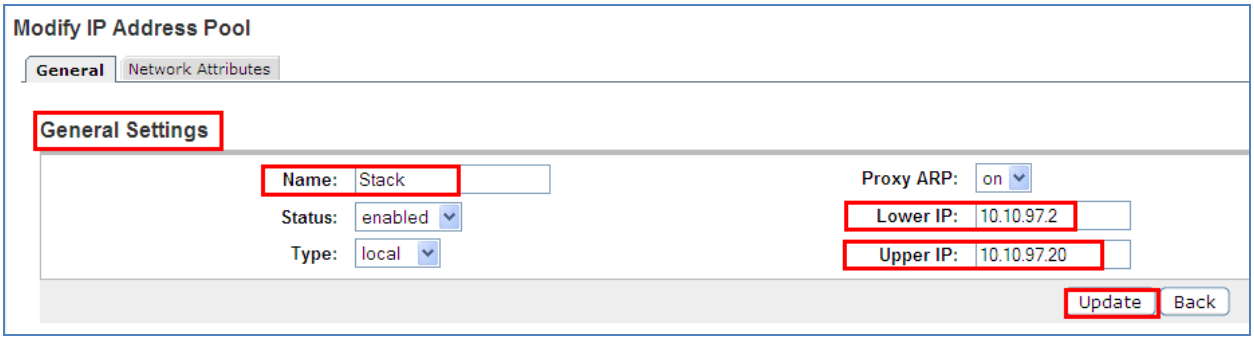
Under the IP Pool list select the **ADD** button.



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.



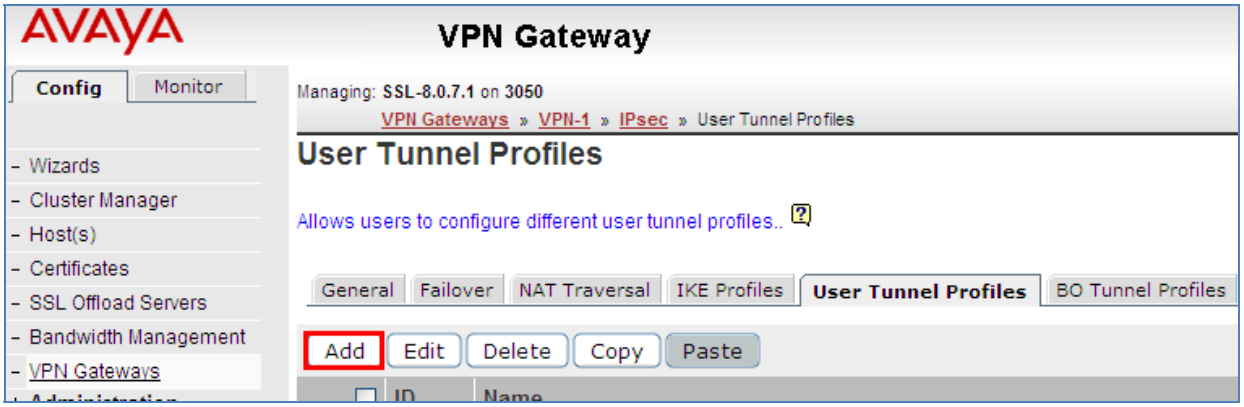
Under the **General Settings** of the IP Pool **named Stack.** The **Lower IP** address was set to **10.10.97.2** and the **Upper IP** address was set to **10.10.97.20**. The **Update** button was selected to save the changes.



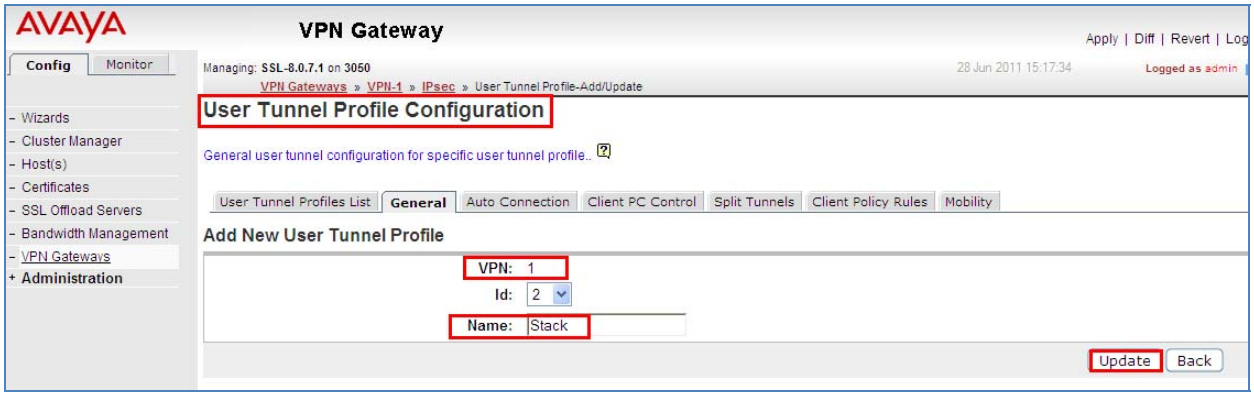
5.4. Add User Tunnel Profile

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

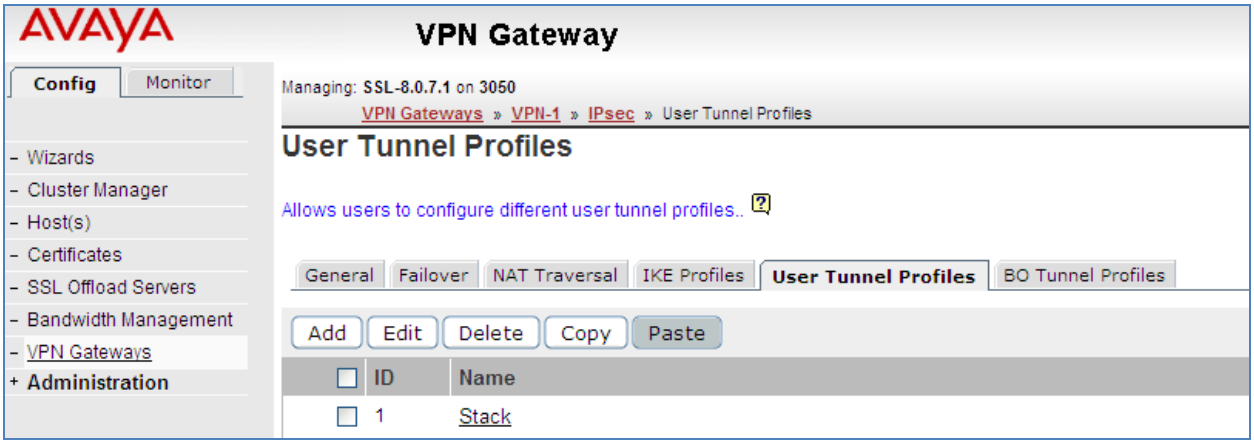
Under User Tunnel Profiles select the **ADD** button.



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.

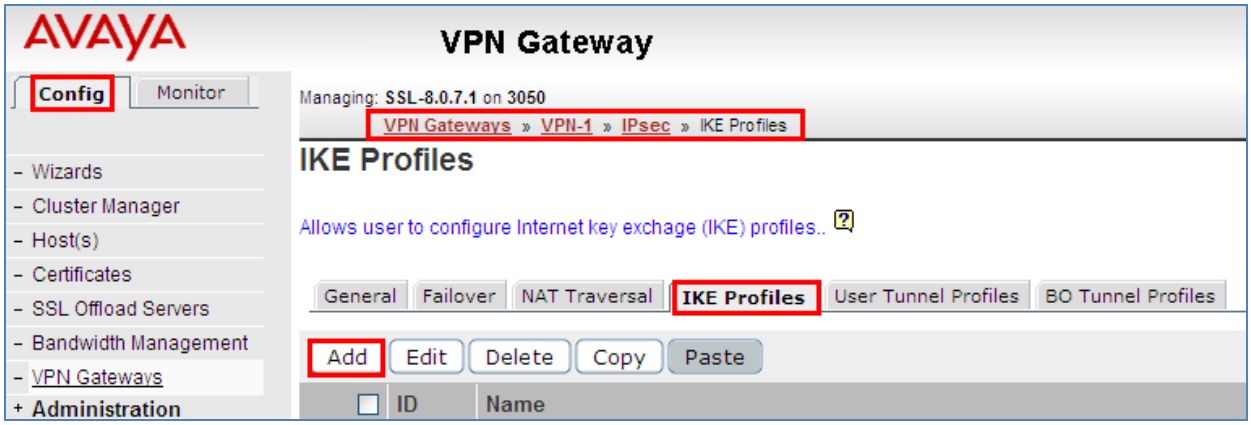


Upon completion, the following screenshot is displayed.

