



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Remote User Access to Avaya one-X® Communicator H.323 over VPN Net Direct SSL tunnel using Avaya VPN Gateway 3050 with Avaya Aura® Communication Manager 6.0.1 Issue – 1.0

Abstract

This Application Notes present a configuration where a remote user with Avaya one-X® Communicator H.323 soft client establishes and terminates a VPN Net Direct SSL Tunnel in the main office location with an Avaya VPN Gateway 3050. After completing the VPN Net Direct SSL tunnel negotiation, the Avaya one-X® Communicator H.323 soft client will register to Avaya Aura® Communication Manager R6.0.1.

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

1. Introduction

1.1. Net Direct Client

Avaya Net Direct is a VPN client that can be downloaded to the remote user pc from the Avaya VPN Gateway 3050. When the remote user exits Net Direct or the SSL VPN session, the client is automatically uninstalled. Net Direct client offers a simple and secure access method. Net Direct includes a network driver that captures network traffic and tunnels it through SSL to the Avaya VPN Gateway. The Avaya VPN Gateway then decrypts the traffic and forwards it to the requested destination. The tunneled network destination is configurable. The Net Direct client is packet based, and since it operates at a lower network level, it supports more applications. By clicking on a Web Portal link the Net Direct client is downloaded, installed and launched on the remote user's pc. While Net direct is running in the background, the remote user can access intranet resources through his or her native applications without the need to install VPN client software manually. When the remote user exits Net Direct or the Portal, the client is automatically uninstalled.

1.2. Interoperability Compliance Testing

The objective of this interoperability test is to verify that the Avaya one-X® Communicator H.323 soft client can interoperate with Avaya VPN Gateway 3050 over a VPN Net Direct SSL tunnel, while registered to Avaya Aura® Communication Manager running as an Evolution Server. Another objective is to confirm that Avaya one-X® Communicator H.323 can make a video call, interoperate with Avaya Aura® Messaging and Avaya Aura® Presence Services, while the VPN Net Direct SSL tunnel is established to the Avaya VPN Gateway 3050.

1.3. Configuration

The configuration used in these Application Notes is shown in **Figure 1**. The Avaya Aura® Communication Manager running as an Evolution Server is used to register Avaya one-X® Communicator soft client while the VPN Net Direct SSL tunnel is established. 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. The diagram indicates logical signaling connections. The Avaya Aura® Presence Services Server is used to provide Presence information to one-X® Communicator H.323 soft client. The Avaya Aura® Messaging server is used to provide voicemail functionality and message waiting indicator (mwi) to the one-X® Communicator H.323 soft client. 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 Net Direct SSL tunnel to the remote user pc. The Juniper SSG 5 is used to simulate a broadband connection thus giving the remote user pc access to the internet.

2. Equipment and Software Validated

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

Avaya Aura®	Software
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 Gateway 3050	Release 8.0.7.1
Avaya one-X® Communicator H.323 Soft client	Release 6.1.0.19-GA-31696
Juniper SSG 5 Router	Release 6.1.0r2.0

3. Configure 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 one-X Communicator 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. It was decided to place the one-X Communicator H.323 soft client endpoint, that would reside on the remote users pc, into ip network region 1.

3.1. Administer IP-Codec

This section describes the **IP Codec Set** screen. IP Codec **G.729** was used for testing purposes with the one-X Communicator H.323 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.729	n	2	20
2: G.711A	n	2	20
3: G.711MU	n	2	20
4:			

On **Page 2** set **Allow Direct-IP Multimedia** to **y** (yes). For this configuration a **Maximum Call Rate for Direct-IP Multimedia** 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			

3.2. Administer IP Network Region

This section describes the **IP Network Region** screen. It was decided to place the one-X Communicator H.323 endpoint into **network region 1**. The **Authoritative Domain** was set to **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 **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			

Go to **Page 4** and ensure that ip codec set 1 is used when connection calls to **dst rgn** (destination region) **1**.

display ip-network-region 1										Page 4 of 20	
Source Region: 1 Inter Network Region Connection Management										I	M
										G	A
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c		
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e	
1	1	y	NoLimit					n	all	t	
2	2								all		

3.3. 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 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						

3.4. Administer Station Screen

This screen describes the **station** form setup for the one-X Communicator H.323 endpoint on Communication Manager. The **Extension** used was **20092** with phone **Type 9640**. Phone type 9640 was the recommended phone type to use for the one-X Communicator H.323 endpoint. The **Name** of the phone was set to **H323, 1XC**. The two parameters **IP Softphone** and **IP Video** were set to **yes** to enable the one-X Communicator extension to make a video call.

display station 20092			Page 1 of 5	
STATION				
Extension: 20092		Lock Messages? n	BCC: 0	
Type: 9640		Security Code:	TN: 1	
Port: S00010		Coverage Path 1: 3	COR: 1	
Name: H323, 1XC		Coverage Path 2:	COS: 1	
		Hunt-to Station:		
STATION OPTIONS				
		Time of Day Lock Table:		
Loss Group: 19		Personalized Ringing Pattern: 1		
		Message Lamp Ext: 20092		
Speakerphone: 2-way		Mute Button Enabled? y		
Display Language: english		Expansion Module? n		
Survivable GK Node Name:				
Survivable COR: internal		Media Complex Ext:		
Survivable Trunk Dest? y		IP SoftPhone? Y		
		IP Video? y		

On Page 2, Direct IP – IP Audio Connections were set to yes (y).

display station 20092	Page 2 of 5	
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Audible Message Waiting? n	
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 20092	Always Use? n	IP Audio Hairpinning? n

3.5. Save Translations

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

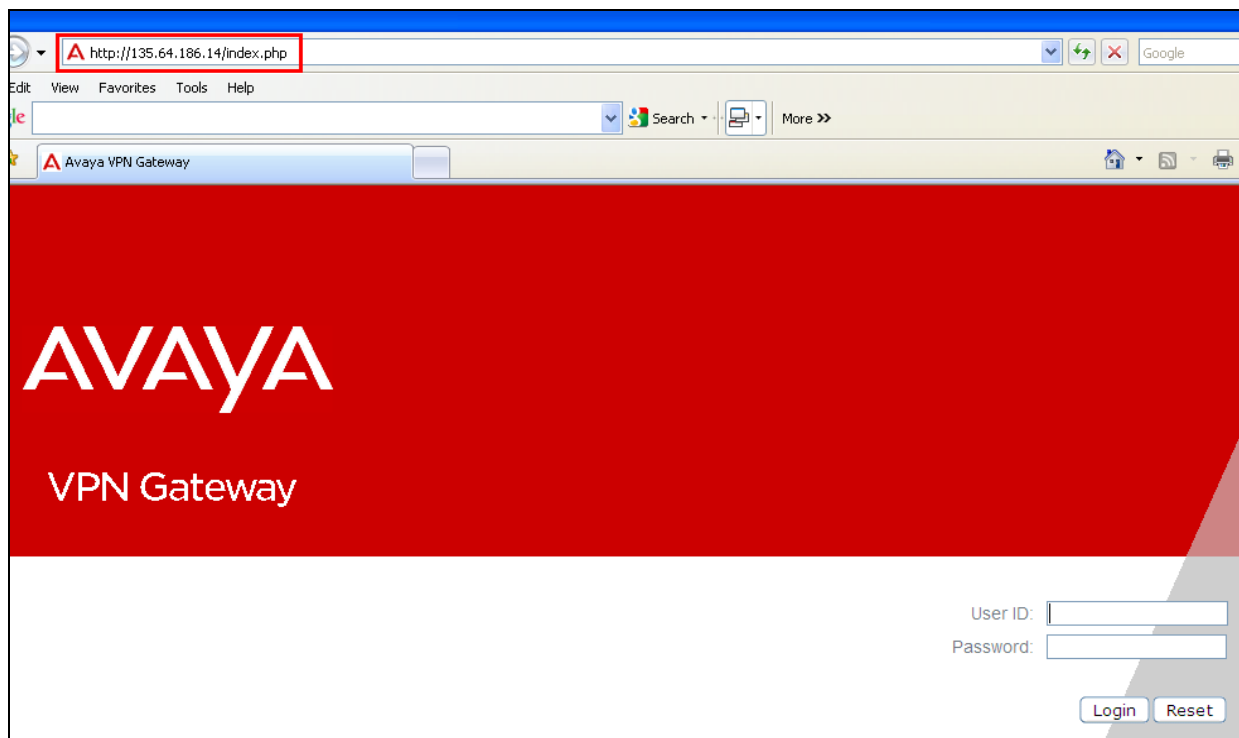
save translation	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

