

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.



Figure 1: VPN Net Direct SSL Tunnel using Avaya VPN Gateway 3050

Solution & Interoperability Test Lab Application Notes ©2011 Avaya Inc. All Rights Reserved.

# 2. Equipment and Software Validated

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

Avaya Aura®	Software
Avaya Aura® Communication Manager	Avaya Aura® Communication Manager
on a S8800 Server	Release 6.0.1
	R16x.00.1.510.0 Update: Service Pack 3
Avaya Media Gateway G650	
IP Server Interface TN2312BP	Hardware 15 Firmware 54
Clan TN799DP	Hardware 16 Firmware 40
IPMedpro TN2602AP	Hardware 08 Firmware 59
Avaya Aura® C363T–PWR Converged	Release 4.5.14
Stackable Switch	
Avaya VPN Gateway 3050	Release 8.0.7.1
Avaya one-X® Communicator H.323	Release 6.1.0.19-GA-31696
Soft client	
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.

Page

1 of

2

```
display ip-codec-set 1

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
                                                                       2 of
                                                                              2
                                                                Page
                          TP 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
                                        0
                   n
```

#### 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
```

Solution & Interoperability Test Lab Application Notes ©2011 Avaya Inc. All Rights Reserved. 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
                                                                М
                                                        GΑ
                                                                t
dst codec direct WAN-BW-limits Video Intervening
                                                     Dyn A G
                                                                С
rgn set WAN Units Total Norm Prio Shr Regions
                                                     CAC R L
                                                                е
    1
        y NoLimit
1
                                                        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**.

d	lisplay :	ip-network-map						Pa	age	1 of	E 63	
			ΙP	ADDRESS	MAPP	ING						
									_			
						Subnet	Network	٢.	Emerg	gency	7	
	IP Addre	ess				Bits	Region	VLAN	Locat	cion	Ext	
	FROM: 1	0.10.97.0				/24	1	n				
	TO: 10	0.10.97.255										

#### 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	
T		DCC. 0
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 Tabl	e:
Loss Group: 19	9 Personalized Ringing Patter	n: 1
	Message Lamp Ex	t: 20092
Speakerphone: 2	-way Mute Button Enable	d? y
Display Language: en	nglish Expansion Modul	e? n
Survivable GK Node Name:		
Survivable COR: in	nternal Media Complex Ex	t:
Survivable Trunk Dest? y	IP SoftPhon	e? Y
	IP Vide	о? у

display station 20092 **2** of 5 Page 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 Display Client Redirection? n MWI Served User Type: 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

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

#### 3.5. Save Translations

Use the save translations command to save these changes.

save translation
SAVE TRANSLATION
Command Completion Status
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.

Αναγα	VPN Ga	teway					Apply	Diff   Revert   Logout		
Config Monitor	Managing: SSL-8.0.7.1 on 3050 Dashboard » Health						23 Jun 2011 17:13:37	Logged as admin		
- Dashboard	Health Dashboard	1								
- <u>Health</u> - Management	Warning: GUI is currer	ntly not locked.								
+ Monitor										
+ Statistics	Lock information is available (	on 'Monitor->GUI Lock' page.								
+ Diagnostics										
	Go To GUI Lock Page									
	Hosts									
	MIP IP : 135.64.18	86.14 PC	Port : 7998 Interface : eth0			Netmask : 255.255.255.255				
	IP	Туре	Status	MIP	Local	Port Status				
	135.64.186.13	master	•	true	true		Summarize			
	Network 1			CPU	Usage		Memory Usage			
	Receptions	Transmissions			Used					
	Packets: 15173255	Packets: 6780960			2.00%					
	Errors: 0	Errors: 0								
	Dropped: 0	Dropped: 0			1			7		
	Overruns: 0	Overruns: 0								
	Frame: 0	Carrier: 0								
		Collisions:0		Fre	e		Free 80.00%			
	Inboud Traffic :845.1 Mb	Outbound Traffic:1386.7 Mb		98.009	6					

#### 4.2. Administer Public Private Interface

Select **Config**  $\rightarrow$  **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**.