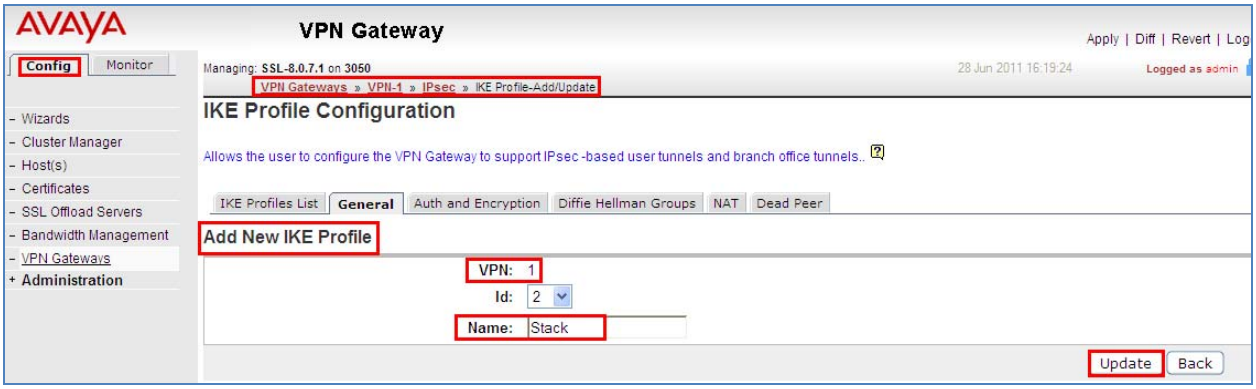


5.5. Administer IKE Profiles

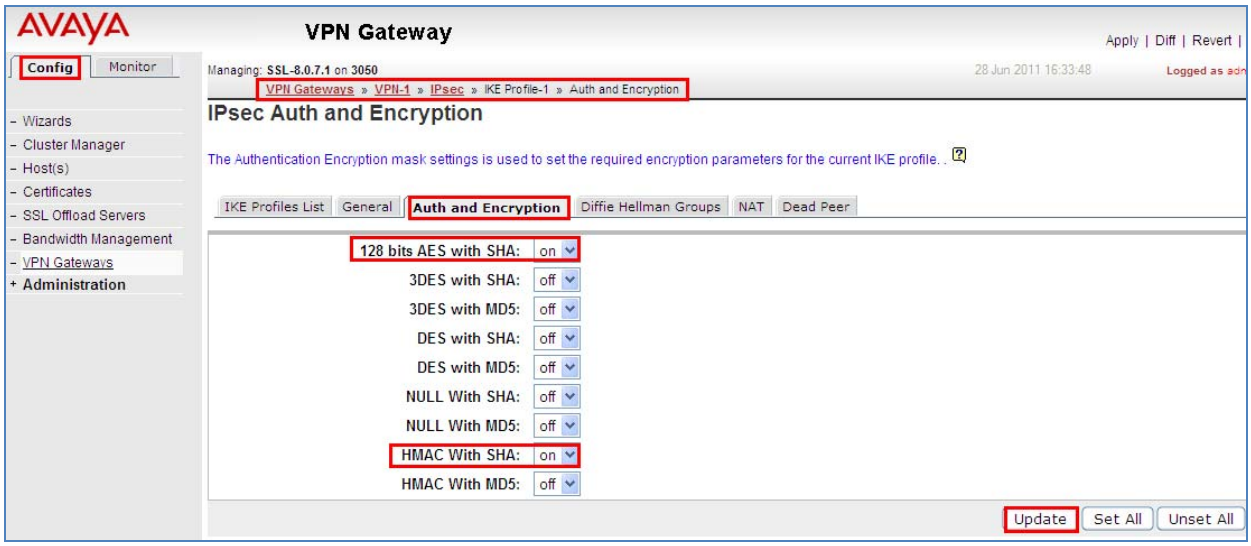
To administer an IKE Profile select **Config → VPN Gateways → VPN 1 → IPSec.** Then select **IKE Profile**. To add a new IKE Profile select the **ADD** button.



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

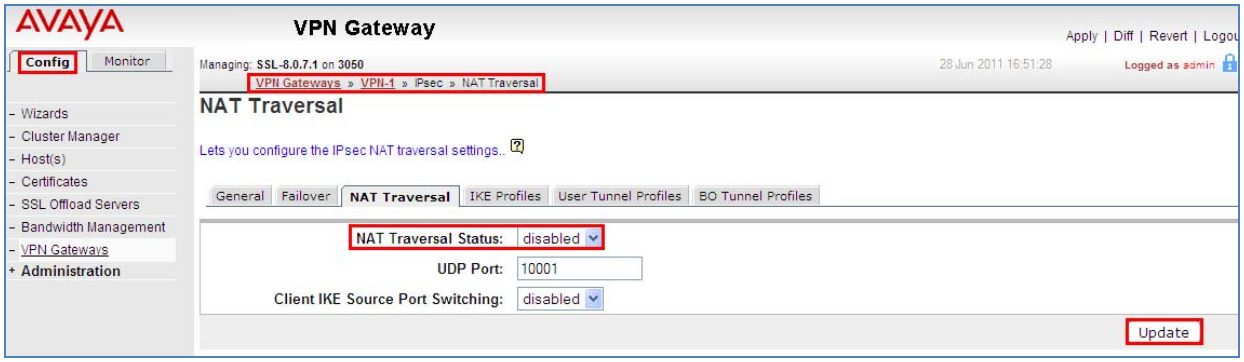


To administer **Auth and Encryption** select **Config → VPN Gateways → VPN 1 → IPSec → IKE Profile 1 → Auth and Encryption.** The **128 bits AES with SHA** was set to **on** and **HMAC with SHA** was set to **on.** The **Update** button was selected to save the changes.



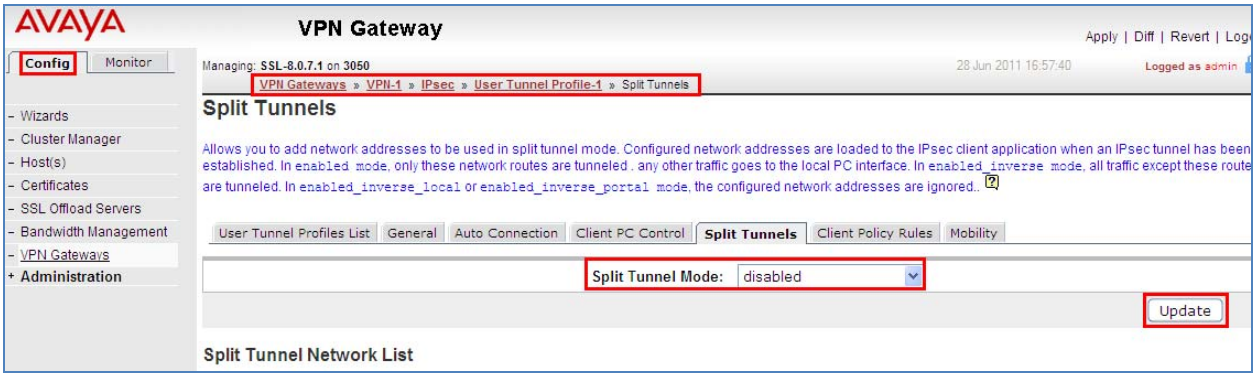
To administer Diffie Hellman group 2 select **Config → VPN Gateways → VPN 1 → IPSec → IKE Profile 1 → Diffie Hellman Group.** The **Diffie Hellman group 2** was set to **on**. The **Update** button was selected to save the changes.

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.