4. Administer Avaya VPN Gateway 3050

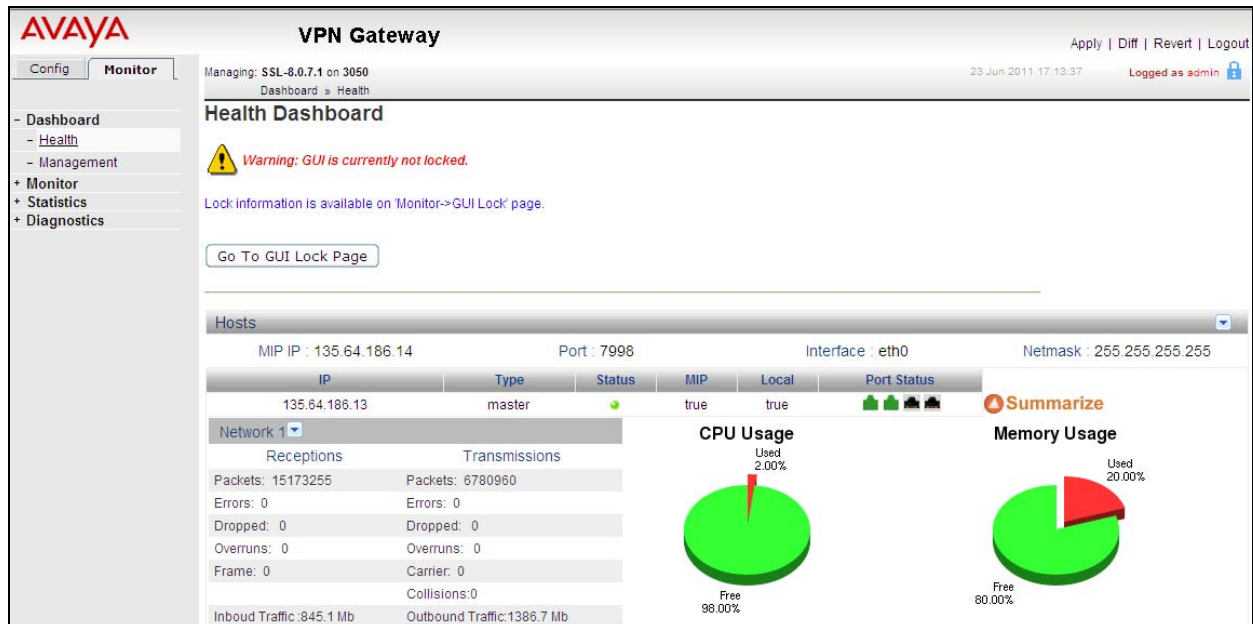
The following steps describe configuration of the VPN Gateway 3050. This section will describe the server configuration needed to establish a VPN Net Direct SSL tunnel between the remote user pc and VPN Gateway 3050. It will describe administering an IP Pool, enabling Net Direct, configuring Split Tunneling and administering a Net Direct link to establish the VPN Net Direct SSL tunnel. This section will also describe configuring the Avaya 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. It will also detail setting up static routes and the creation of the SSL VPN Gateway or Gateway Portal . It will also describe creating a Trusted Group and assigning the Net direct Link to that Group. Administering of User Accounts is also discussed.

4.1. 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.



4.2. Administer Public Private Interface

Select **Config** → **Host(s)** on the graphical user interface to configure the public and private side of the VPN Gateway. In order to have 135.64.186.x network side configured as the private interface and the 172.16.1.x network side configured as the public interface, the **Default Gateway** was set to **172.16.1.2**. Select **Update**.

AVAYA VPN Gateway

Managing: SSL-8.0.7.1 on 3050
Cluster » Host-isd@a135-64-186-13 » System

24 Jun 2011 09:50:04 Logged as admin

System Information

Assigns an administratively-assigned name to the managed Avaya VPN Gateway (AVG) host and also adds a description of the physical location of the managed AVG host.

General Host Routes Ports Interfaces Licenses

Host Type: master

System Name:

System Location:

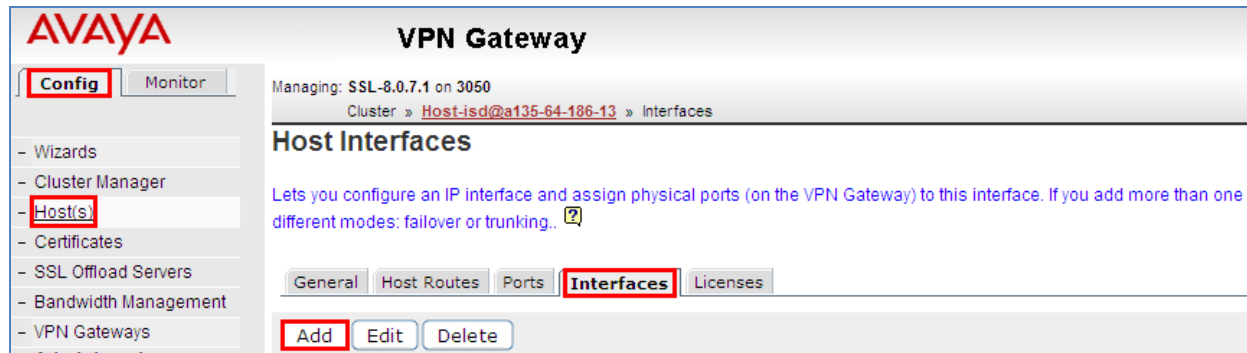
Default Gateway: 172.16.1.2 (format: 10.10.1.75, 0.0.0.0 to remove)

Dont Fragment bit: copy

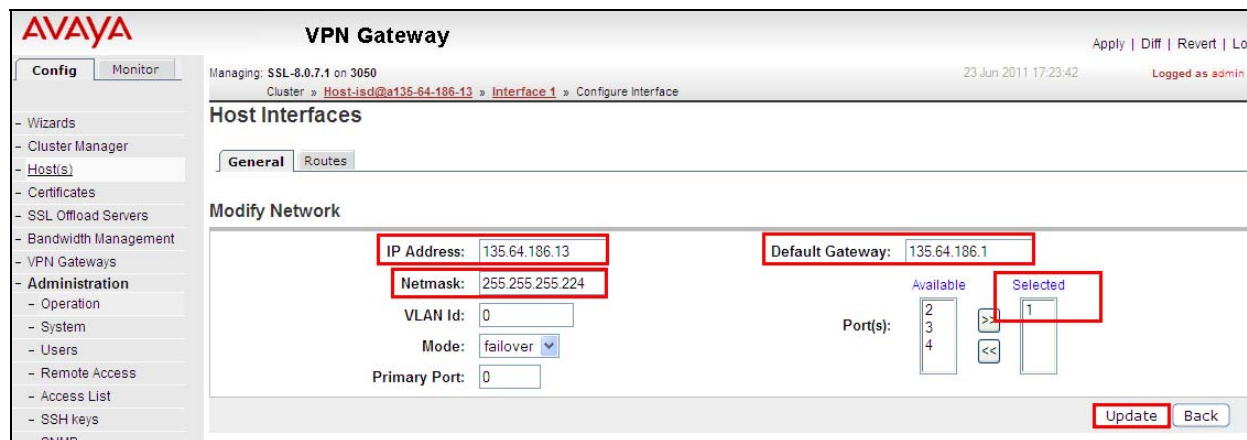
Update

4.3. Administer Interface One

Select **Config** → **Hosts** → **Interfaces** on the graphical user interface of the VPN Gateway 3050. Select the **ADD** option.

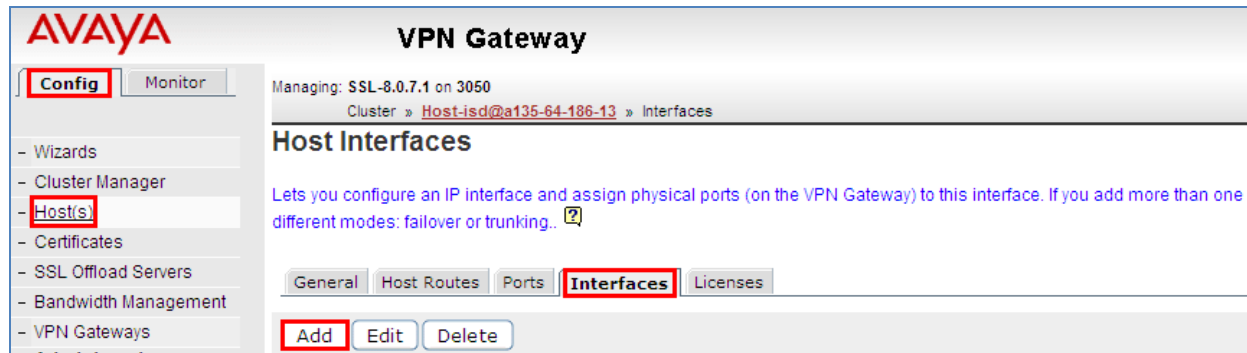


Interface One had **IP address** set to **135.64.186.13**, the inside interface. The **Netmask** was set to **255.255.255.224** and the **Default Gateway** was **135.64.186.1**. Interface **1** was **Selected** from the **Port(s)** column. The **Update** button was selected to update the configuration.

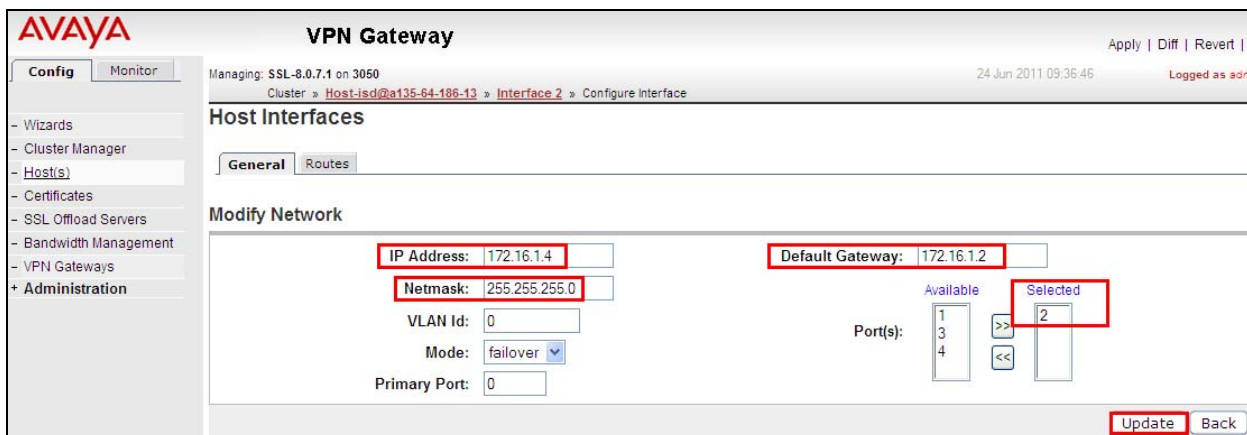


4.4. Administer Interface Two

Select **Config** → **Hosts** → **Interfaces** on the graphical user interface of the VPN Gateway 3050. Select the **ADD** option.