Αναγα	VPN Gateway Apply   Diff   Revert   L
Config Monitor	Managing: SSL-8.0.7.1 on 3050 24 Jun 2011 09:50:04 Logged as admit Cluster » <u>Host-isd@a135-64-186-13</u> » System
- Wizards	System Information
- Cluster Manager Host(s)	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.
- Certificates	General Host Routes Ports Interfaces Licenses
<ul> <li>SSL Offload Servers</li> </ul>	General most codes fors interfaces licenses
<ul> <li>Bandwidth Management</li> </ul>	Host Type: master Y
<ul> <li>VPN Gateways</li> </ul>	host type. master
+ Administration	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**  $\rightarrow$  **Hosts**  $\rightarrow$  **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.

Αναγά	VPN Gateway	Apply   Diff   Revert   L
Config Monitor	Managing: SSL-8.0.7.1 on 3050 Cluster » <u>Host-isd@a135-64-186-13</u> » <u>Interface 1</u> » Configure Interface	23 Jun 2011 17:23:42 Logged as admin
- Wizards - Cluster Manager - <u>Host(s)</u> - Certificates	Host Interfaces	
Sact Onitidal Servers     Bandwidth Management     VPN Gateways     Administration     Operation     System     Users     Remote Access	IP Address: 135.64.186.13 Netmask: 255.255.224 VLAN Id: 0 Mode: failover V Primary Port: 0	Default Gateway: 135.64.186.1 Available Selected Port(s): 2 4 4 C
- Access List - SSH keys		Update Back )

### 4.4. Administer Interface Two

Select **Config**  $\rightarrow$  **Hosts**  $\rightarrow$  **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.

Αναγα	VPN Gateway	Apply   Diff   Re	vert
Config Monitor	Managing: SSL-8.0.7.1 on 3050 Cluster » <u>Host-isd@a135-64-186-13</u> » <u>Interface 2</u> » Configure Interface	24 Jun 2011 09:36:46 Logged :	as adm
- Wizards - Cluster Manager - <u>Host(s)</u> - Certificates - SSL Offload Servers	Host Interfaces General Routes Modify Network		
<ul> <li>Bandwidth Management</li> <li>VPN Gateways</li> </ul>	IP Address: 172.16.1.4	Default Gateway: 172.16.1.2	
+ Administration	Netmask:  255.255.0    VLAN Id:  0    Mode:  failover     Primary Port:  0	Available     Selected       1     >>       2     2       4     <	
		Update Ba	ack

#### 4.5. Administer Static Routes

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

AVAYA	VPN Gateway
Config Monitor	Managing: SSL-8.0.7.1 on 3050 Cluster » <u>Host-isd@a135-64-186-13</u> » Routes
- Wizards	Host Routes
- Cluster Manager	Late you manage static routes for a specific best when more than one interface is configured.
- Host(s)	Lets you manage static routes for a specific nost when more than one menace is configured 4
- Certificates	Course U. D. L. Dark Takeford University
- SSL Offload Servers	General Host Routes Ports Interfaces Licenses
- Bandwidth Management	
- VPN Gateways	

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.

Αναγα	VPN Gateway Apply   Diff   Revert   L
Config Monitor	Managing: SSL-8.0.7.1 on 3050 24 Jun 2011 10:22:33 Logged as admi Cluster » <u>Host-isd@a135-64-186-13</u> » Configure Host Route
- Wizards	Host Routes
- Cluster Manager	
- Host(s)	Lets you manage static routes for a specific host when more than one interface is configured.