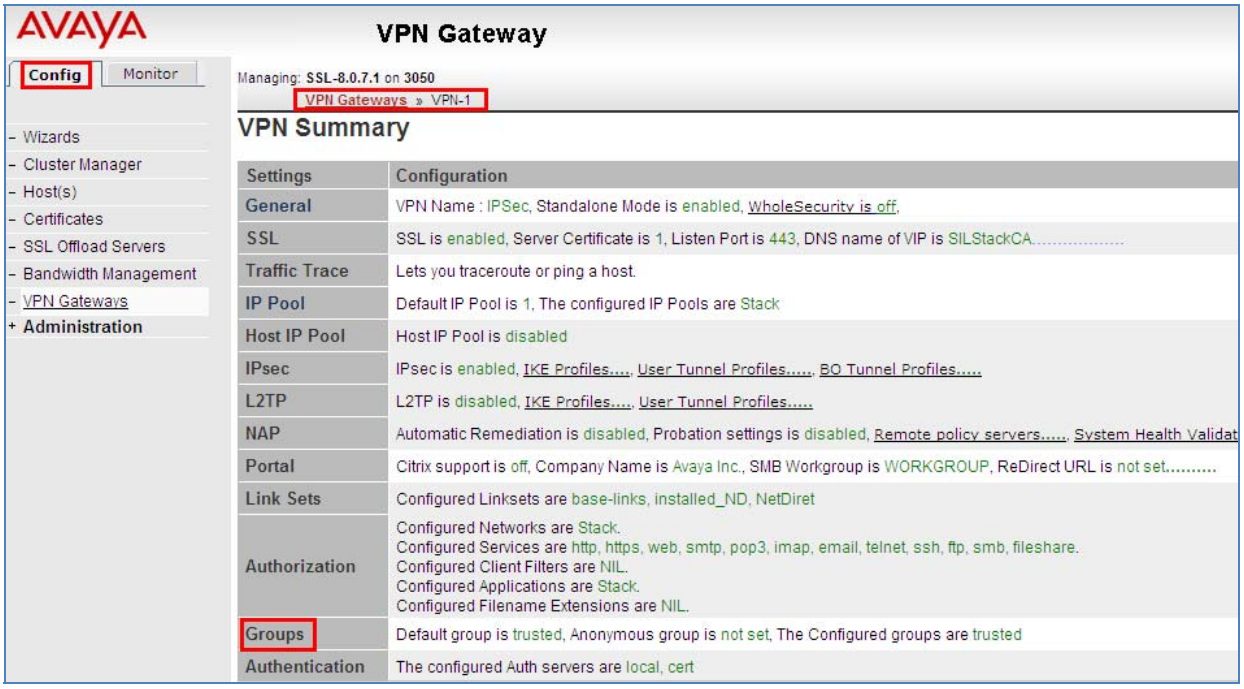
5.6. Administer Split Tunnel

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.

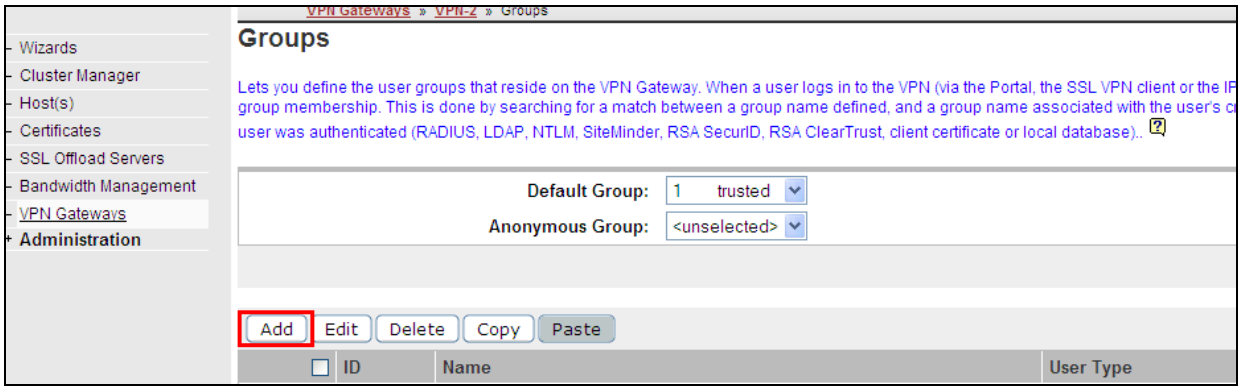


5.7. Administer Trusted Group

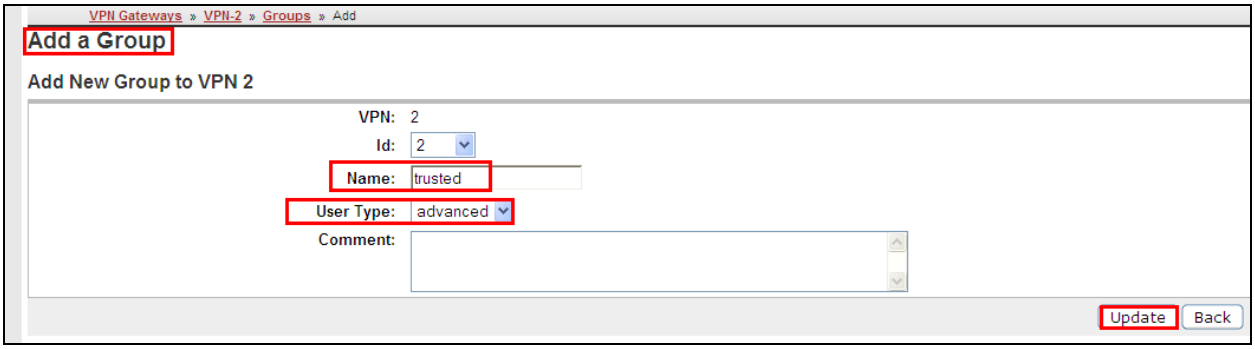
To administer a Trusted Group select **Config → VPN Gateway → VPN 1**. Then under settings select **Groups** on the graphical user interface.



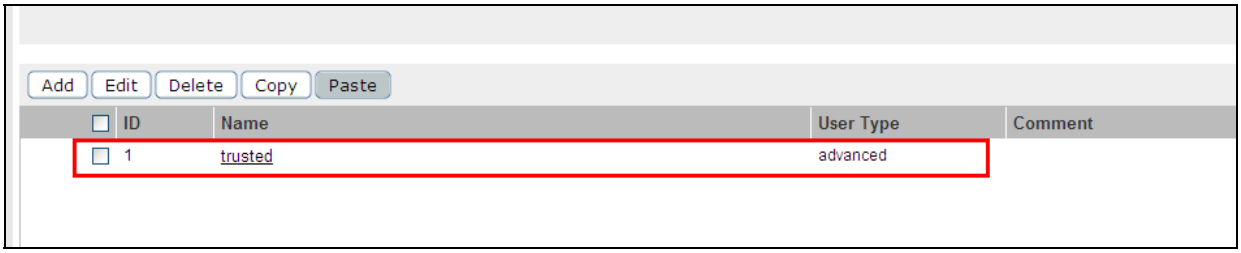
Select the **Add** button under Groups



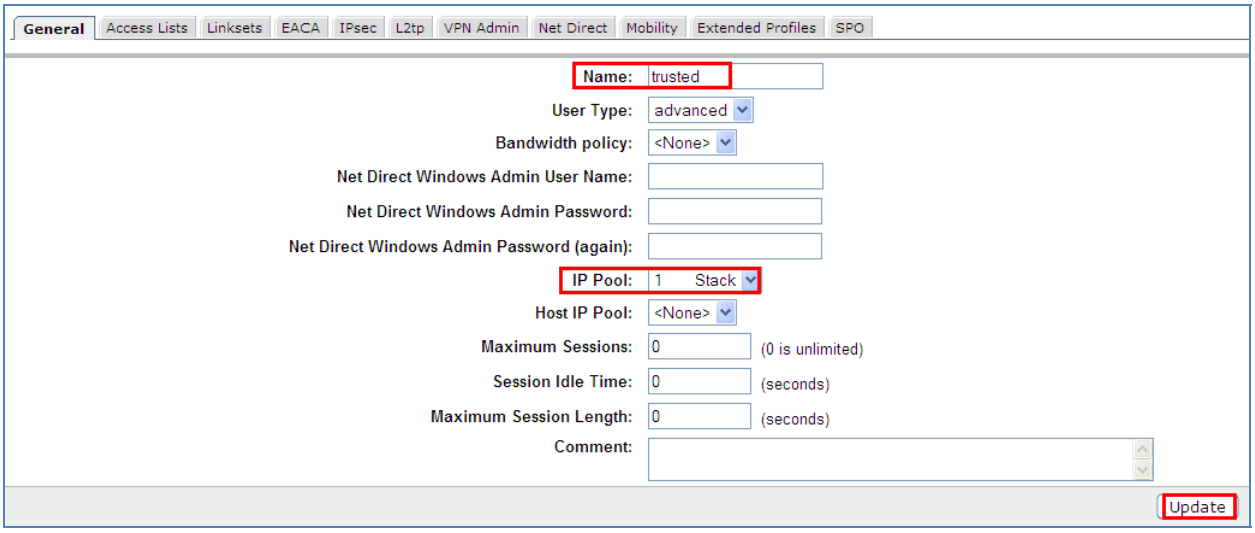
Under **the Add a Group** the Group **Name** was set to **trusted**. The **User Type** was set to **advanced.** The **Update** button was selected.



The following **trusted** group was added.