Interface Two had **IP address** set to **172.16.1.4**, the outside interface. The **Netmask** was set to **255.255.255.0** and the **Default Gateway** was **172.16.1.2**. Interface **2** was **Selected** from the **Port(s)** column. The **Update** button was selected to update the configuration.

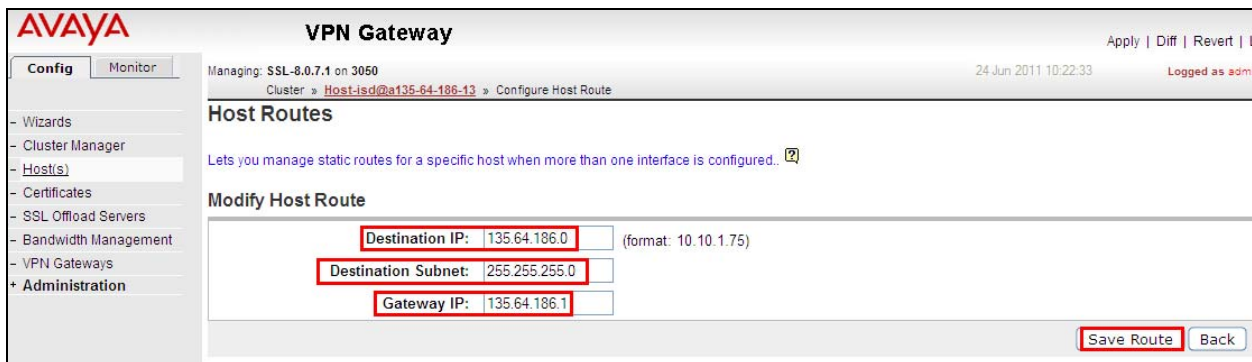


4.5. Administer Static Routes

A static route was created to ensure traffic on the Private network would use interface one. Select **Config** → **Host(s)** → **Host Routes** on the graphical user interface of the VPN Gateway 3050. Select the **ADD** option.



The **Destination IP** was set to **135.64.186.0**. The **Destination Subnet** was set to **255.255.255.0**. The **Gateway IP** was set to **135.64.186.1**. The **Save Route** button was selected to save the changes.



4.6. Administer SSL VPN Gateway

To create the SSL VPN Gateway, select **Config** → **VPN Gateway** on the graphical user interface. Select the **Add** button.



The **VPN Name** was **SSL**. The SSL VPN Portal **IP Address** was set to **172.16.1.6**. This is the IP Address the remote user will use to access the SSL VPN tunnel. The default **Port** number was **443**. The **SSL Status** was **enabled**. The **Create VPN** button was selected to save the changes.

AVAYA VPN Gateway

Managing: SSL-8.0.7.1 on 3050
VPN Gateways » Add a VPN

24 Jun 2011 11:06:09 Logged as admin

VPN Gateways

Add a VPN

VPN Identifier: 3

VPN Name: SSL

IP Address: 172.16.1.6

Port: 443 (1-65534)

SSL Status: enabled

Certificate Number: <unset>

Warning: New VPNs are directly applied to the database.

Create VPN Back

The following screen is displayed.

AVAYA VPN Gateway

Managing: SSL-8.0.7.1 on 3050
VPN Gateways

24 Jun 2011 13:05:02 Apply

VPN Gateways

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

Add Edit Delete Quick VPN

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

4.7. Administer IP Pool

To administer the IP Pool, select **Config** → **VPN Gateway** → **VPN 2**. Then under settings select **IP Pool** on the graphical user interface.

AVAYA VPN Gateway

Managing: SSL-8.0.7.1 on 3050
VPN Gateways » VPN-2

VPN Summary

Settings	Configuration
General	VPN Name : SSL, Standalone Mode is enabled, WholeSecurity is off.
SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is ssl.silstack.com.....
Traffic Trace	Lets you traceroute or ping a host.
IP Pool	Default IP Pool is 2, The configured IP Pools are
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. 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 'IP Pool' configuration. A text box explains the IP Pool menu's purpose. Below this, there's a 'Default IP Pool' section with a dropdown menu set to '2' and 'SSL'. The 'IP Pool List' table shows one entry with ID '2', Name 'SSL', Type 'local', Proxy ARP 'on', and Status 'on'. The 'Add' button in the table's toolbar is highlighted with a red box.

ID	Name	Type	Proxy ARP	Status
2	SSL	local	on	on

For the SSL VPN Gateway **VPN 2**. The IP Pool **Name** was set to **SSL**. 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 'IP Pool Configuration' page for adding a new IP address pool. The 'VPN' dropdown is set to '2'. The 'IP Pool ID' dropdown is set to '1'. The 'Name' text field contains 'SSL'. The 'Status' dropdown is set to 'enabled'. The 'Type' dropdown is set to 'local'. The 'Proxy ARP' dropdown is set to 'on'. The 'Update' button is highlighted with a red box.

Under the **General Settings** of the IP Pool **named SSL**. The **Lower IP** address was set to **10.10.97.21** and the **Upper IP** address was set to **10.10.97.40**. The **Update** button was selected to save the changes.

The screenshot shows the 'Modify IP Address Pool' page for the 'SSL' pool. The 'General' tab is selected. The 'Name' text field contains 'SSL'. The 'Status' dropdown is set to 'enabled'. The 'Type' dropdown is set to 'local'. The 'Proxy ARP' dropdown is set to 'on'. The 'Lower IP' text field contains '10.10.97.21'. The 'Upper IP' text field contains '10.10.97.40'. The 'Update' button is highlighted with a red box.

4.8. Enable Net Direct

To enable Net Direct select **Config** → **VPN Gateway** → **VPN 2**. Then under **Settings**, select **VPN Client** on the graphical user interface.

AVAYA VPN Gateway

Managing: SSL-8.0.7.1 on 3050

VPN Gateways » VPN-2

VPN Summary

Settings	Configuration
IPsec	IPsec is disabled, IKE Profiles.... , User Tunnel Profiles.... , BO Tunnel Profiles....
L2TP	L2TP is disabled, IKE Profiles.... , User Tunnel Profiles....
NAP	Automatic Remediation is disabled, Probation settings is disabled, Remote policy servers.... , Svst
Portal	Citrix support is off, Company Name is Avaya Inc., SMB Workgroup is WORKGROUP, ReDirect URL is
Link Sets	Configured Linksets are base-links, netdirect, installed_ND
Authorization	Configured Networks are NIL. Configured Services are http, https, web, smtp, pop3, imap, email, telnet, ssh, ftp, smb, fileshare. Configured Client Filters are NIL. Configured Applications are NIL. 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
EACA	EACA is disabled, Failover action : teardown. No SRS rules are configured.
VPN Client	Net Direct is on, Split Networks are 135.64.186.70/255.255.255.255, 135.64.186.40/255.2....

Under VPN Client select **Net Direct**. In the **General Settings** set **Net Direct Client** to **on**. The **Update** button was selected to save the changes.

Net Direct Split Networks FailOver Servers Old Clients XML Configuration TDI LSP Mobility Advanced

Net Direct links should be configured for any of the configured linksets in [VPN Gateways->VPN-2->Linksets](#) page.

General Settings | Net Direct Banner | Net Direct License | Download Net Direct Setup

General Settings

Net Direct Client: on

Idle Check: off

Retry Connection Time: 180 (seconds)

Rekey Traffic Limit: 0

Rekey Time Limit: 28800 (seconds)

UDP Port: 5000-5001

Net Direct/SPO Operating Systems:

Available	Selected
generic_win	all winxp
linux	
mac	
unknown	
vista	
win2k	
win7	

Update

Under **Split Networks** the **Split Tunnel Mode** was **disabled** to tunnel all the network traffic through the Net Direct client to the SSL VPN Gateway. The **Update** button was selected to save the changes.

Managing: SSL-8.0.7.1 on 3050 24 Jun 2011 14:16:36 Logged as admin

[VPN Gateways](#) » [VPN-2](#) » VPN Client » Split Tunnels

Networks for Split Tunnels

Allows you to configure the network ranges or IP addresses to which traffic should be tunneled through the VPN Gateway.. [?](#)

Net Direct **Split Networks** FailOver Servers Old Clients XML Configuration TDI LSP Mobility Advanced

Split Tunnel Mode: disabled

Update

4.9. Administer Net Direct Link

To administer a Net direct Link select **Config** → **VPN Gateway** → **VPN 2**. Then under **Settings** select **Link Sets** on the graphical user interface.

