



Avaya Solution & Interoperability Test Lab

Configuring Cisco 3020 VPN Concentrator to Provide WebVPN Access by Using Cisco Secure Socket Layer (SSL) VPN Client to Support Avaya IP Softphone – Issue 1.0

Abstract

These Application Notes describe the steps to configure a WebVPN tunnel between a Cisco SSL VPN Client (SVC) and the Cisco VPN 3020 concentrator to support Avaya IP Softphone. The Cisco VPN concentrator is configured to provide a Secure Socket Layer (SSL) VPN remote-access connectivity to Cisco SSL VPN Client and uses an internal database for authentication. The Avaya IP Softphone utilizes this tunnel to connect with Avaya Communication Manager behind the VPN concentrator for a secure communication.

1. Introduction

WebVPN provides Secure Socket Layer (SSL) VPN remote-access connectivity for almost any user who uses a Web browser and its native SSL encryption. This enables the companies to extend their secure enterprise networks to any authorized user by providing remote access connectivity to corporate resources from any Internet-enabled location. This capability also provides a secure communication channel for enterprise VoIP users at remote locations. Cisco IOS SSL VPN supports clientless access to applications such as intranet content, email and network file shares. Since the Avaya IP Softphones need to interface directly with network layer, the SSL VPN Client applications just provide such environment that enables IP Softphones to have a secure VoIP communication through the SSL VPN tunnel.

These Application Notes describe the steps on how to configure a WebVPN tunnel between a Cisco SSL VPN Client (SVC) and the Cisco VPN 3020 concentrator to support Avaya IP Softphone. The Cisco IOS SSL VPN is a router-based Secure Sockets Layer VPN solution and it enables remote client's full network access remotely to virtually any application. In this sample configuration, the Cisco VPN 3020 concentrator is configured as a VPN Server to establish a VPN tunnel with Cisco SSL VPN client for remote access. Avaya IP Softphone that resides on the same PC with Cisco SSL VPN client will utilize this VPN tunnel to connect with Avaya Communication Manager. Signaling and audio packets from the IP Softphone will be encrypted through this tunnel across a simulated IP Network (Internet).

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 1**. The Corporate IP Network location contains the Cisco VPN 3020 concentrator functioning as a VPN Server. Avaya Communication Manager running on an S8710 server and an Avaya G650 Media Gateway are also located at the Corporate IP Network location. The Corporate IP Network is mapped to **IP Network Region 1** in Avaya Communication Manager.

The Cisco SSL VPN clients are located in the public network and configured to establish a VPN tunnel to the Public IP address of the Cisco concentrator via HTTPS connection. The Cisco concentrator will assign IP addresses to the SSL VPN clients. The assigned IP addresses, also known as the inner addresses, will be used by the Avaya IP Softphones when communicating inside the VPN tunnel and in the private corporate network to Avaya Communication Manager.

Avaya Communication Manager maps the Avaya IP Softphones to the appropriate IP Network Region using this inner IP address and applies the IP Network Region specific parameters to the IP Softphones. In these Application Notes, the G.729 codec with two 20ms voice samples per packet is assigned to the IP Softphone.