- Certificates	Modify Host Route
- SSL Offload Servers	
- Bandwidth Management	Destination IP: 135.64.186.0 (format: 10.10.1.75)
- VPN Gateways	Destination Subnet: 255 255 0
+ Administration	Gateway IP: 135.64.186.1
	Save Route Back

#### 4.6. Administer SSL VPN Gateway

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

Ανάγα	v	PN Gateway				Apply   Dif		
Config Monitor	Managing: SSL-8.0.7.1 on 3050 24 Jun 2011 11:34:39 VPN Gateways							
- Wizards	VPN Gatew	VPN Gateways						
- Cluster Manager			0					
- Host(s)	Lists the configure	ed VPN(s) and also allows	s you to add, edit and delete VPN(s). 🖽					
- Certificates								
- SSL Offload Servers	Add Edit	Delete Quick VP	<sup>N</sup>					
- Bandwidth Management	🗖 ID	Name	IP Address(es)	Port	SSL	IPsec		
- VPN Gateways	1	IPSec	172.16.1.3	443	Enabled	Enabled		
+ Administration	2	SSL	172.16.1.6	443	Enabled	Disabled		

Solution & Interoperability Test Lab Application Notes ©2011 Avaya Inc. All Rights Reserved. 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.

Αναγα	VPN Gateway	Apply   Diff   Revert   Lo
Config Monitor	Managing: SSL-8.0.7.1 on 3050 VPN Gateways » Add a VPN	24 Jun 2011 11:06:09 Logged as admin
- Wizards	VPN Gateways	
- Cluster Manager	Add a VPN	
- Host(s)		
<ul> <li>Certificates</li> <li>SSL Offload Servers</li> <li>Bandwidth Management</li> <li><u>VPN Gateways</u></li> <li>Administration</li> </ul>	VPN Identifier: 3 V VPN Name: SSL IP Address: 172.16.1.6 Port: 443 (1.65534)	
	SSL Status: enabled V Certificate Number: <a href="mailto:sunset">cunset</a> Warning: New VPNs are directly applied to the database.	Create VPN Back

The following screen is displayed.

Ανάγα		VPN Gateway				Apply				
Config Monitor	Managing: SSL-8.0.7.1 VPN Gatew	Managing: SSL-8.0.7.1 on 3050 24 Jun 2011 13:05:02 VPN Gateways								
- Wizards	VPN Gatewa	VPN Gateways								
- Cluster Manager			0							
- Host(s)	Lists the configured	/VPN(s) and also allows you	to add, edit and delete VPN(s). 🖽							
- Certificates										
- SSL Offload Servers		Delete Quick VPN								
- Bandwidth Management	🗖 ID	Name	IP Address(es)	Port	SSL	IPsec				
- VPN Gateways	1	IPSec	172.16.1.3	443	Enabled	Enabled				
+ Administration	2	SSL	172.16.1.6	443	Enabled	Disabled				

#### 4.7. Administer IP Pool

To administer the IP Pool, select Config  $\rightarrow$  VPN Gateway  $\rightarrow$  VPN 2. Then under settings select IP Pool on the graphical user interface.

AVAYA	v	PN Gateway
Config Monitor	Managing: SSL-8.0.7 VPN Gate	7.1 on 3050 <u>eways</u> » VPN-2
- Wizards	VPN Summ	hary
- Cluster Manager	Settings	Configuration
- Host(s)	General	VPN Name : SSL, Standalone Mode is enabled, <u>WholeSecurity is off</u> ,
- Certificates	SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is ssl.silstack.com
- Bandwidth Management	Traffic Trace	Lets you traceroute or ping a host.
- VPN Gateways	IP Pool	Default IP Pool is 2, The configured IP Pools are
+ Administration	Host IP Pool	Host IP Pool is disabled

Under the **IP Pool List** select the **Add** button.

Ανάγα	VPN Gateway				
Config Monitor	Managing: SSL-8.0.7.1 on 3050 <u>VPN Gateways</u> » <u>VPN-2</u> » IP Pool			24 Jun 2	2011 11:47:51
- Wizards	IP Pool				
- Cluster Manager	The IP Real many is used to configure the d	opired method for appianit	a IP address and network attributes	to VPN cliente. The IP nee	L comos into
- Host(s)	to access a host using an IPsec VPN client (	formerly the Nortel VPN cli	ent) or Net Direct client connection.	The IP address is used as	a new sourc
- Certificates	the VPN Gateway and the destination host, o	once the remote user is au	thenticated and the VPN tunnel is se	et up., 🙎	
- SSL Offload Servers					
<ul> <li>Bandwidth Management</li> </ul>	Default IF	Pool: 2 SSL 🗸	('None' indicates that no IP Pool	will be used by default)	
<ul> <li><u>VPN Gateways</u></li> </ul>			× ·		
+ Administration					
	IP Pool List				
	Add Edit Delete Alloc Info	Copy Paste			
	D Name	Туре		Proxy ARP	Status
	2 <u>SSL</u>	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.