AVAYA **VPN Gateway**

Managing: SSL-8.0.7.1 on 3050 [VPN Gateways](#) » [VPN-2](#)

VPN Summary

Settings	Configuration
General	VPN Name : SSL, Standalone Mode is enabled , WholeSecurity is off .
SSL	SSL is enabled , Server Certificate is 1, Listen Port is 443, DNS name of VIP is ssl.silstack.com.
Traffic Trace	Lets you traceroute or ping a host.
IP Pool	Default IP Pool is 2, The configured IP Pools are
Host IP Pool	Host IP Pool is disabled
IPsec	IPsec is disabled , IKE Profiles.... , User Tunnel Profiles.... , BO Tunnel Profiles....
L2TP	L2TP is disabled , IKE Profiles.... , User Tunnel Profiles....
NAP	Automatic Remediation is disabled , Probation settings is disabled , Remote policy servers....
Portal	Citrix support is off , Company Name is Avaya Inc., SMB Workgroup is WORKGROUP, ReDirect U
Link Sets	Configured Linksets are base-links , netdirect , Installed_ND Configured Networks are NIL .

Under the **Portal Linksets** select the **Add** option.

[VPN Gateways](#) » [VPN-2](#) » [Linksets](#)

Portal Linksets

Allows you to create a linkset, i.e. a set of hypertext links that can be accessed from simultaneously.. [?](#)

Add **Edit** **Delete** **Copy** **Paste**

<input type="checkbox"/>	ID	Name
<input type="checkbox"/>	1	base-links

In the **Add New Linkset**, the **Name** for **netdirect** was added. The **Update** button was selected to save the changes.

In the **Add Portal Links** the **Link Type** was set to **NetDirect**. The **Continue** button was selected.

The following **netdirect** link was created.

<input type="checkbox"/>	ID	Name
<input type="checkbox"/>	1	base-links
<input type="checkbox"/>	2	netdirect
<input type="checkbox"/>	3	Installed_ND

4.10. Administer Trusted Group

To administer a Trusted Group select **Config** → **VPN Gateway** → **VPN 2**. Then under **Settings** select **Groups** on the graphical user interface.

AVAYA

VPN Gateway

Config

Monitor

Wizards

Cluster Manager

Host(s)

Certificates

SSL Offload Servers

Bandwidth Management

VPN Gateways

Administration

Managing: SSL-8.0.7.1 on 3050

VPN Gateways » VPN-2

VPN Summary

Settings	Configuration
General	VPN Name : SSL, Standalone Mode is enabled, WholeSecurity is off.
SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is ssl.silstack.com
Traffic Trace	Lets you traceroute or ping a host.
IP Pool	Default IP Pool is 2, The configured IP Pools are
Host IP Pool	Host IP Pool is disabled
IPsec	IPsec is disabled, IKE Profiles....., User Tunnel Profiles....., BO Tunnel Profiles.....
L2TP	L2TP is disabled, IKE Profiles....., User Tunnel Profiles.....
NAP	Automatic Remediation is disabled, Probation settings is disabled, Remote policy servers.....
Portal	Citrix support is off, Company Name is Avaya Inc., SMB Workgroup is WORKGROUP, ReDirect
Link Sets	Configured Linksets are base-links, netdirect, Installed_ND
Authorization	Configured Networks are NIL. Configured Services are http, https, web, smtp, pop3, imap, email, telnet, ssh, ftp, smb, fileshare Configured Client Filters are NIL. Configured Applications are NIL. 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 **Add** button under Groups.

Wizards

Cluster Manager

Host(s)

Certificates

SSL Offload Servers

Bandwidth Management

VPN Gateways

Administration

VPN Gateways » VPN-2 » 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 IPsec client) the user is assigned to a group membership. This is done by searching for a match between a group name defined, and a group name associated with the user's credentials (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.

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.

Add Edit Delete Copy Paste			
<input type="checkbox"/> ID	Name	User Type	Comment
<input type="checkbox"/> 1	trusted	advanced	

After selecting the group named **trusted** the following page is displayed. The **IP Pool** called **SSL** created in **Section 4.7** was assigned to the group named **trusted**. The **Update** button was selected to save the changes.

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: administrator

Net Direct Windows Admin Password:

Net Direct Windows Admin Password (again):

IP Pool: 2 SSL

Host IP Pool: <None>

Maximum Sessions: 0 (0 is unlimited)

Session Idle Time: 0 (seconds)

Maximum Session Length: 0 (seconds)

Comment:

Update

4.11. Map Net Direct Linkset to Trusted Group

To map the linkset to the trusted group select **Linksets** under **Modify a Group**.

managing: SSL-6.0.7.1 on 3030

VPN Gateways » VPN-2 » Group-1 » Modify Group

Modify a Group

Lets you configure the general settings of a user group.. ?

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


Name:

User Type:

Under **Linksets**, select the option **To add a new portal linkset, click here.**

Allows you to map linksets to the current group.. ?

General Access Lists **Linksets** EACA IPsec L2tp VPN Admin Net Direct

 No new portal linksets remaining. To add a new portal linkset, click [here](#).


Under **Portal Linksets**, the **Linksets** for **netdirect** from Section 4.9 was added.

VPN Gateways » VPN-2 » Group-1 » Linksets

Portal Linksets

Allows you to map linksets to the current group.. ?

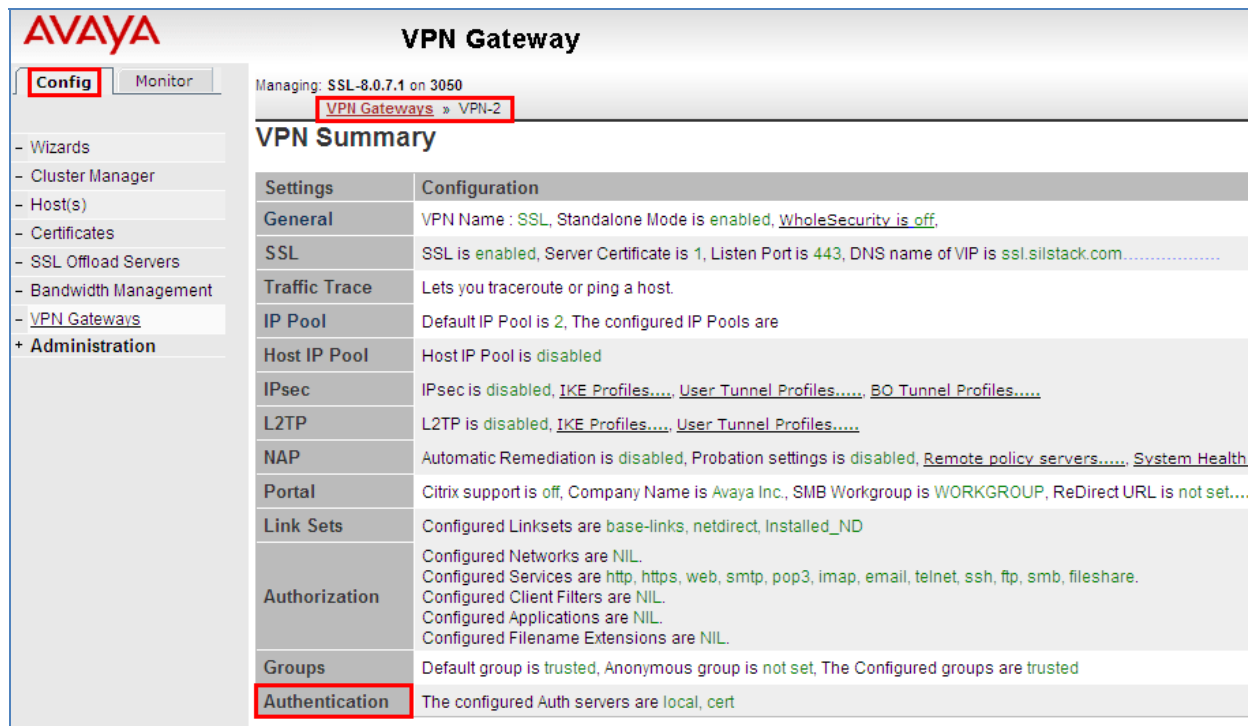
General Access Lists **Linksets** EACA IPsec L2tp VPN Admin Net Direct

 No new portal linksets remaining. To add a new portal linkset, click [here](#).

<input type="checkbox"/>	ID	Name
<input type="checkbox"/>	1	base-links
<input type="checkbox"/>	2	Installed_ND
<input type="checkbox"/>	3	netdirect

4.12.Administer User Authentication

To administer an Authentication Account, select **Config → VPN Gateway → VPN 2**. Then under **Settings** select **Authentication** on the graphical user interface.



AVAYA **VPN Gateway**

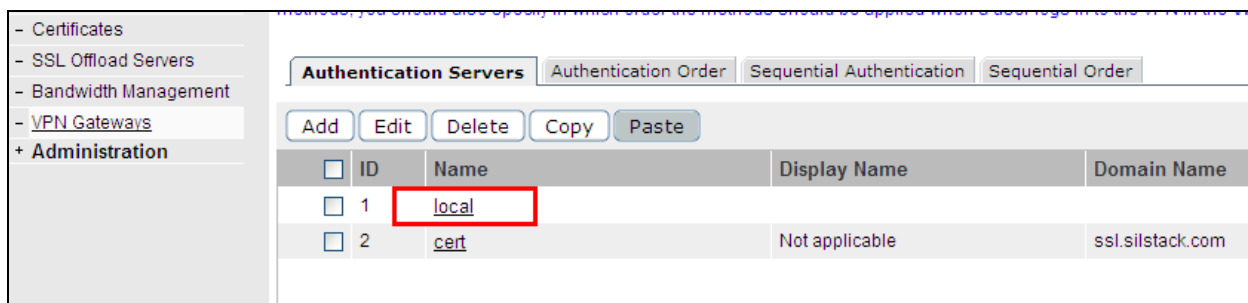
Managing: SSL-8.0.7.1 on 3050

VPN Gateways » VPN-2

VPN Summary

Settings	Configuration
General	VPN Name : SSL, Standalone Mode is enabled , WholeSecurity is off .
SSL	SSL is enabled , Server Certificate is 1, Listen Port is 443, DNS name of VIP is ssl.silstack.com.....
Traffic Trace	Lets you traceroute or ping a host.
IP Pool	Default IP Pool is 2, The configured IP Pools are
Host IP Pool	Host IP Pool is disabled
IPsec	IPsec is disabled , IKE Profiles..... , User Tunnel Profiles..... , BO Tunnel Profiles.....
L2TP	L2TP is disabled , IKE Profiles..... , User Tunnel Profiles.....
NAP	Automatic Remediation is disabled , Probation settings is disabled , Remote policy servers..... , System Health
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, netdirect, Installed_ND
Authorization	Configured Networks are NIL. Configured Services are http, https, web, smtp, pop3, imap, email, telnet, ssh, ftp, smb, fileshare. Configured Client Filters are NIL. Configured Applications are NIL. 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 VPN Gateway 3050 after installation.