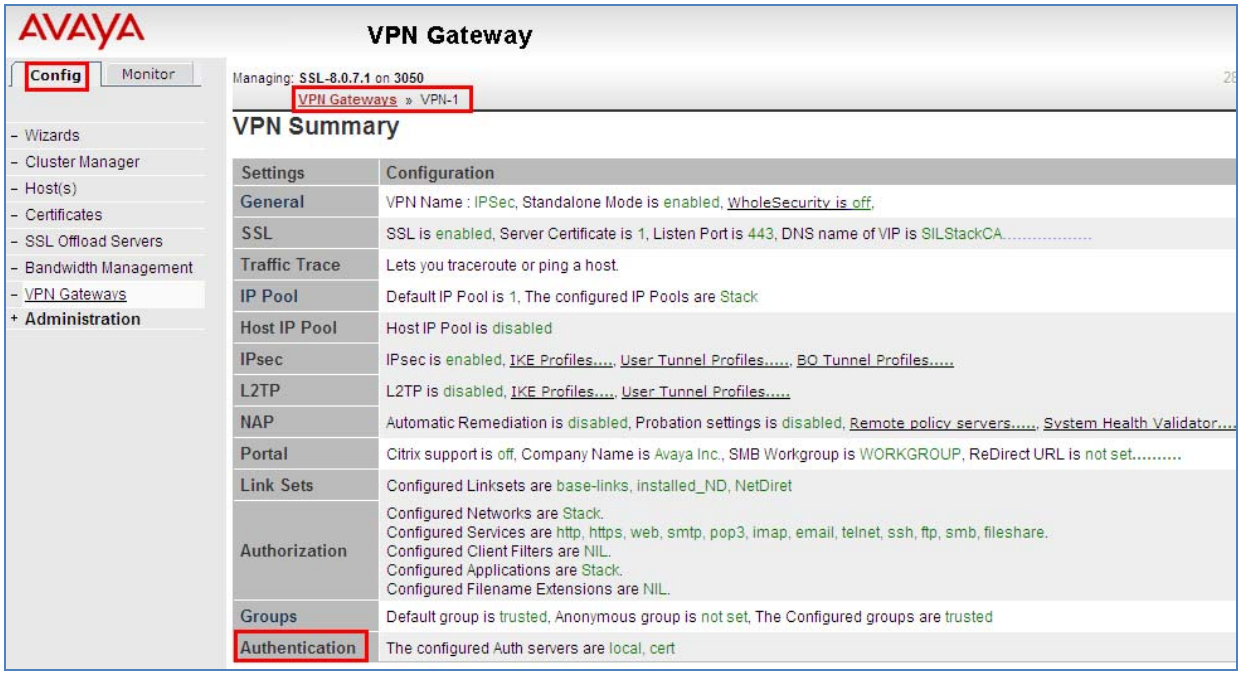


After selecting the group named trusted the following page is displayed. The **IP Pool** called **Stack** created in **Section 5.3** was assigned to the group named **trusted.** The **Update** button was selected to save the changes.



5.8. Administer User Authentication

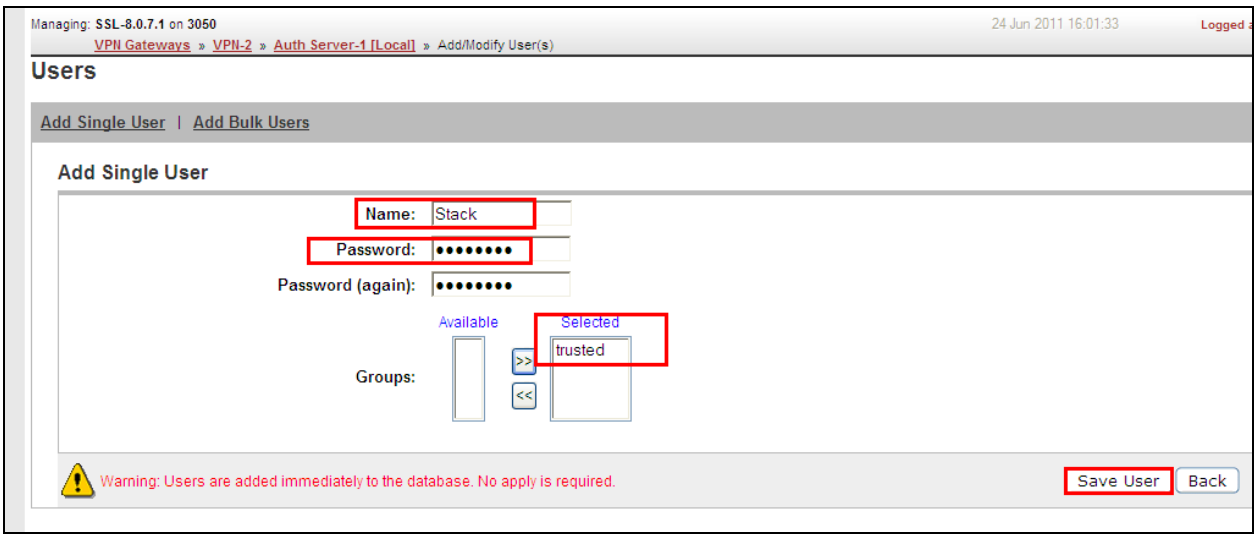
To administer an Authentication Account select **Config → VPN Gateway → VPN 1**. Then under **Settings**, select **Authentication** on the graphical user interface.



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

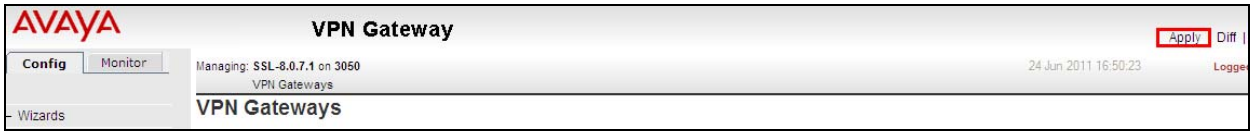
Select the **Add** option under **Config → VPN Gateways → VPN 1 → Auth Server 1(Local) → User.**

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.



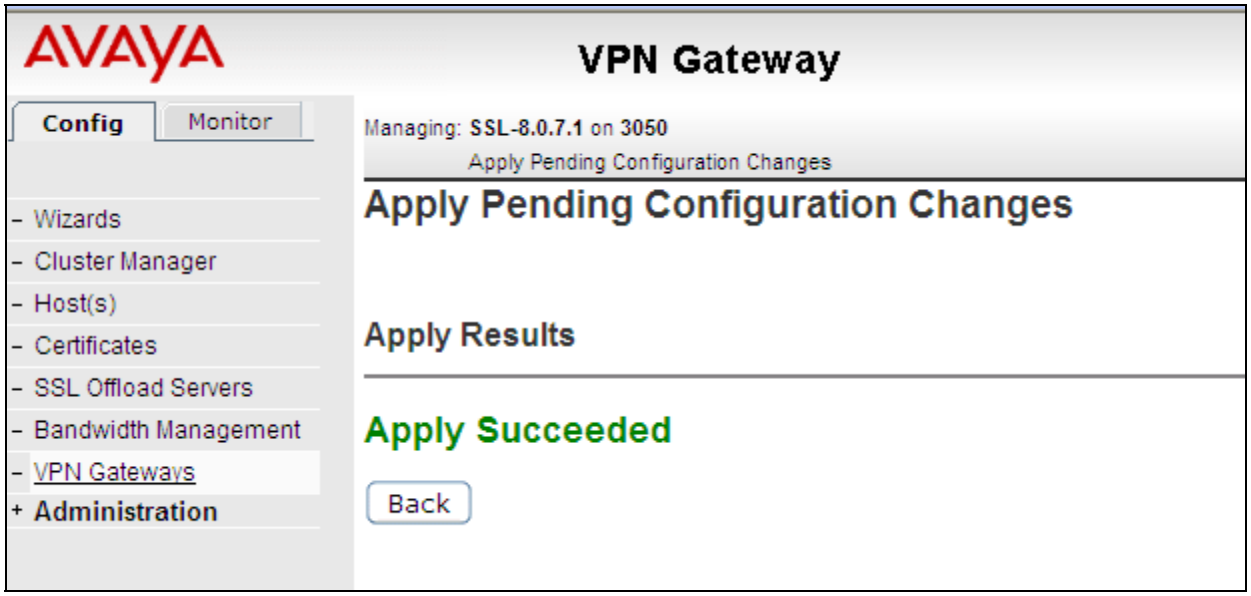
5.9. Apply Changes

For the changes to take affect 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.