Αναγα	VPN Gateway	Apply   Diff   Revert   /
Config Monitor	Managing: SSL-8.0.7.1 on 3060	J11 11:51:09 Logged as adm
- Wizards	IP Pool Configuration	
- Cluster Manager	Add new IP Address Pool	
- Host(s)		
- Certificates	VPN: 2	
- SSL Offload Servers	IP Pool ID: 1	
- Bandwidth Management	Name: SSL	
- VPN Gateways		
+ Administration	Status: enabled	
	Type: local Y	
	Proxy ARP: on Y	
		Update Back

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.

Modify IP Address Pool		
General Network Attributes		
General Settings		
	Name: SSL	Proxy ARP: on 💌
	Status: enabled 🛩	Lower IP: 10.10.97.21
	Type: local 💌	Upper IP: 10.10.97.40
		Update Back

Solution & Interoperability Test Lab Application Notes ©2011 Avaya Inc. All Rights Reserved.

#### 4.8. Enable Net Direct

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

AVAYA	VPN Gateway			
Config Monitor	Managing: SSL-8.0.7.1 VPN Gatew	on 3050 <u>avs</u> » VPN-2		
- Wizards	VPN Summa	iry		
- Cluster Manager	Settings	Configuration		
- Host(s)	5	5		
- Certificates	IPsec	IPsec is disabled, IKE Profiles, User Tunnel Profiles, BO Tunnel Profiles		
<ul> <li>SSL Offload Servers</li> </ul>	L2TP	L2TP is disabled, IKE Profiles, User Tunnel Profiles		
<ul> <li>Bandwidth Management</li> </ul>	NAP	Automatic Remediation is disabled, Probation settings is disabled, Remote policy servers, Syste		
- VPN Gateways	Portal	Citrix support is off, Company Name is Avaya Inc., SMB Workgroup is WORKGROUP, ReDirect URL is		
+ Administration	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 Faile	Over Servers Old Client	s XML Configuration	TDI LSP	Mobility	Advanced				
Net Direct links should be configu	ured for any of the configure	d linksets in <u>VPN_Gate</u>	ways->VPN	-2->Link	u <mark>sets</mark> page.				
General Settings   Net Direct Ba	nner   <u>Net Direct Lice</u>	nse   Download Net	Direct Setu	p					
General Settings									
Net Direct Client:	on 💙					Available		Selected	
Idle Check:	off 🛩					generic_win	]	all	
Retry Connection Time:	180 (seconds)					mac		winxp	
Rekey Traffic Limit:	0	N	et Direct/SP	) Operati	ng Systems:	unknown vista			
Rekey Time Limit:	28800 (seconds)					win2k			
LIDD Porter	5000-5001					WIII/			
									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 🔒
VPII 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  $\rightarrow$  VPN Gateway  $\rightarrow$  VPN 2. Then under Settings select Link Sets on the graphical user interface.

Αναγα	۱	/PN Gateway
Config Monitor	Managing: SSL-8.0.7.1 VPN Gatewa	on 3050 a <u>vs</u> » VPN-2
- Wizards	VPN Summa	ry
- Cluster Manager	Settings	Configuration
- Host(s)	General	VPN Name : SSL, Standalone Mode is enabled, WholeSecurity is off,
- Certificates	SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is ssl.silstack.com.
- Bandwidth Management	Traffic Trace	Lets you traceroute or ping a host.
- <u>VPN Gateways</u>	IP Pool	Default IP Pool is 2, The configured IP Pools are
+ Administration	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.