Authentication Servers **Authentication Order** **Sequential Authentication** **Sequential Order**

Add **Edit** **Delete** **Copy** **Paste**

<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 **Users** option.

Managing: SSL-8.0.7.1 on 3050
 VPN Gateways » VPN-2 » Auth Server-1 » General

Authentication Servers

Allows you to configure the general settings of Local Database authentication method.. ?

General **Users** Password Change Advanced

Name:

Display Name:

Then select the **Add** button.

General **Users** Password Change Advanced

Prefix: Max:

Users

Lets you add user(s) to the local authentication database. When the user attempts to log in to the VPN and local database authentication password you define here. The group name is used for authorization, controlling access to resources by checking the specified group. The group name you specify when adding a user must therefore exist in the current VPN, along with one or more access resources.

Add Edit Delete Import/Export

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.

Managing: SSL-8.0.7.1 on 3050 24 Jun 2011 16:01:33 Logged in

VPN Gateways » VPN-2 » Auth Server-1 [Local] » Add/Modify User(s)

Users

[Add Single User](#) | [Add Bulk Users](#)

Add Single User

Name:

Password:

Password (again):

Available Selected

Groups:

Warning: Users are added immediately to the database. No apply is required.

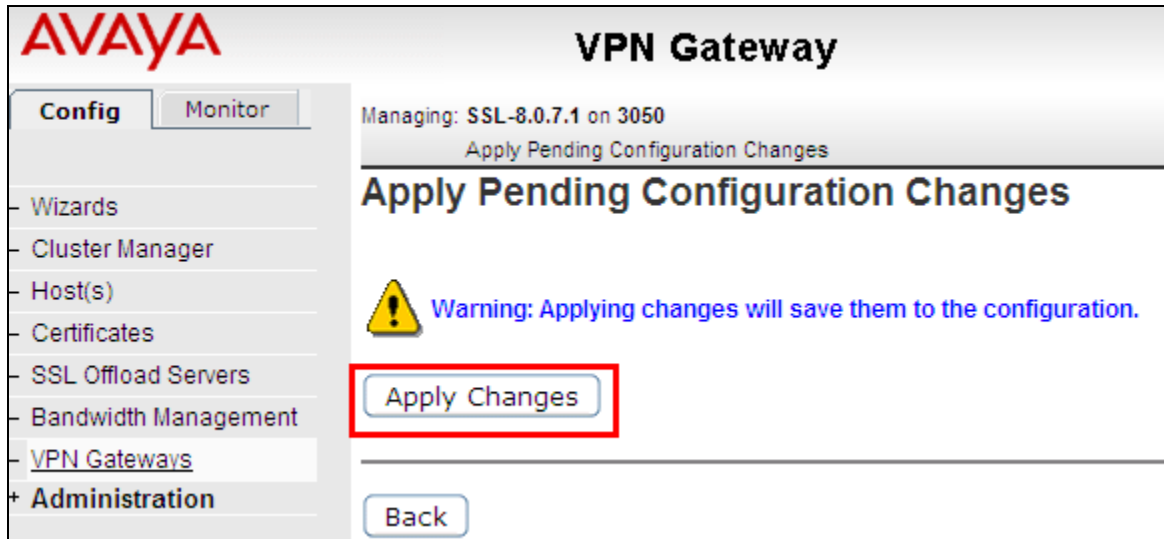
Save User Back

4.13. Apply Changes

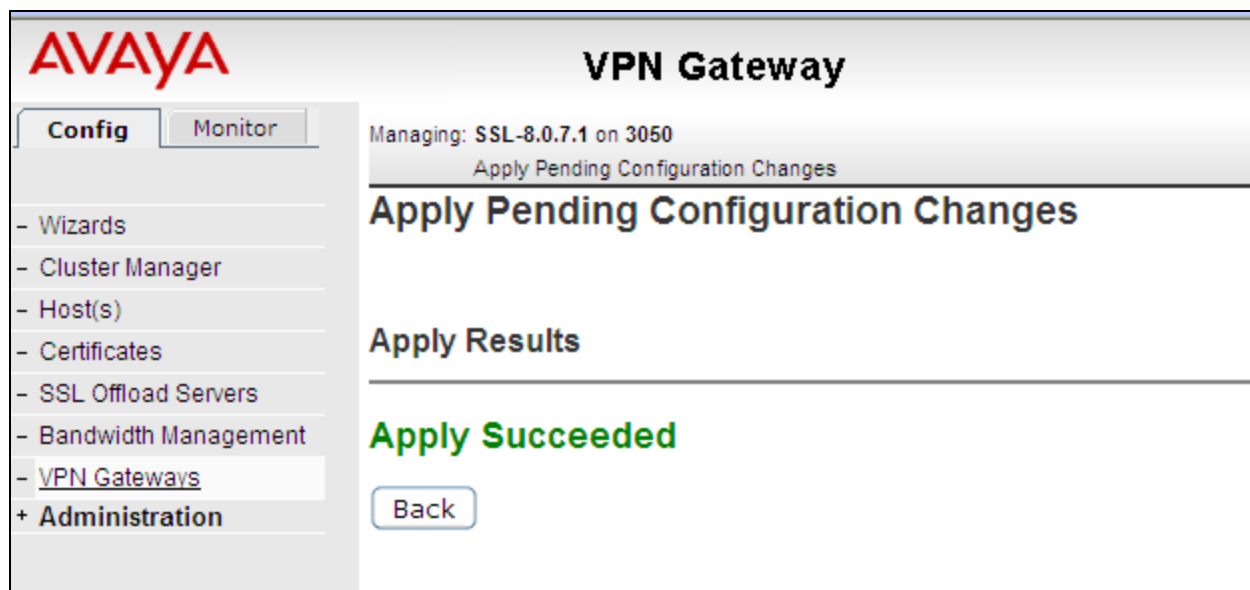
For the changes to take effect on the VPN Gateway 3050 select the **Apply** button on the top right hand side of the graphical user interface.



Select the **Apply Changes** button.

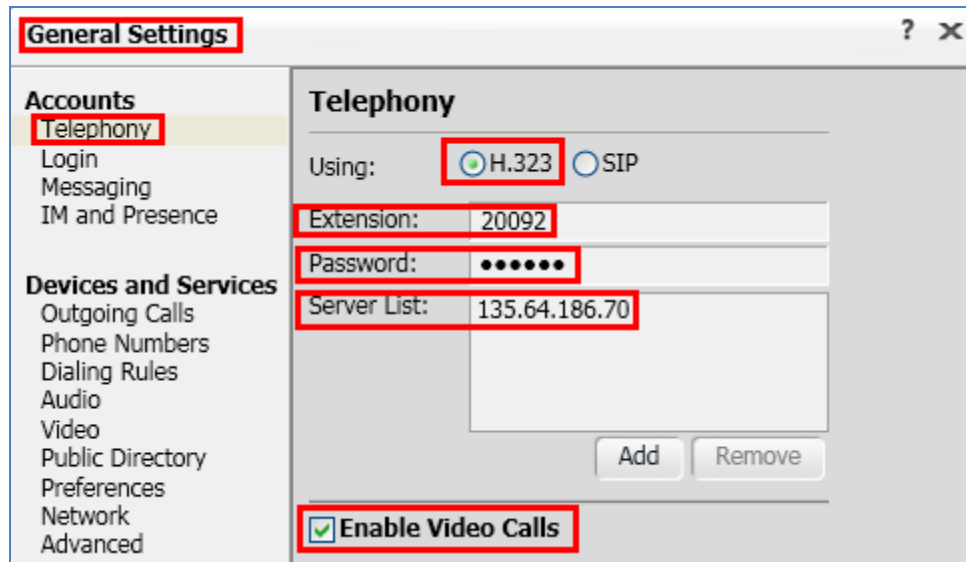


The following screenshot shows the changes were successful.