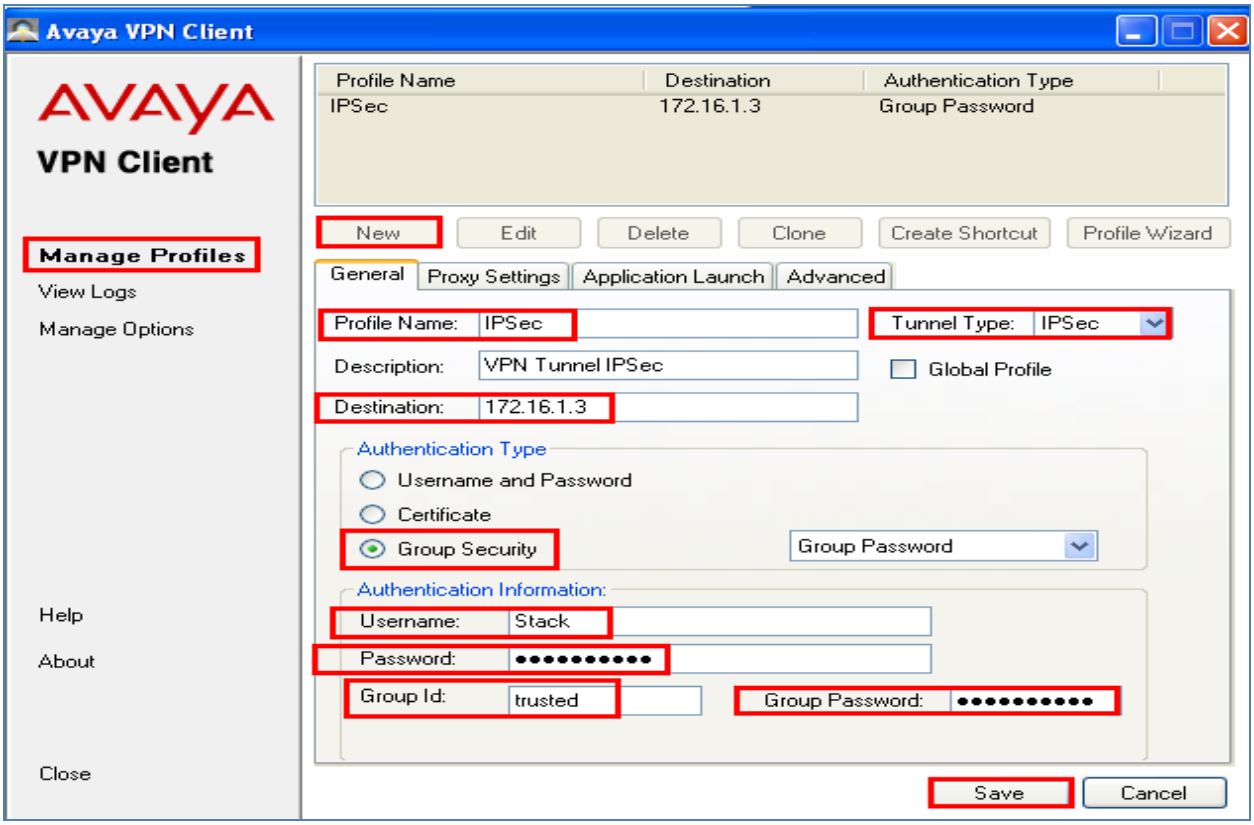
The following screenshot shows the changes were successful.



6. Avaya VPN Client Settings

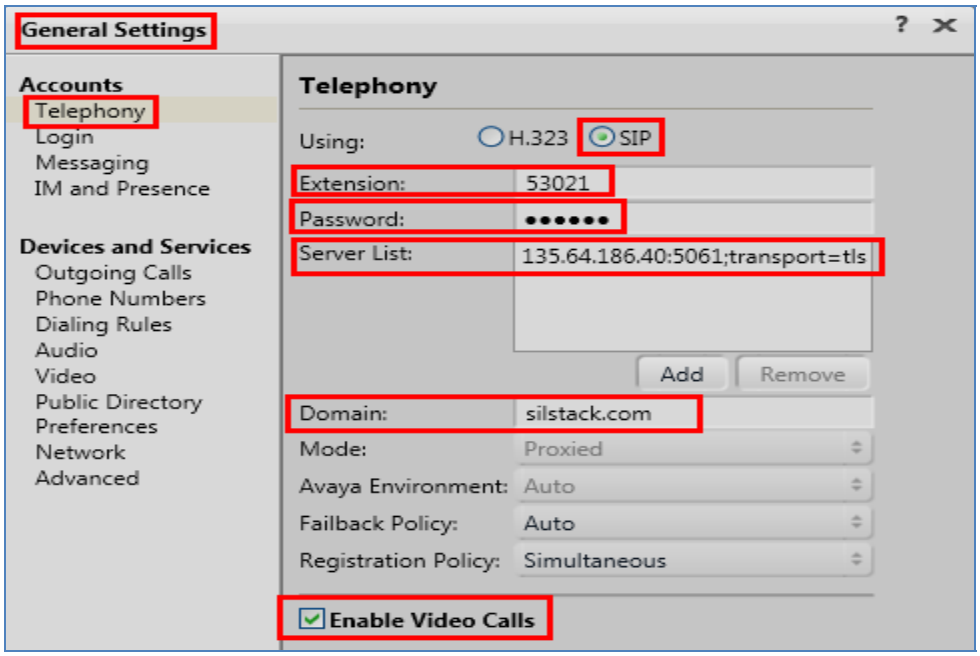
The following section describes the setting needed to administer the VPN Client. Open the VPN Client and select the **Edit the profile** heading.

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.

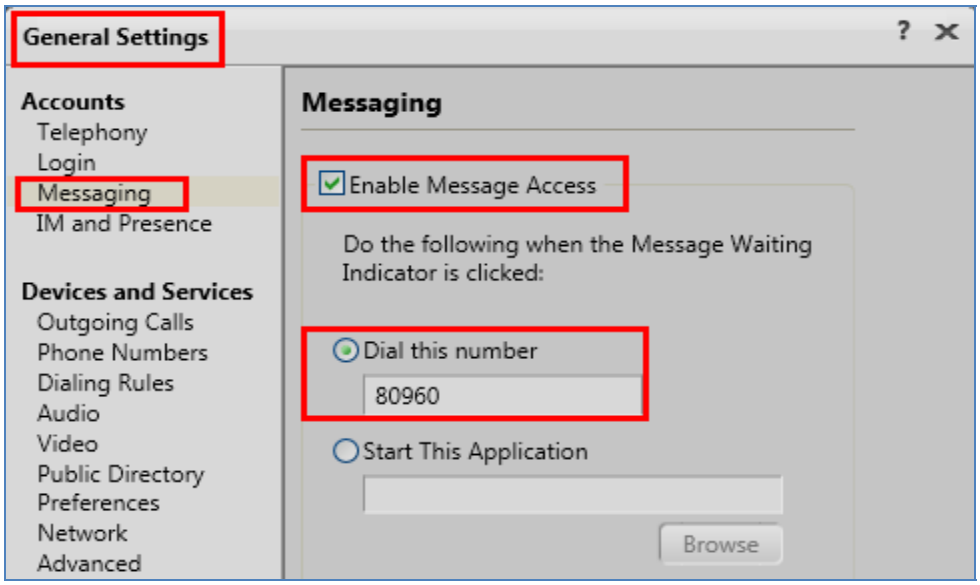


7. Avaya one-X® Communicator SIP Settings

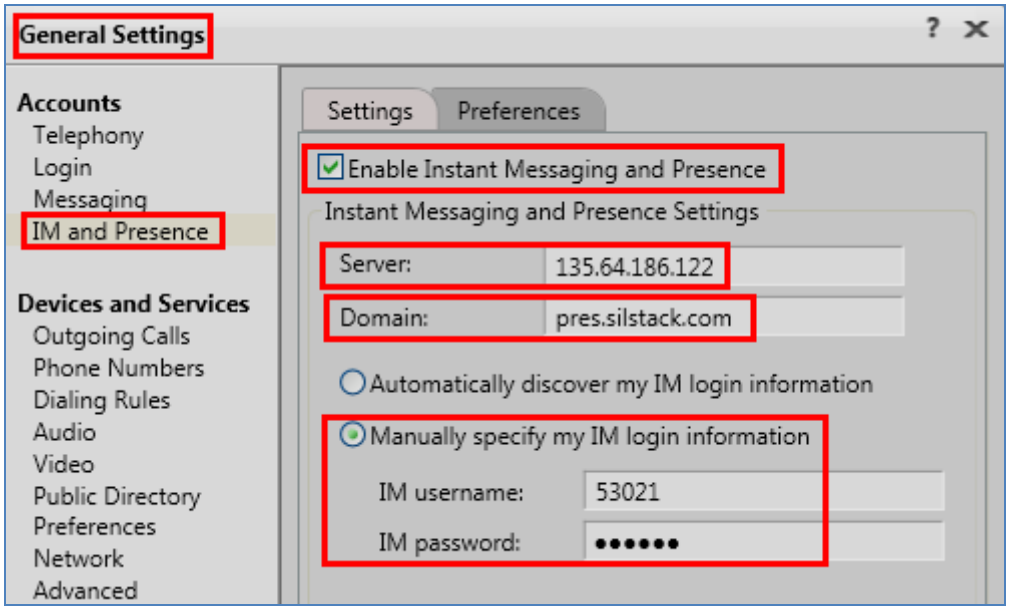
The following section describes the settings needed to administer one-X Communicator SIP soft client. On the one-X Communicator SIP soft client select **General Settings**. Under **Telephony** the **SIP** option was enabled. The **Extension** was set to **53021**. The **Password** was set and the **Server 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