	VEN Galeways » VEN-Z » LINKSEIS
	Portal Linksets
nager	Allows you to create a linkset, i.e. a set of hypertext links that can be accessed fro
	simultaneously 🕐
6	
d Servers	Add Edit Delete Copy Paste
Management	
<u>vays</u>	D Name
ation	1 <u>base-links</u>

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

Add New Linkset	
VPN:	2
ld:	4
Name:	netdirect
Text:	
Autorun:	false 💌
	Update Back

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

Add Portal Links	
ld:	4 💌
Text:	
Link Type:	Net Direct
	Continue
	Continue

The following **netdirect** link was created.

Config Monitor	Managing: SSL-8.0.7.1 on 3050				
	VPN Gateways » VPN-2 » Linksets				
- Wizards	Portal Linksets				
- Cluster Manager	Allows you to create a linkest, i.e. a set of hypertext links that can be accessed from the Bortal's Home tab.				
- Host(s)	Allows you to create a linkset, i.e. a set of hypertext links that can be accessed from the Portal's Home tab.				
- Certificates	Simulario doly				
- SSL Offload Servers	Add Edit Delete Conv Paste				
- Bandwidth Management					
- VPN Gateways	D Name				
+ Administration	1 <u>base-links</u>				
	2 <u>netdirect</u>				
	3 Installed_ND				

#### 4.10. Administer Trusted Group

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

Αναγα		VPN Gateway			
Config Monitor	Managing: SSL-8.0.7.1 VPN Gatev	I on 3050 <u>vays</u> » VPN-2			
- Wizards	VPN Summa	ary			
- Cluster Manager	Settings	Configuration			
- Host(s)	General	VPN Name : SSL, Standalone Mode is enabled, <u>WholeSecurity is off</u> ,			
- Certificates	SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is ssl.silstack.com.			
- Bandwidth Management	Traffic Trace	Lets you traceroute or ping a host.			
- VPN Gateways	IP Pool	Default IP Pool is 2, The configured IP Pools are			
+ Administration	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, file 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.

	VPN Gateways » VPN-2 » Groups
- Wizards	Groups
- Cluster Manager	Late you define the user groups that reside on the VPN Gateway. When a user long in to the VPN (via the Portal, the SSI, VPN client or the
- Host(s)	group membership. This is done by searching for a match between a group name defined, and a group name associated with the user's
- Certificates	user was authenticated (RADIUS, LDAP, NTLM, SiteMinder, RSA SecurID, RSA ClearTrust, client certificate or local database) 🕅
<ul> <li>SSL Offload Servers</li> </ul>	
- Bandwidth Management	Default Group: 1 trusted 🔽
<ul> <li><u>VPN Gateways</u></li> </ul>	Anonymous Group:
+ Administration	
	Add Edit Delete Copy Paste
	D 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	
VF	N: 2
	ld: 2 💌
Nan	ie: trusted
User Ty	e: advanced 💙
Comme	nt:
	Update Back

The following **trusted** group was added.

(	Add	Edit Delet	Copy Paste		
		🔲 ID	Name	User Type	Comment
		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.

ieneral 👔	Access Lists	Linksets	EACA	IPsec	L2tp	VPN Ad	min	Net Direct	Mob	ity Exter	ded Profiles	SPO	
								Nar	ne: t	usted		]	
								User Ty	pe:	dvanced	*		
							Band	width pol	icy:	None> 🔽			
				Net Dir	ect Wi	indow <mark>s</mark> A	Admin	n <mark>User Na</mark> r	ne:	dministrat	or	]	
				Net D	irect W	Vindows	<mark>Ad</mark> mi	in Passwo	ord:	•••••		]	
			Net Di	irect Wi	ndows	Admin	Passv	word (aga	in):	•••••		]	
								IP Po	ool:	SSL	~		
							1	Host IP Po	ool:	None> 💙			
						M	aximu	um Sessic	ns: (		(0 is unli	imited)	
						-	Sessio	on <mark>Idle Ti</mark> r	ne:		(second	s)	
					I	Maximur	m Ses	sion Leng	gth:		(second	s)	
								Comme	ent:				< >
													Unda

### 4.11. Map Net Direct Linkset to Trusted Group

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

Managing, 33L	Gateways » VP	<u>N-2</u> » <u>Grou</u>	i <mark>p-1</mark> » M	odify Grou	ip								
Modify a	Group												
Lets you confi	gure the genera	I settings of	fauserg	group 🛙	)								
General	Access Lists	Linksets	EACA	IPsec	L2tp	VPN Admin	Net Direct	Mol	bility	Extended I	Profiles	SPO	
							Nom		tructo	d		1	
							ivani	e.	iuste				

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 <u>here</u> .