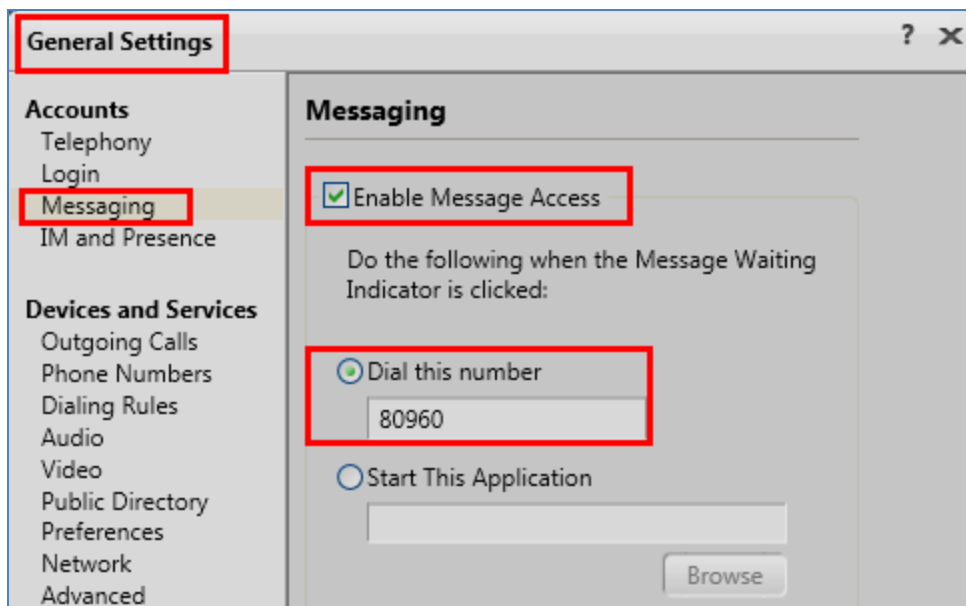


5. Avaya one-X® Communicator H.323 Settings

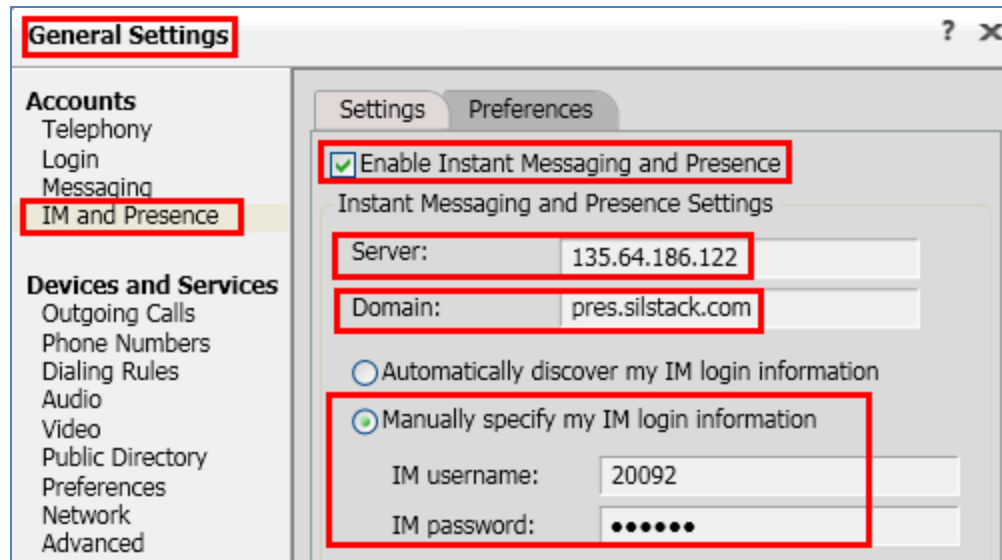
The following section describes the settings needed to administer one-X Communicator H.323 soft client. On the one-X Communicator H.323 soft client select **General Settings**. Under **Telephony** the **H.323** option was enabled. The **Extension** was set to **20092**. The **Password** was set and the **Server list** was set to **135.64.186.70**. This is the IP Address of the PROCR in Communication Manager. The **Enable Video Calls** was also selected.



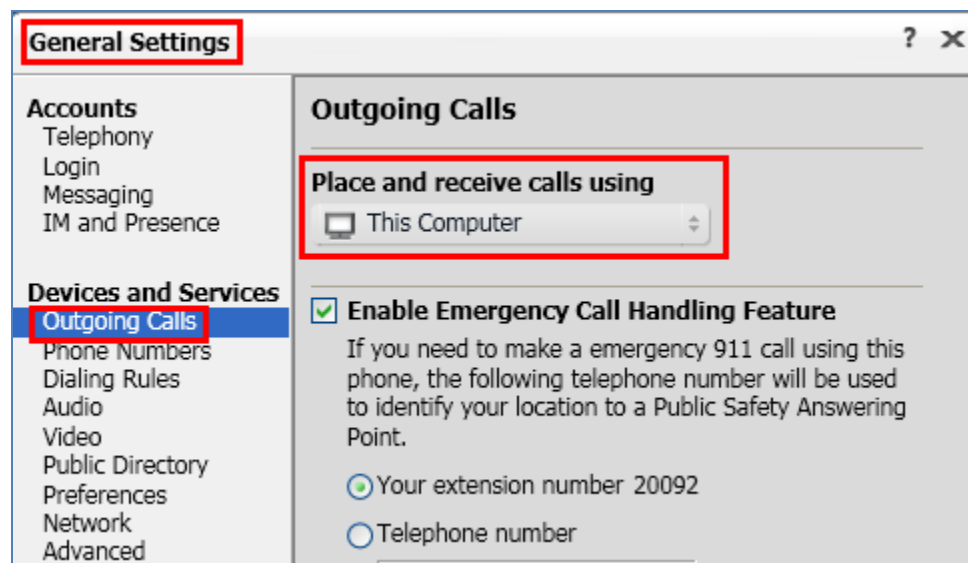
Under **General Settings** the **Messaging** option was selected. The **Enable Message Access** was selected and the **Dial this number** was set to **80960**, the hunt group number of the voicemail.



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 **20092** 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**.



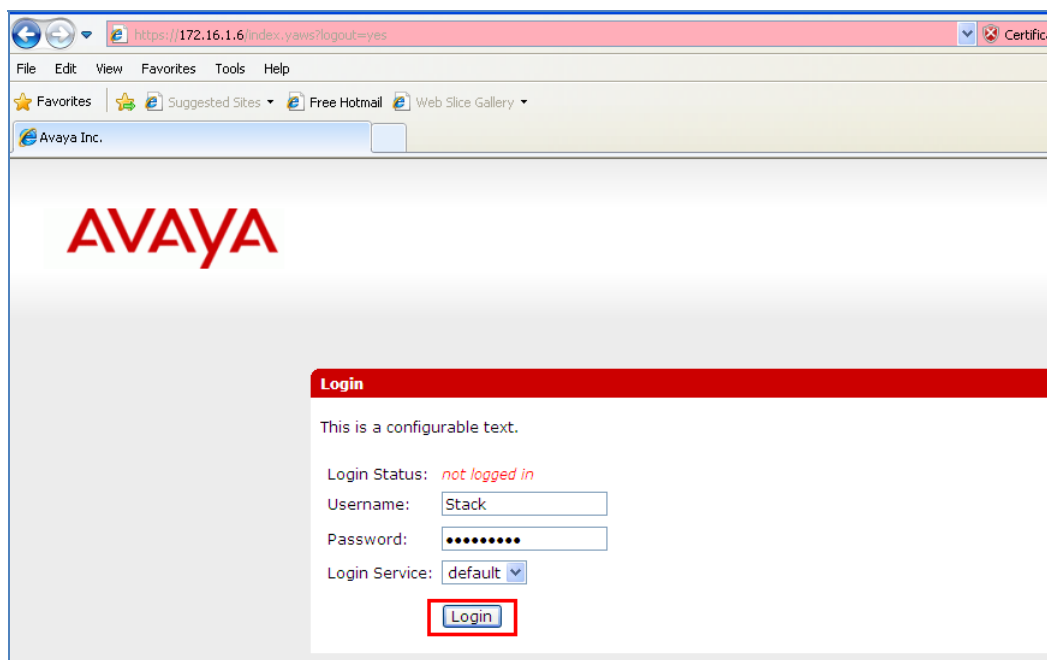
6. Verification Steps

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 SSL VPN Net Direct Tunnel is connected from the remote user pc to the VPN Gateway 3050.
2. Verified one-X Communicator H.323 extension 20092 is registered to Communication Manager while the SSL VPN Net Direct Tunnel is connected.
3. Verified one-X Communicator H.323 extension 20092 is able to make a Video Call while the SSL VPN Net Direct Tunnel is connected.
4. Verified that a message could be left for one-X Communicator H.323 extension 20092 and that the message waiting indicator turned on while the SSL VPN Net Direct Tunnel is connected.
5. Verified that Presence information is seen on one-X Communicator H.323 extension 20092 while the SSL VPN Net Direct Tunnel is connected.
6. Verified that an Instant Messaging is sent from one-X Communicator extension 20092 while the SSL VPN Net Direct Tunnel is connected.