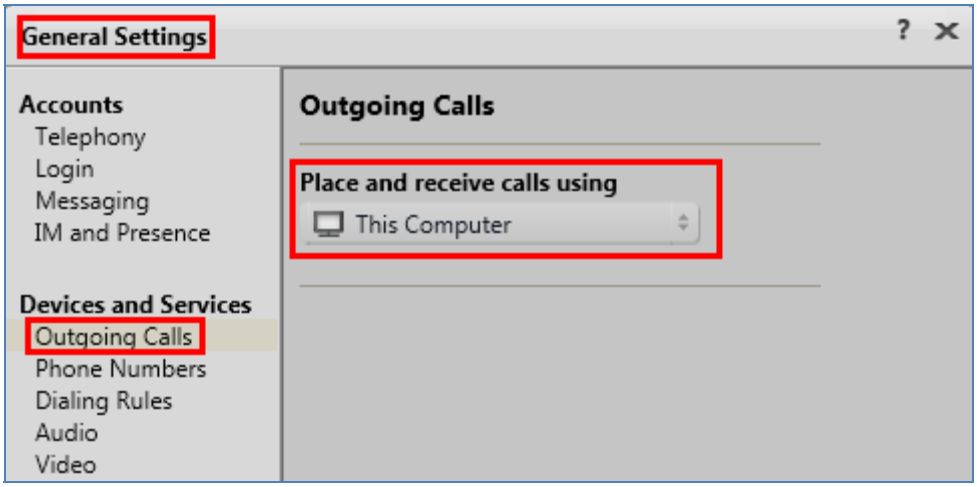
Under **General Settings** the **Messaging** option was selected. The **Enable Message Access** was selected and the **Dial this number** was set to **80960** the hunt group number of the voicemail.



Under **General Settings** the I**M 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**.



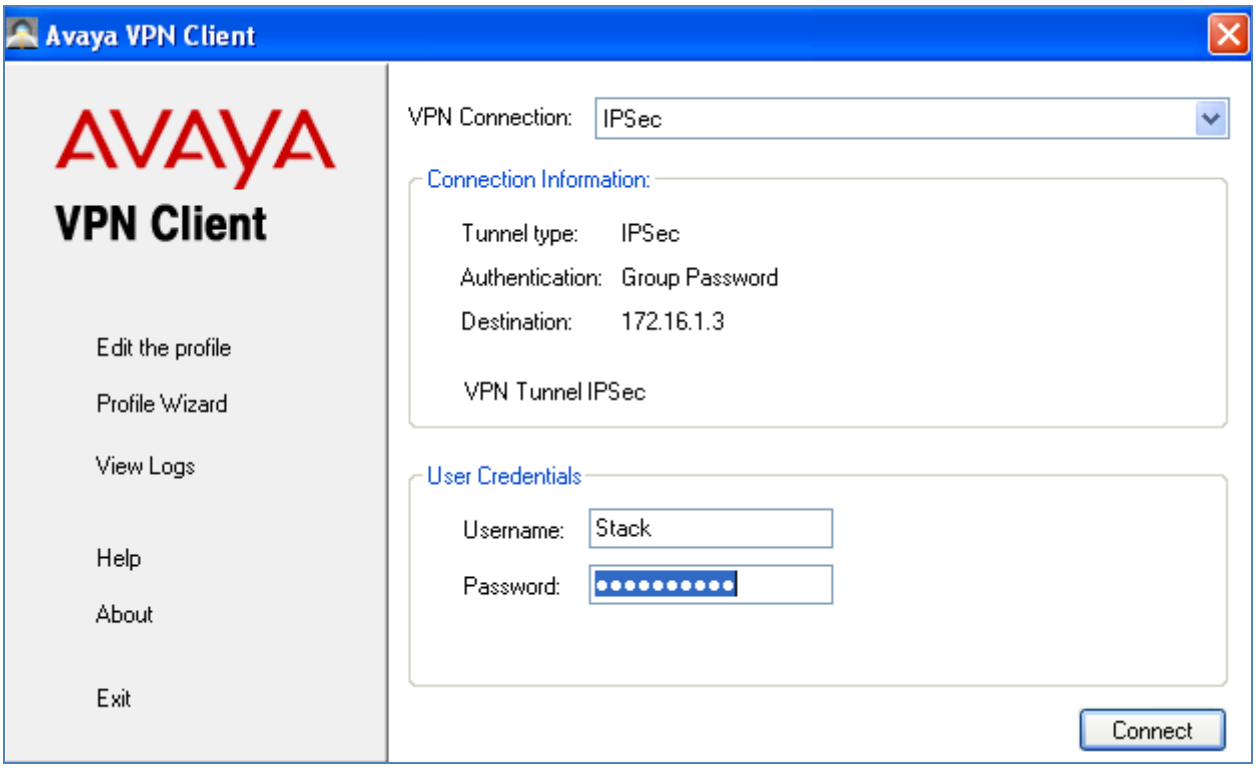
8. Verification Steps

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

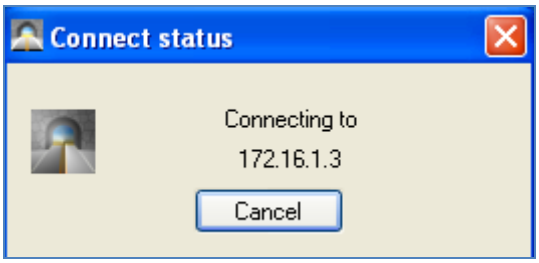
1. Verified the IPSec VPN Tunnel is connected from the remote user pc to the VPN Gateway 3050.
2. Verified one-X Communicator SIP extension 53021 is registered to Session Manager while the IPSec VPN Tunnel is connected.
3. Verified one-X Communicator SIP extension 53021 is able to make a Video Call while 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

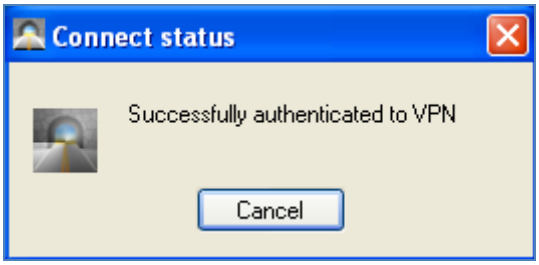
The remote user accesses the IPSec VPN Tunnel by connecting to the IPSec Gateway 172.16.1.3, configured in **Section 5.2,** with VPN client software. The remote user enters the Authentication User account administered in **Section 5.8** and selects the **Connect** button.



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

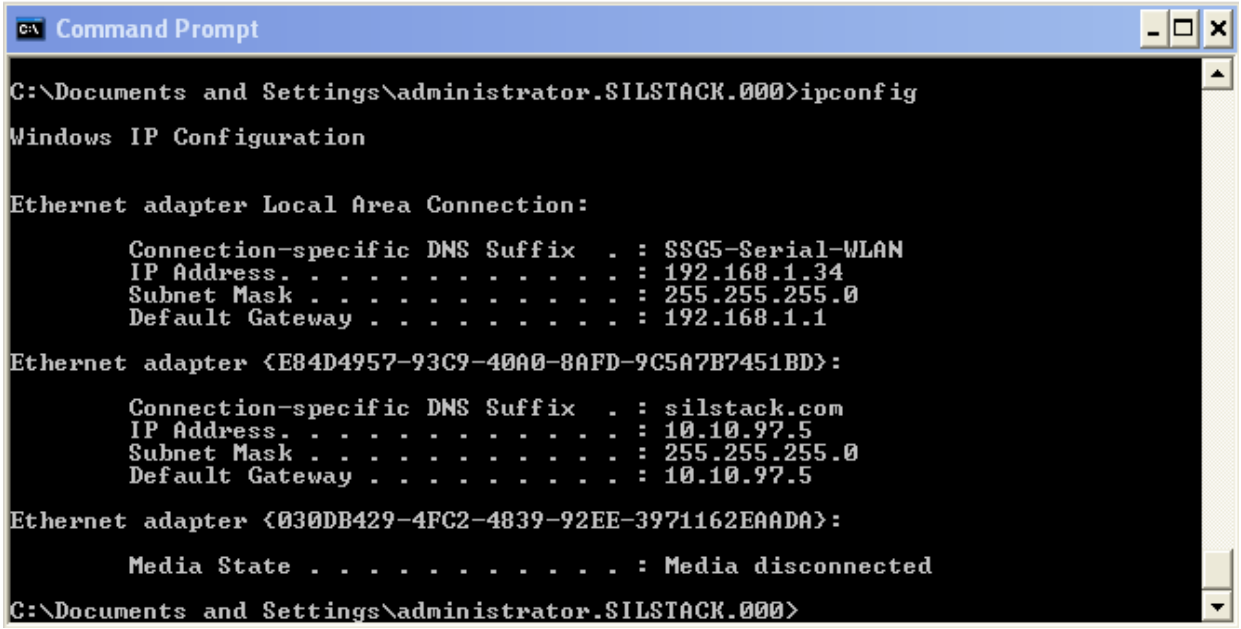


The following screenshot shows the remote user successfully authenticated to the IPSec VPN Tunnel