Delete

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

VPN Gatev	<u>VPN Gateways</u> » <u>VPN-2</u> » <u>Group-1</u> » Linksets						
Portal Links	sets						
Allows you to map I	Allows you to map linksets to the current group <table-cell></table-cell>						
General Acces	ss Lists Linksets	EACA	IPsec	L2tp	VPN Admin	Net Direct	
i No new port	al linksets remaining	j. To add (	a new po	rtal link	set, click <u>here</u>		
Delete							
D ID	Name						
1	base-links						
2	Installed_ND						
3	netdirect						

#### 4.12. Administer User Authentication

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

AVAYA		VPN Gateway
Config Monitor	Managing: SSL-8.0.7.1 VPN Gatev	on 3050 <u>vays</u> » VPN-2
- Wizards	VPN Summa	ary
- Cluster Manager	Settings	Configuration
- Host(s)	General	VPN Name : SSL, Standalone Mode is enabled, <u>WholeSecurity is off</u> ,
- Certificates	SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is ssl.silstack.com
- Bandwidth Management	Traffic Trace	Lets you traceroute or ping a host.
- VPN Gateways	IP Pool	Default IP Pool is 2, The configured IP Pools are
+ Administration	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.

- Certificates		<del>na aloo apool</del>	ny ni minori ordor dio mod		o oppriod mion		
- SSL Offload Servers	Authenticatio	n Servers	Authentication Order	Sequential /	Authentication	Sequential	Order
- Bandwidth Management	]						
- VPN Gateways	Add Edit	Delete	Copy Paste				
+ Administration							
		Name		Display	Name		Domain Name
	1	<u>local</u>					
	2	<u>cert</u>		Not appl	icable		ssl.silstack.com

Select the Users option.

Config Monitor	Managing: SSL-8.0.7.1 on 3050 <u>VPN Gateways</u> » <u>VPN-2</u> » <u>Auth Server-1</u> » General					
- Wizards	Authentication Servers					
- Cluster Manager	and the second					
- Host(s)	Allows you to configure the general settings of Local Database authentication method 🖼					
- Certificates						
- SSL Offload Servers	General Users Password Change Advanced					
<ul> <li>Bandwidth Management</li> </ul>	Neme: Jacob					
- VPN Gateways	Name: local					
+ Administration	Display Name:					

#### Then select the **Add** button.

Certificates     SSL Offload Servers     Departure of the Management	General Users Password Change Advanced
VPN Gateways     Administration	Prefix: * Max: 50 v
	Users Lets you add user(s) to the local authentication database. When the user attempts to log in to the VPN and local database auther 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           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.

anaging: SSL-8.0.7.1 on 3050	24 Jun 2011 16:01:33	Logge
Jsers		
Add Single User   Add Bulk Users		
Add Single User		
Name: Stack		
Password:		
Password (again):		
Groups:		
Warning: Users are added immediately to the database. No apply is required.	Save User	Back

#### 4.13. Apply Changes

ABM; Reviewed: SPOC 09/12/2011 Solution & Interoperability Test Lab Application Notes ©2011 Avaya Inc. All Rights Reserved. For the changes to take affect on the VPN Gateway 3050 select the **Apply** button on the top right hand side of the graphical user interface.

Ανάγα	VPN Gateway	C	Apply Diff
Config Monitor	Managing: SSL-8.0.7.1 on 3050 VPN Gateways	24 Jun 2011 16:50:23	Logge
- Wizards	VPN Gateways		

Select the **Apply Changes** button.

Αναγα	VPN Gateway		
Config Monitor	Managing: SSL-8.0.7.1 on 3050 Apply Pending Configuration Changes		
- Wizards	Apply Pending Configuration Changes		
- Cluster Manager			
- Host(s)	Warning: Applying changes will save them to the configuration		
- Certificates	warning. Applying changes will save them to the conlight atom.		