6.1. Verify Access and Connection to SSL VPN Net Direct Tunnel

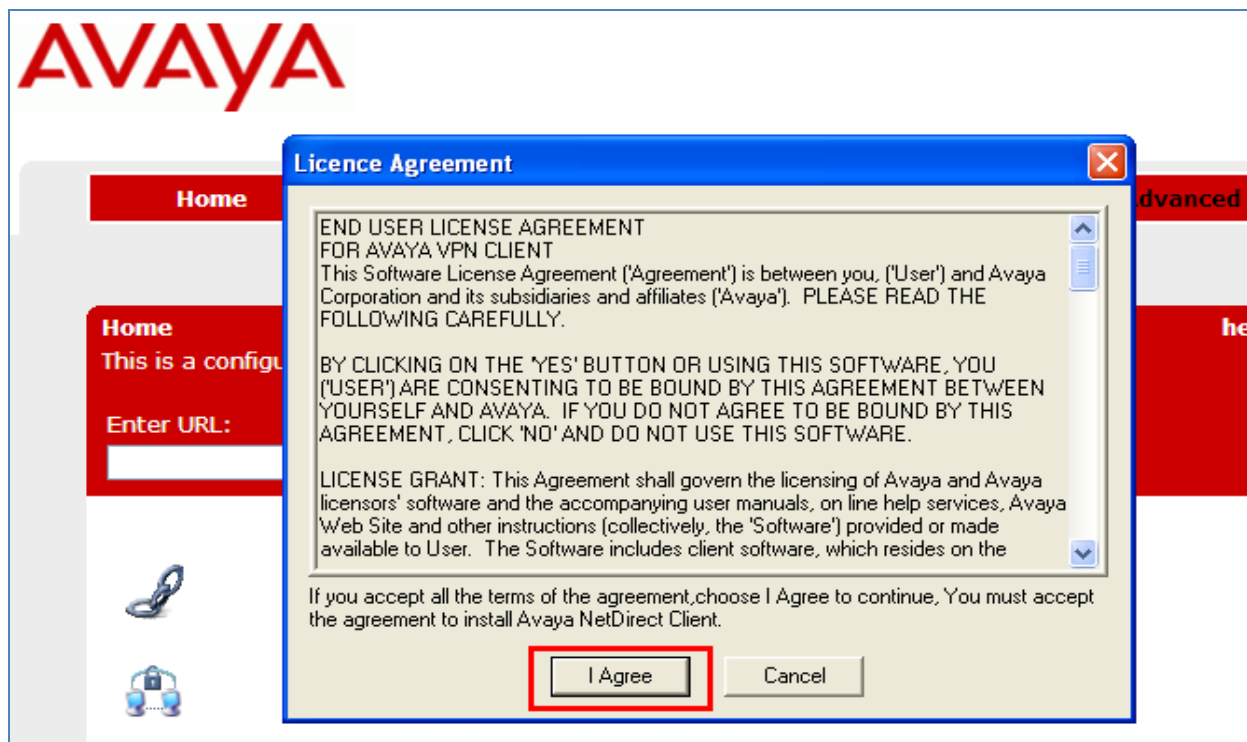
The remote user accesses the SSL VPN Tunnel by browsing to the IP Address of the SSL VPN Gateway or Portal IP address **https://172.16.1.6**. The remote user enters the Authentication User account administered in **Section 4.12** and presses the **Login** button.



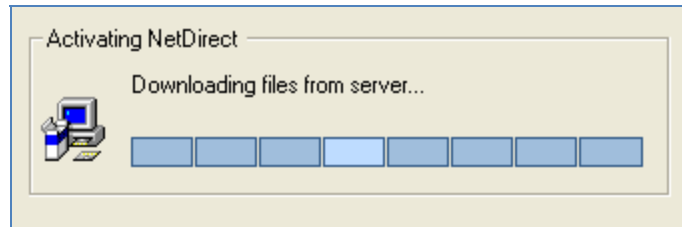
The following screen is displayed. The remote user accesses the SSL VPN Net Direct link administered in **Section 4.9**.



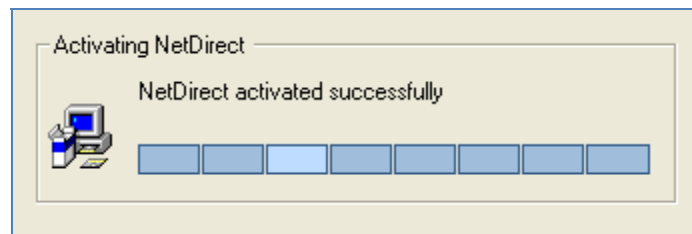
After selecting the SSL VPN Net Direct Link, the following screen is displayed. Select the **I Agree** button on the License Agreement.



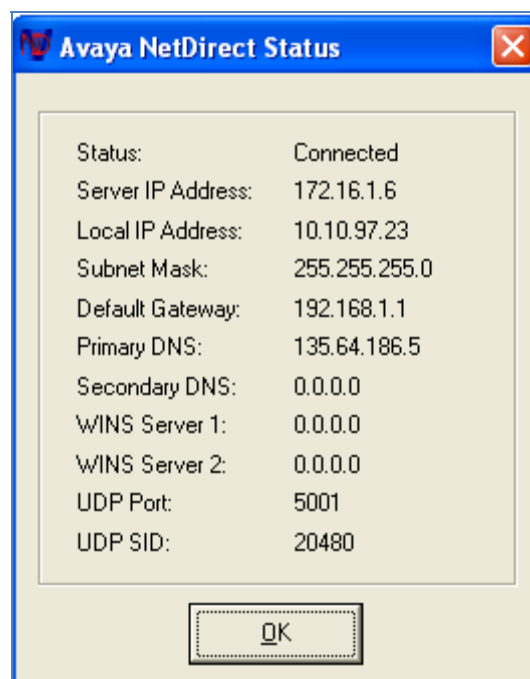
The SSL VPN Net Direct Link downloads the VPN client software to the remote user PC.



The VPN client is downloaded successfully to the remote user PC.



The following screen is displayed.



An ipconfig is performed at the command line of DOS on the remote user pc.

```

C:\ Command Prompt

Connection-specific DNS Suffix . : SSG5-Serial-WLAN
IP Address. . . . . : 192.168.1.36
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter {F3FF0F16-D44B-4390-9B50-20B9CE24C1C3}:

Connection-specific DNS Suffix . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :

Ethernet adapter {F9A48A6B-180D-4C62-8D68-BD5543731C6F}:

Media State . . . . . : Media disconnected

Ethernet adapter Local Area Connection 4:

Connection-specific DNS Suffix . :
IP Address. . . . . : 10.10.97.23
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.97.24

C:\Documents and Settings\administrator.SILSTACK>

```

6.2. Verify Avaya one-X® Communicator H.323 Registered to Avaya Aura® Communication Manager

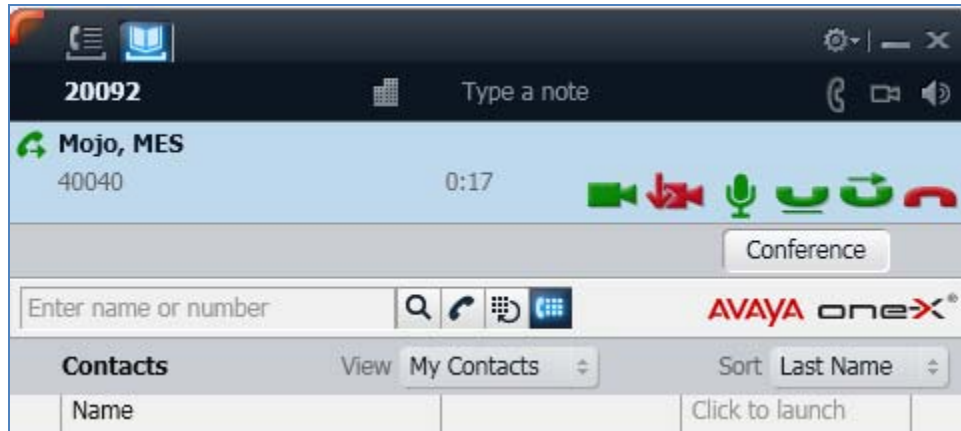
A **list registered-ip-stations** was performed from the command line of the SAT terminal on Communication Manager. The result shows the one-X Communicator extension **20092** registered to Communication Manager while the SSL VPN Net Direct Tunnel is connected. It also shows IP Address **10.10.97.23** assigned to the remote user pc that one-X Communicator H.323 soft client resides on. The results also show one-X Communicator H.323 extension 20092 assigned to **ip network region 1**.

```
list registered-ip-stations
```

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper	IP Address
20092	9630 1	oneX_Comm 6.1019	y	10.10.97.23	135.64.186.70
20093	9640 1	oneX_Comm 6.1018	y	135.64.186.199	135.64.186.70
20090	9630 1	oneX_Comm 6.1018	y	135.64.186.213	135.64.186.70

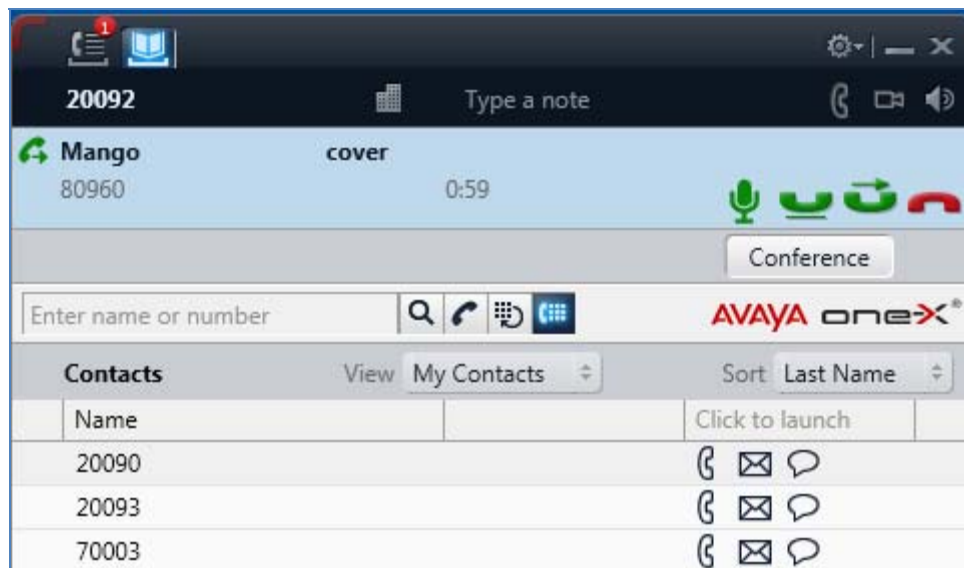
6.3. Verify Video using Avaya one-X® Communicator H.323

The following screenshots show a successful **Video Call** made from **one-X Communicator H.323** extension **20092** to another video endpoint while the SSL VPN Net Direct Tunnel is connected.