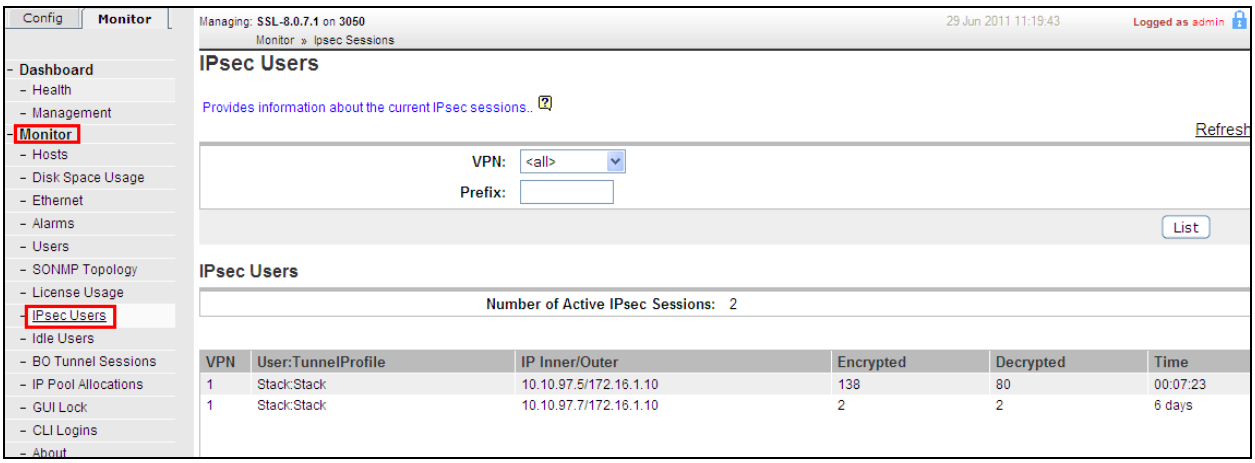


The following screenshot shows a Status of the IPSec VPN Tunnel while connected.

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

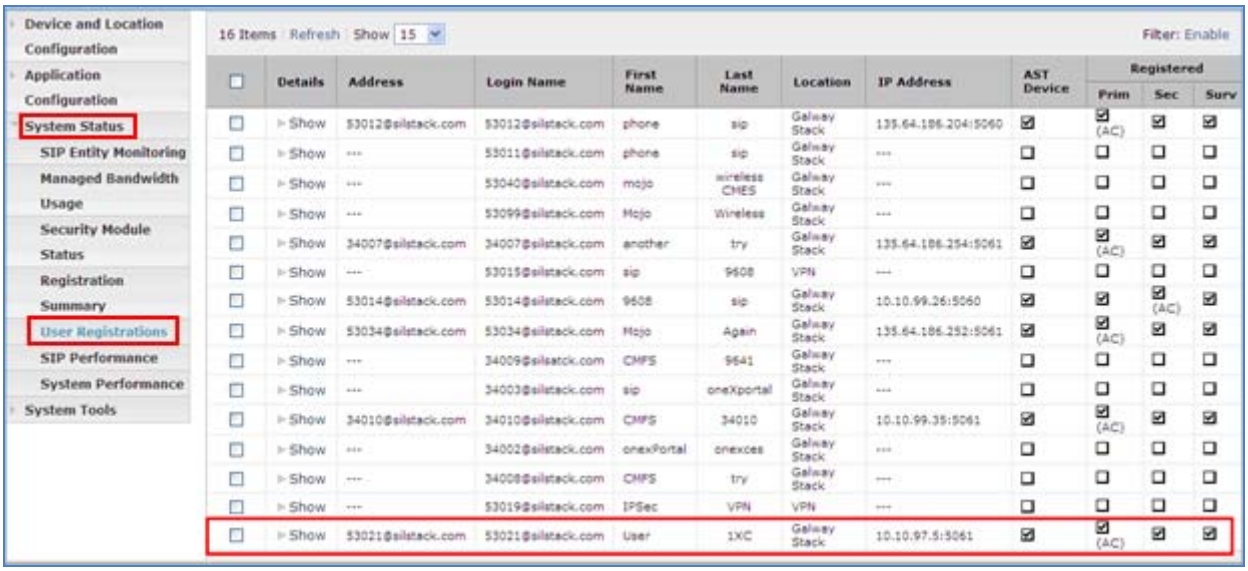


An additional status of the IPSec VPN Tunnel is completed from the VPN Gateway 3050. Under the heading **Monitor** select the subheading **IPSecUser**



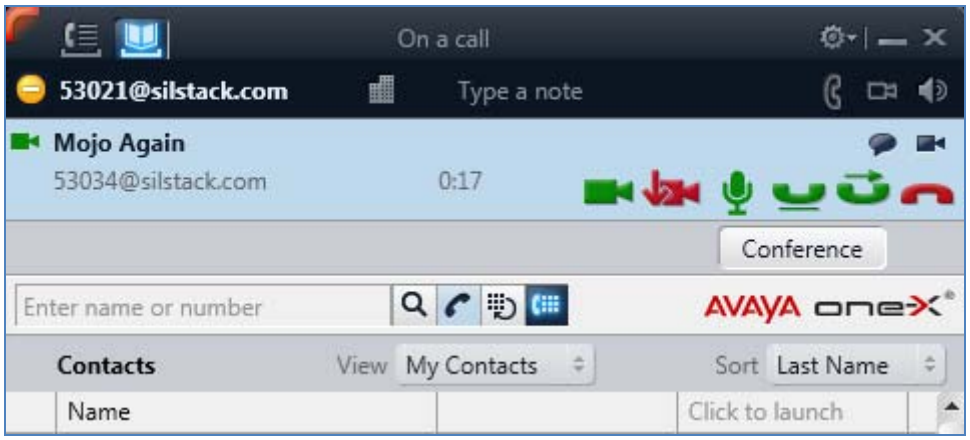
8.2. Verify Avaya one-X® Communicator SIP Registered to Avaya Aura® Session Manager

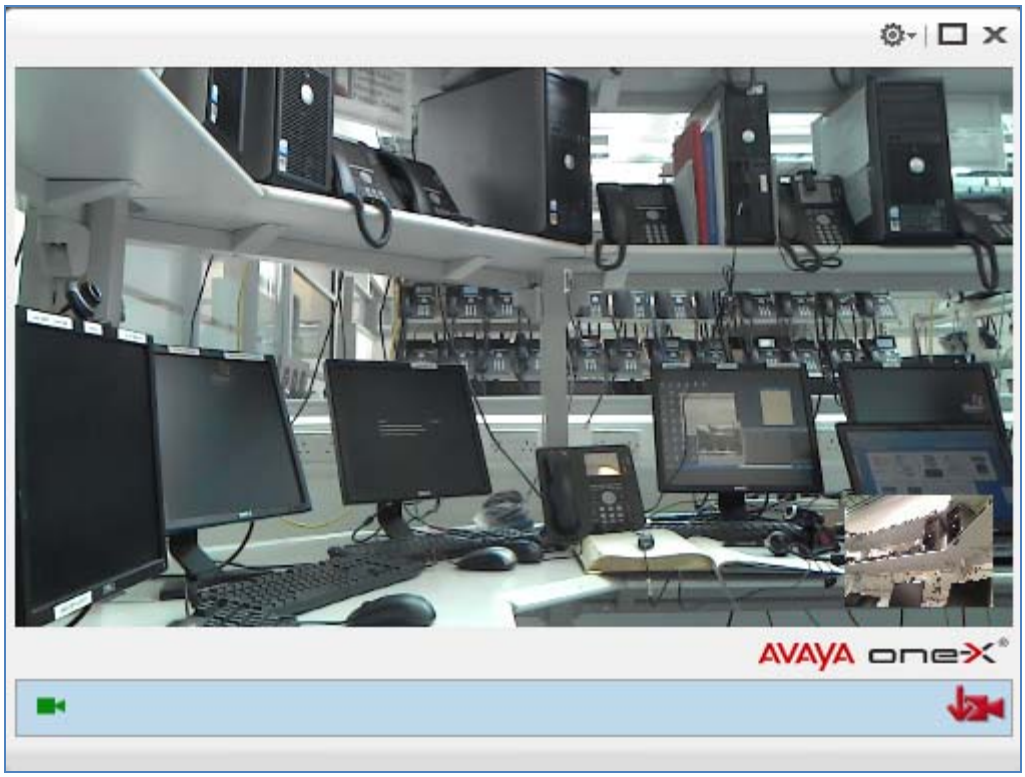
Select **Session Manager → System Status → User Regaisteration.** The following screenshot shows one-X Communicator SIP extension 53021 registered to Session Manager..