<ul> <li>SSL Offload Servers</li> </ul>	(Apply Changes)		
<ul> <li>Bandwidth Management</li> </ul>	Apply changes		
<ul> <li>VPN Gateways</li> </ul>			
+ Administration	Back		

The following screenshot shows the changes were successful.

Αναγα	VPN Gateway
Config Monitor	Managing: SSL-8.0.7.1 on 3050 Apply Pending Configuration Changes
- Wizards	Apply Pending Configuration Changes
- Cluster Manager	
- Host(s)	
- Certificates	Apply Results
- SSL Offload Servers	
<ul> <li>Bandwidth Management</li> </ul>	Apply Succeeded
- VPN Gateways	
+ Administration	Back

# 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.

General Settings		?	×
Accounts Telephony Login	Telephony Using: OH.323 OSIP		
Messaging IM and Presence	Extension: 20092 Password: ••••••		
Devices and Services Outgoing Calls Phone Numbers Dialing Rules Audio Video Public Directory Preferences	Server List: 135.64.186.70 Add Remove		
Network Advanced	✓ Enable Video Calls		

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.

General Settings		?	×
Accounts Telephony Login	Messaging		
Messaging IM and Presence Devices and Servic	Do the following when the Message Waiting Indicator is clicked:		
Outgoing Calls Phone Numbers Dialing Rules Audio	Dial this number 80960		
Video Public Directory Preferences Network Advanced	O Start This Application Browse		

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.

General Settings		? x
Accounts Telephony Login Messaging	Settings Preferences	
IM and Presence	Instant Messaging and Presence Settings	
Devices and Services	Domain: pres.silstack.com	
Phone Numbers Dialing Rules	OAutomatically discover my IM login information	
Audio Video Public Directory	<ul> <li>Manually specify my IM login information</li> </ul>	
Preferences	IM username: 20092	
Advanced	IM password:	_

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

General Settings	? :	×
Accounts Telephony	Outgoing Calls	
Login Messaging IM and Presence	Place and receive calls using This Computer	
Devices and Services Outgoing Calls Phone Numbers Dialing Rules Audio Video Public Directory Preferences Network	<ul> <li>Enable Emergency Call Handling Feature         If you need to make a emergency 911 call using this         phone, the following telephone number will be used         to identify your location to a Public Safety Answering         Point.         Your extension number 20092         Telephone number     </li> </ul>	

## 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.

ABM; Reviewed:	Solution & Interoperability Test Lab Application Notes	25 of 34
SPOC 09/12/2011	©2011 Avaya Inc. All Rights Reserved.	1XCVPNSSL

- 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.

🚱 💿 💌 🙋 https://172.16.1.6/index.ya	ws?lagaut=yes	🔽 😵 Certificat
File Edit View Favorites Tools Help		
🖕 Favorites 🛛 🚖 🙋 Suggested Sites 👻 🙋	] Free Hotmail 🙋 Web Slice Gallery 👻	
🖉 Avaya Inc.		
Ανανα		
	Login	
	This is a configurable text.	
	Login Status: not logged in	
	Username: Stack	
	Password'	
	Login	

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

4					
	Home	Flies +	Tools +	Access +	Advanced +
	Home This is a configurabl Enter URL:	e text. Please add link	sets to the area be	low. Ive as Bookmark	help 🛛
	<i>2</i>				

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

AVAY	Δ	
	Licence Agreement	
Home		dvanced
	END USER LICENSE AGREEMENT FOR AVAYA VPN CLIENT This Software License Agreement ('Agreement') is between you, ('User') and Avaya Corporation and its subsidiaries and affiliates ('Avaya'). PLEASE READ THE	
Home	FOLLOWING CAREFULLY.	h
This is a configuent	BY CLICKING ON THE 'YES' BUTTON OR USING THIS SOFTWARE, YOU ('USER') ARE CONSENTING TO BE BOUND BY THIS AGREEMENT BETWEEN YOURSELF AND AVAYA. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, CLICK 'NO' AND DO NOT USE THIS SOFTWARE.	