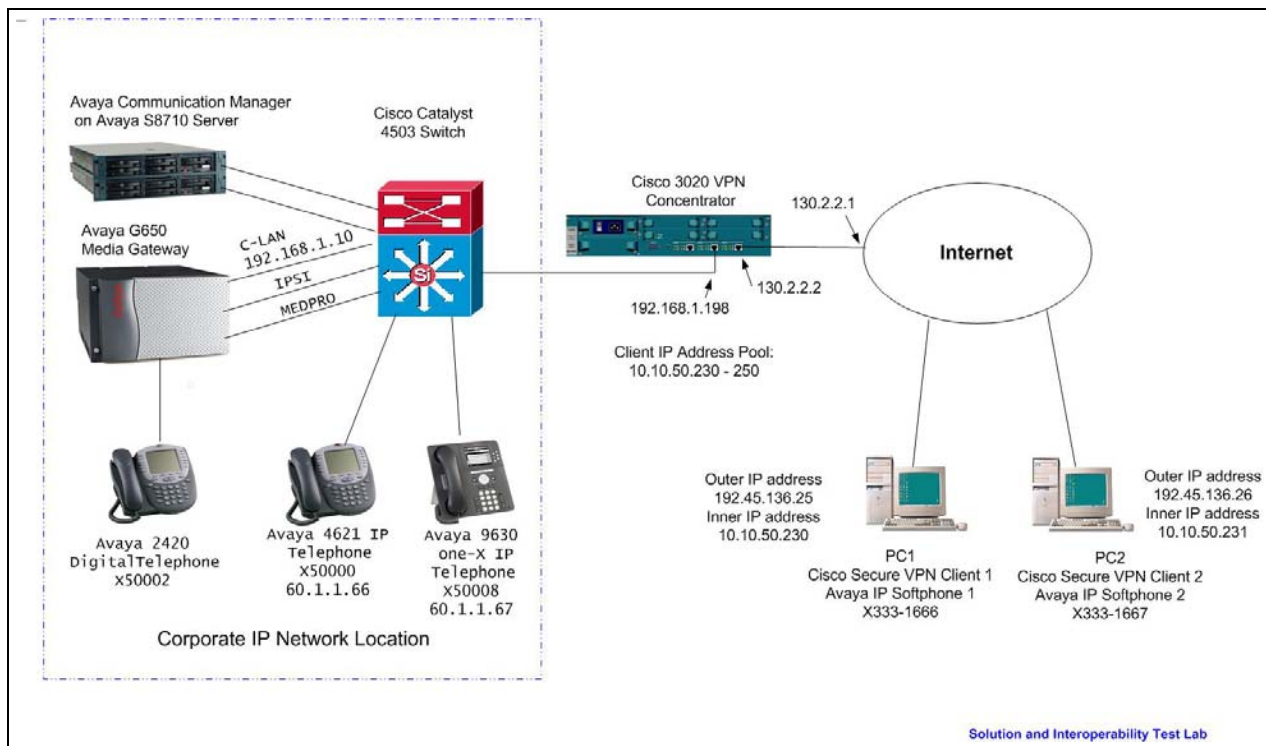


Figure 1: Network Diagram

3. Equipment and Software Validated

Table 1 lists the equipment and software/firmware versions used in the sample configuration provided.