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

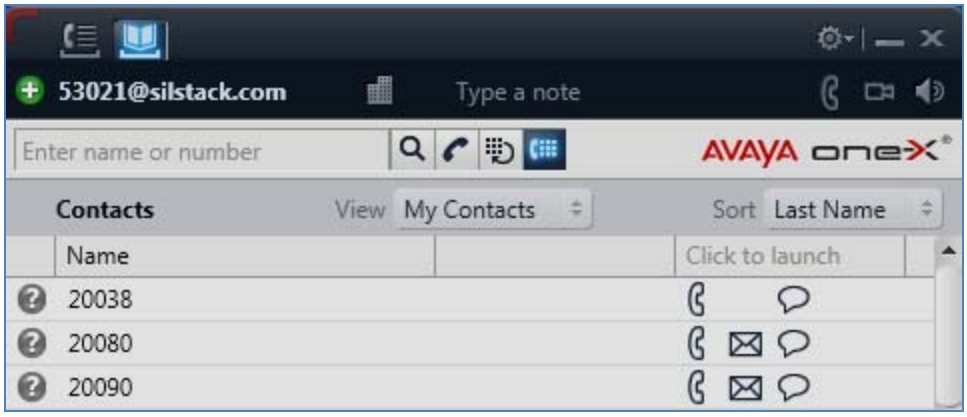
The following screenshots show a successful **Video Call** made from **one-X Communcator SIP** extension **53021** to another video endpoint, while the IPSec VPN Tunnel is connected.



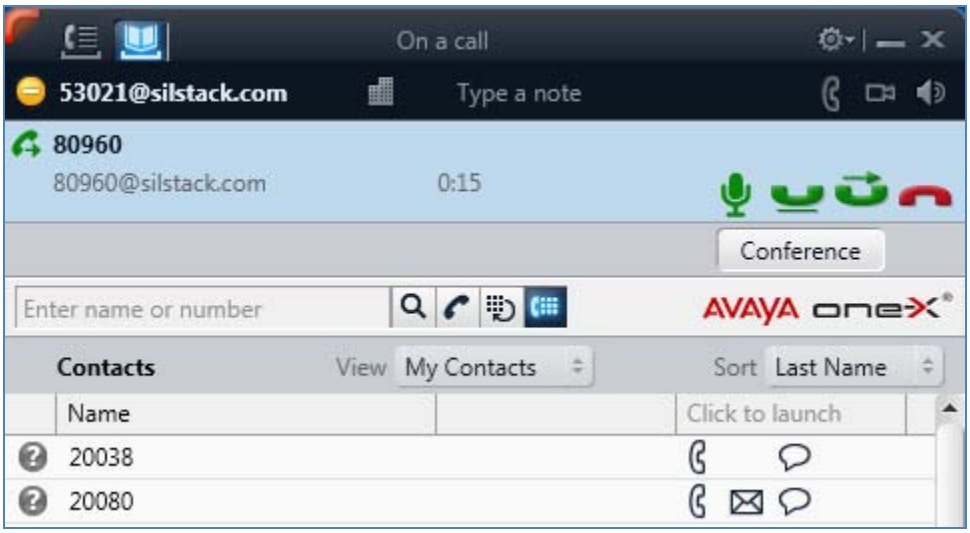


8.4. Verify MWI using Avaya one-X®Communicator SIP

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

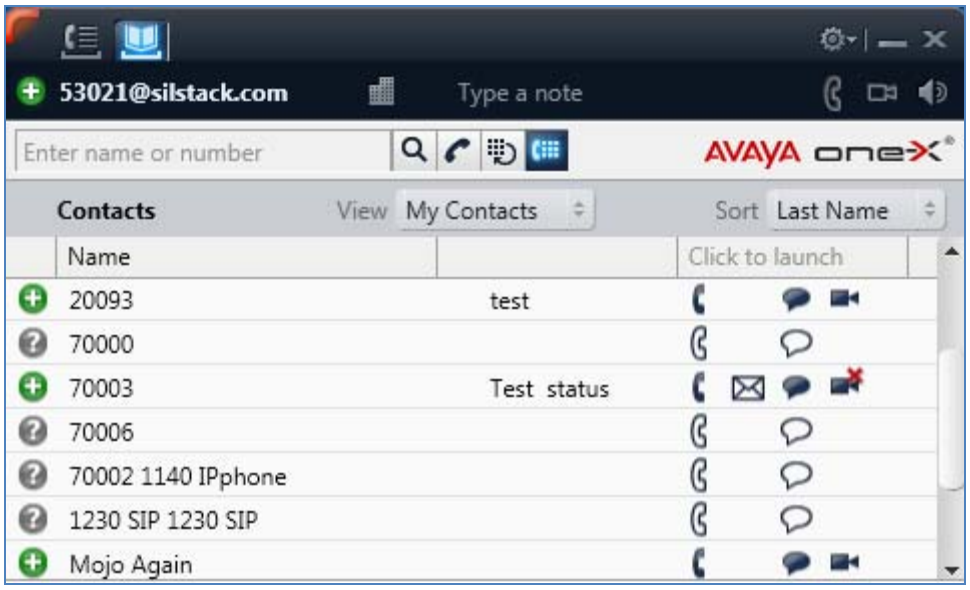


The following screenshot shows that a message can be left with the one-X Communicator SIP extension 53021 and that the message waiting indicator was turned on while the IPSecVPN Tunnel is connected.

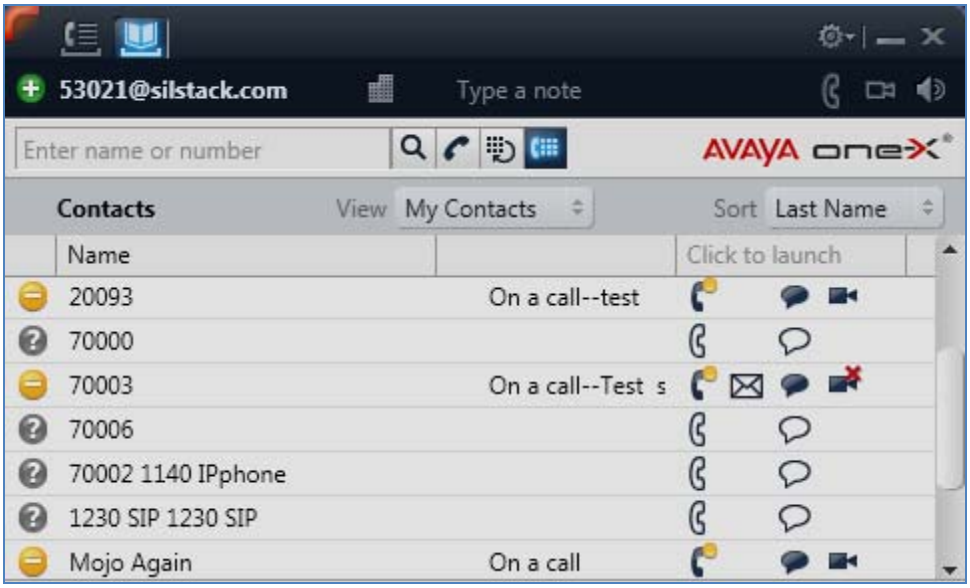


8.5. Verify Presence using Avaya one-X® Communicator SIP

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

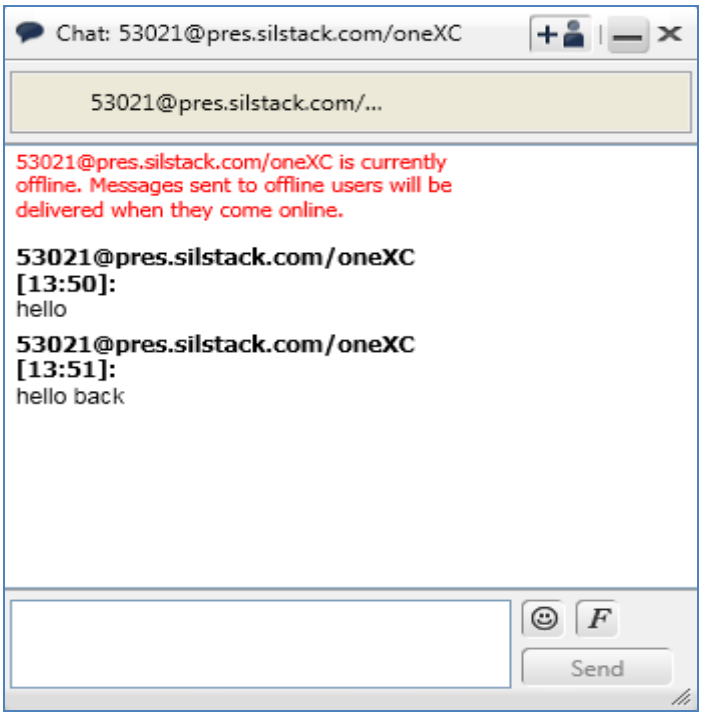


The following screenshot shows Presence busy information for the Contacts of one-X Communicator SIP extension 53021 while the IPSecVPN Tunnel is connected.



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

The following screenshotYou 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.

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