	LICENSE GRANT: This Agreement shall govern the licensing of Avaya and Avaya licensors' software and the accompanying user manuals, on line help services, Avaya Web Site and other instructions (collectively, the 'Software') provided or made available to User. The Software includes client software, which resides on the	
Ð	If you accept all the terms of the agreement,choose I Agree to continue, You must accept the agreement to install Avaya NetDirect Client.	
	I Agree Cancel	

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

Activati	ing NetDirec	:t				
a 🗐	Download	ing file:	s from s	server		
72						

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

Activat	ing NetDirect
	NetDirect activated successfully
Þ	

The following screen is displayed.

Ŋ	🖤 Avaya NetDirect Status 🛛 🛛 🔀					
	Status:	Connected				
	Server IP Address:	172.16.1.6				
	Local IP Address:	10.10.97.23				
	Subnet Mask:	255.255.255.0				
	Default Gateway:	192.168.1.1				
	Primary DNS:	135.64.186.5				
	Secondary DNS:	0.0.0.0				
	WINS Server 1:	0.0.0.0				
	WINS Server 2:	0.0.0.0				
	UDP Port:	5001				
	UDP SID:	20480				
	<u>D</u> K					

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

🛤 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 registratiered-ip-stations was performed from the command line of the SAT termainal on Communication Manager. The result shows the one-X Communicator extension 20092 registered to Communcation 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 register	ed-ip-stat:	ions		
		REGISTI	ERED	IP STATIONS
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address
20092	9630 <b>1</b>	oneX_Comm 6.1019	У	<b>10.10.97.23</b> 135.64.186.70
20093	9640 1	oneX_Comm 6.1018	У	135.64.186.199 135.64.186.70
20090	9630 1	oneX_Comm 6.1018	У	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.

10092	4		Type a n	note		@+ _ 6 ⊏	- × • •
<b>G Mojo, MES</b> 40040		(	):17		<b>Ja</b> 1	υü	~
					Co	nference	
Enter name or number		Q	r 🗓 🕻		AVA		<b>≥</b> ×°
Contacts Name	View	My (	Contacts	\$	Sort Click to	Last Name launch	•



### 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.

		@- _×
20092	📕 🛛 Type a note	G 🖙 📣
💪 Mango	cover	
80960	0:59	ų ų ū n
		Conference
Enter name or number	Q 🖍 🐑 💷	AVAYA onex*
Contacts	View My Contacts 💠	Sort Last Name 🗘
Name		Click to launch
20090		6 🛛 🖓
20093		G M P
70003		6 🛛 🖓

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.

[]     [		©- _×
20092	I Type a note	G 🖙 🔹
C Mango 80960	cover 0:04	1 uite
		Conference
Enter name or numb	er 🛛 🔍 🌈 🐑 💷	AVAYA onex*
Contacts	View My Contacts 💠	Sort Last Name 💠
Name		Click to launch
20090	· · · · · · · · · · · · · · · · · · ·	
20093		G M P
70003		G M P

#### 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.

	£ 🛄	On	a call		@- _	. x
•	20092	4	Type a note		G 🖙	<b>4</b> D
r	<b>EXT 20091</b> 20091		7:08	<b>/2</b>	٧Ū	~
				Co	onference	
Ent	ter name or number	Q	r 🐑 📖	AVA	<mark>ya</mark> one	• <b>&gt;</b> <*
	Contacts	View M	y Contacts 💠	Sort	Last Name	\$
	Name		1	Click to	launch	
0	20090			( 🖂	<b>9</b>	
0	20093		test	( 🖂	🗭 🖬	
0	70003		Test status	( 🖂	9 m	

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.

P Chat: 20092		+ <u></u> -×
20092	C	
20092 [10:45]: hi		
Me [10:46]: hello back		

# 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 <u>http://support.avaya.com</u>.

- [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 <sup>®</sup> and <sup>TM</sup> 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 <u>interoplabnotes@list.avaya.com</u>