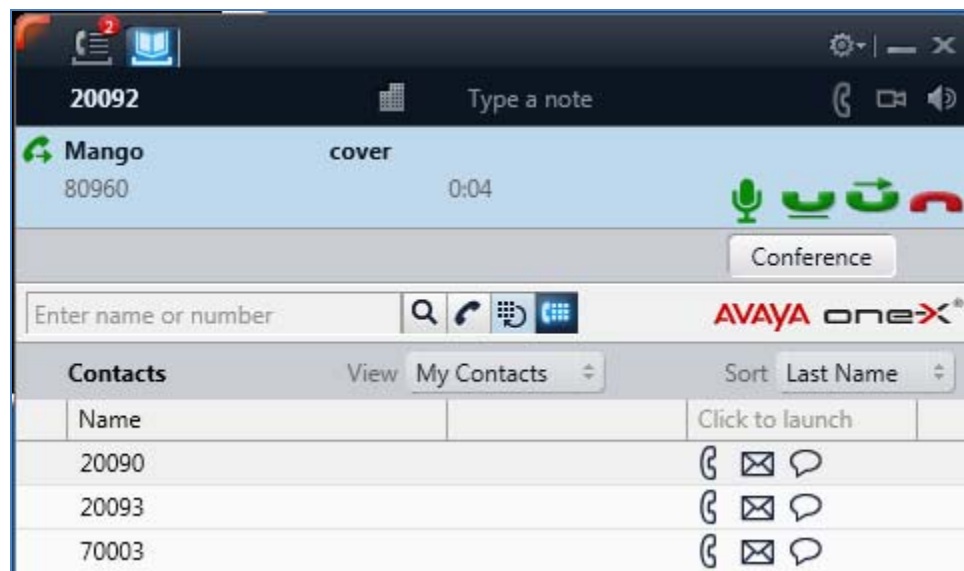


6.4. Verify MWI using Avaya one-X® Communicator H.323

The following screenshot shows the one-X Communicator H.323 extension 20093 can access Avaya Aura Messaging while the SSL VPN Net Direct Tunnel is connected.

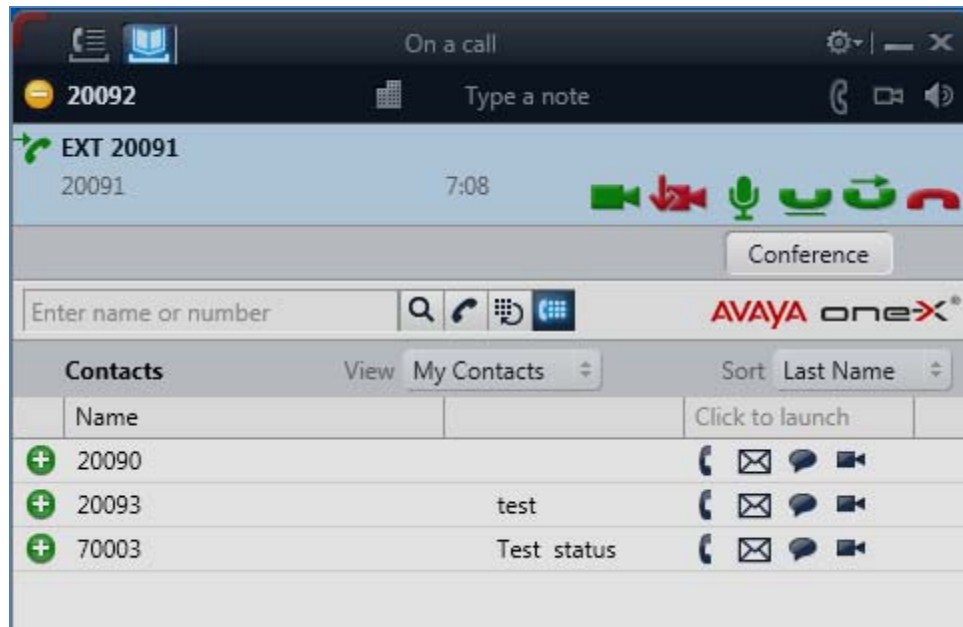


The following screenshot shows that a message can be left with the one-X Communicator extension 20092 and that the message waiting indicator was turned on while the SSL VPN Net Direct Tunnel is connected.

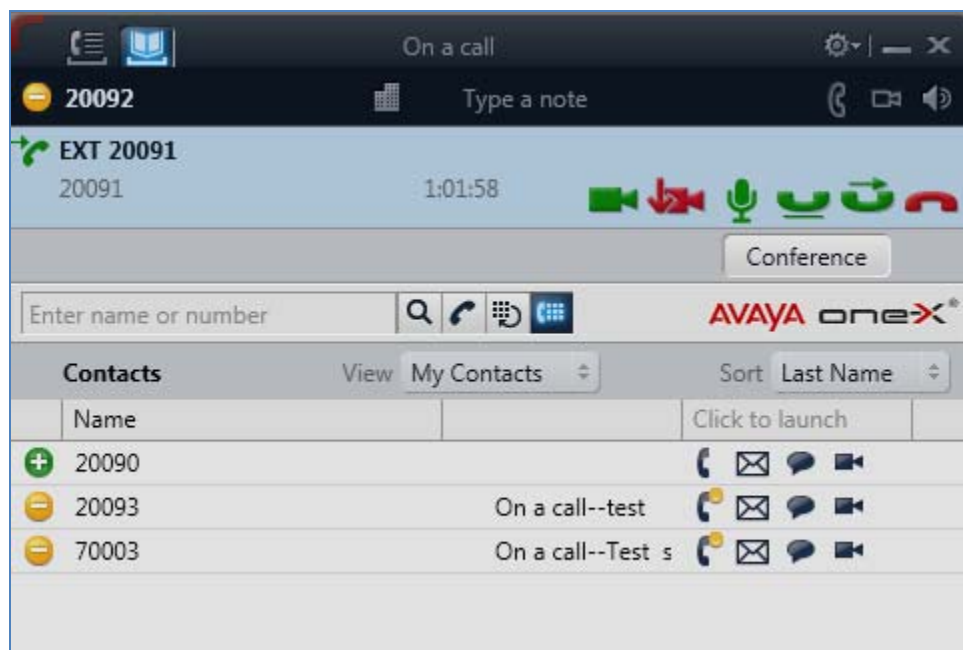


6.5. Verify Presence using Avaya one-X® Communicator H.323

The following screenshot shows Presence busy information for the one-X Communicator H.323 extension 20092 while the SSL VPN Net Direct Tunnel is connected.

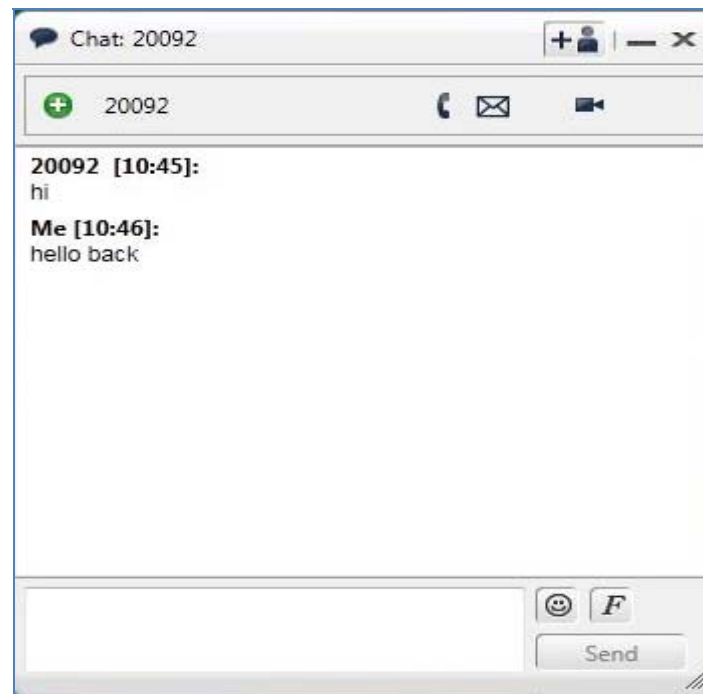


The following screenshot shows Presence busy information for the Contacts of one-X Communicator H.323 extension 20092 while the SSL VPN Net Direct Tunnel is connected.



6.6. Verify Instant Messaging using Avaya one-X Communicator H.323

The following screenshot shows Instant Messaging information for the one-X Communicator H.323 extension 20092 while the SSL VPN Net Direct Tunnel is connected.



7. Conclusion

These Application Notes have described the administration steps required so that Avaya one-X® Communicator H.323 soft client can interoperate with Avaya VPN Gateway 3050, over a VPN Net Direct SSL tunnel, while registered to Avaya Aura® Communication Manager running as an Evolution Server. It has also confirmed that Avaya one-X® Communicator H.323 can make a video call, interoperate with Avaya Aura® Messaging and Avaya Aura® Presence Services, while the VPN Net Direct SSL tunnel is established to the Avaya VPN Gateway 3050.

8. 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® Communication Manager Server Options, June 2010, Document Number 03-603479.
- [4] Administering Avaya Aura® Presence Services 6.0 , September 2010.
- [5] 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