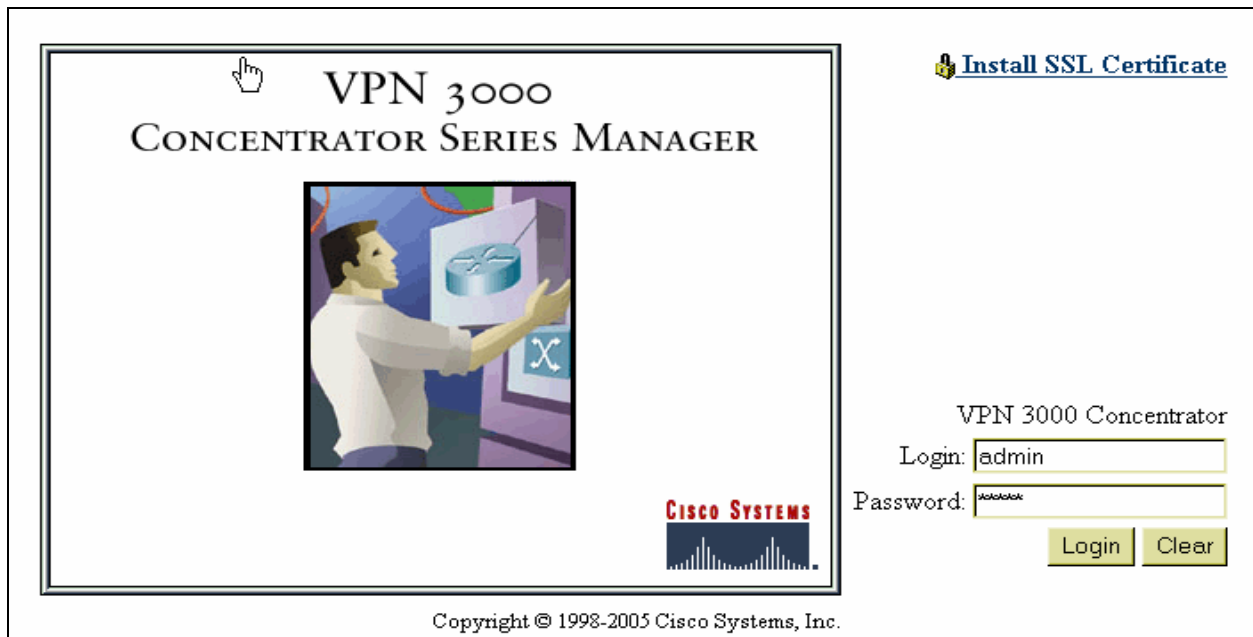
Equipment	Software Version
Avaya S8710 Server with G650 Media Gateway	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya IP Softphone	R 6.0 with SP2
Avaya 9600 Series IP Telephone	R1.5 (H.323)
Avaya 4600 Series IP Telephone	R2.8 (H.323)
Avaya 2420 Digital Telephone	NA
Cisco 3020 VPN Concentrator	R4.7.2.N
Cisco Secure VPN Client	R1.0.2.127

Table 1 – Equipment Version Information

4. Cisco 3020 VPN Concentrator Configuration

These Application Notes assume that the Cisco 3020 VPN Concentrator has been configured with basic IP connectivity and is connected into the network. The required software has been installed on the device. For steps to upgrade the software refer to reference [1]. The Cisco 3020 VPN Concentrator depicted in **Figure 1** has been configured with private IP address 192.168.1.198.

1. From a web browser, enter the URL of the Cisco 3020 VPN Concentrator interface's IP address <http://192.168.1.198> and log in as admin with administrative privileges in the window shown below.



VPN 3000
CONCENTRATOR SERIES MANAGER

[Install SSL Certificate](#)

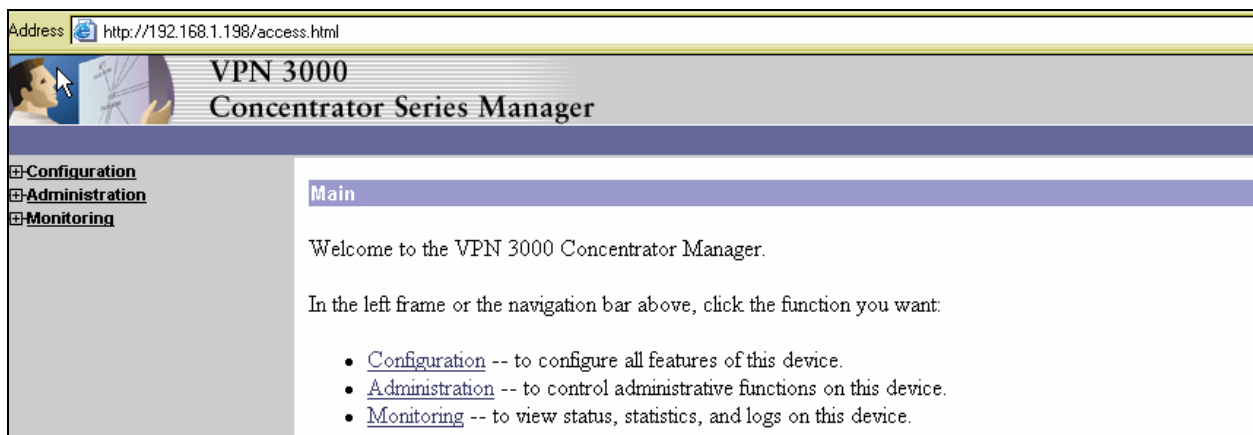
VPN 3000 Concentrator

Login:

Password:

Copyright © 1998-2005 Cisco Systems, Inc.

After successful login, the main menu is displayed.



Address <http://192.168.1.198/access.html>

VPN 3000
Concentrator Series Manager

[+Configuration](#)
[+Administration](#)
[+Monitoring](#)

Main

Welcome to the VPN 3000 Concentrator Manager.

In the left frame or the navigation bar above, click the function you want:

- [Configuration](#) -- to configure all features of this device.
- [Administration](#) -- to control administrative functions on this device.
- [Monitoring](#) -- to view status, statistics, and logs on this device.

2. This step shows how to enable the SSL VPN client on the VPN concentrator.

Note: New VPN Concentrators that run release 4.7 or later come pre-loaded with the SSL VPN Client. By default, the SSL VPN Client is disabled and needs to be enabled.

- Select **Configuration → Tunneling and Security → WebVPN → Cisco SSL VPN Client** from the left navigation panel.
- Click **Enable the Cisco SSL VPN Client**.
- Click **Apply**.

Configuration | Tunneling and Security | WebVPN | Cisco SSL VPN Client

Cisco SSL VPN Client version (CISCO STC win2k+ 1.0.0 1,0,0,179 Tue 03/08/2005 15:31:20.43) is enabled. These settings override all group Cisco SSL VPN Client settings. Choose one of the following actions and click the Apply button:

☐ Disable the Cisco SSL VPN Client

☒ Enable the Cisco SSL VPN Client

☐ Uninstall the Cisco SSL VPN Client

☐ Install a new Cisco SSL VPN Client

3. Add Groups for SSL client remote users.

- Select **Configuration** → **User Management** → **Groups** → **Add**
- Enter **SSLGroup** as **Group Name**.
- Enter **password** and repeat **password** in **Verify** field.
- Since this example uses internal database (on the VPN concentrator) for SSL VPN user authentication, select **Internal** for the **Type** field.
- Click **Add**.

Note: if external authentication method is used, for example, third party authentication server, select **External** in the **Type** field.

The screenshot shows the 'VPN 3000 Concentrator Series Manager' web interface. The left sidebar contains a tree view with categories: Configuration, Administration, and Monitoring. Under 'Configuration', there are sub-items: Interfaces, System, User Management (selected), Base Group, Groups, and Users. Under 'Administration', there are: Policy Management, Tunneling and Security, and Monitoring. The main content area is titled 'Configuration | User Management | Groups | Add'. It includes a text box explaining the 'Inherit?' checkbox. Below this is a tabbed interface with tabs: Identity (selected), General, IPsec, Client Config, Client FW, HW Client, PPTP/L2TP, WebVPN, and NAC. The 'Identity Parameters' table has three columns: Attribute, Value, and Description. The rows are: Group Name (SSLGroup), Password (password), Verify (password), and Type (Internal). At the bottom are 'Add' and 'Cancel' buttons.

Attribute	Value	Description
Group Name	SSLGroup	Enter a unique name for the group.
Password	password	Enter the password for the group.
Verify	password	Verify the group's password.
Type	Internal	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

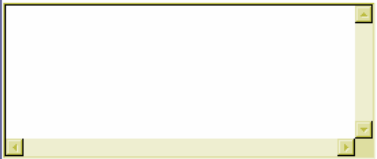
4. Configure WebVPN properties.

- Select the **WebVPN** Tab in the same window in order to enable the SSL VPN Client for group name **SSLGroup**.
- Select the necessary options as shown below.
- Click **Apply** when done.

Note: the Cisco SSL VPN Client Keepalive Frequency option is needed only to ensure that an SSL VPN Client connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.

The Keep Cisco SSL VPN Client option ensures that the SSL VPN Client is always installed on the client PC. If this option is not selected, the SSL VPN Client needs to be installed every time you want a WebVPN tunnel from the client PC.

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity	General	IPSec	Client Config	Client FW	HW Client	PPTP/L2TP	WebVPN	NAC
WebVPN Parameters								
Attribute	Value	Inherit?	Description					
Enable URL Entry	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Check to place the URL entry box onto the home page.					
Enable File Access	<input type="checkbox"/>		Check to enable Windows file access through HTTPS. When enabling File Access, a NetBIOS Name Server needs to be configured under System Servers .					
Enable File Server Entry	<input type="checkbox"/>		Check to place the file server entry box onto the home page. File Access must be enabled.					
Enable File Server Browsing	<input type="checkbox"/>		Check to enable browsing the Windows network for domains/workgroups, servers and shares. File Access must be enabled.					
Enable Port Forwarding	<input checked="" type="checkbox"/>		Check to enable port forwarding.					
Enable Outlook/Exchange Proxy	<input type="checkbox"/>		Check to enable the Outlook/Exchange proxy.					
Apply ACL	<input type="checkbox"/>		Check to apply the WebVPN ACL defined for the users of this group.					
Enable Auto Applet Download	<input type="checkbox"/>		Check to enable auto applet download on login.					
Enable Citrix MetaFrame	<input type="checkbox"/>		Check to allow access using Citrix MetaFrame terminal services.					
Enable Cisco SSL VPN Client	<input checked="" type="checkbox"/>		Check to enable use of the Cisco SSL VPN Client.					
Require Cisco SSL VPN Client	<input checked="" type="checkbox"/>		Check to require use of the Cisco SSL VPN Client.					
Keep Cisco SSL VPN Client	<input checked="" type="checkbox"/>		Check to keep the Cisco SSL VPN Client installed on the client workstation.					
Cisco SSL VPN Client Keepalive Frequency	<input type="text"/>	<input checked="" type="checkbox"/>	(seconds) Enter the Cisco SSL VPN Client Keepalive Frequency. Enter 0 to disable.					
Port Forwarding Name	Application Access	<input checked="" type="checkbox"/>	Enter the display name the users see when using TCP Port forwarding.					
Homepage	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the URL of the web page to be displayed to the user upon login.					
Content Filter Parameters								
Filter Java/ActiveX	<input type="checkbox"/>	<input type="checkbox"/>	Check to remove <applet>, <embed> and <object> tags from HTML.					
Filter Scripts	<input type="checkbox"/>		Check to remove <script> tags from HTML.					
Filter Images	<input type="checkbox"/>		Check to remove tags from HTML.					
Filter Cookies from Images	<input type="checkbox"/>		Check to remove cookies that are delivered with images. Advertisers use cookies to track visitors.					
WebVPN ACLs								
		<input checked="" type="checkbox"/>	<p>The WebVPN Access Control List to apply to user sessions.</p> <ul style="list-style-type: none"> If you do not define any filters, all connections are permitted. If you configure a permit filter, the default action is to deny connections other than what the filter defines. A WebVPN ACL can have a total of 255 characters. Source and destination IDs are IP addresses and wildcard masks or hostnames. WebVPN ACLs are not applied to SSL VPN Client connections. Only IP ACLs are applied to the SSL VPN Client. 					
<p>Syntax for protocol filters:</p> <p>[permit deny] [ip smtp imap4 pop3 cifs http https] Src-ID Dst-ID</p> <p>Example: permit ip any host 10.86.9.22</p> <p>Example: permit ip any 192.168.1.0 0.0.0.255</p> <p>Syntax for URL filters:</p> <p>[permit deny] URL URL-definition</p> <p>Example: deny url http://www.example.com</p>								
<div> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>								

5. Add users on Cisco VPN concentrator.

- Select **Configuration → User Management → Users → Add**.
- Enter user name and password.
- Select **SSLGroup** in the **Group** field.
- Click **Add**.

The screenshot shows the 'VPN 3000 Concentrator Series Manager' web interface. The left sidebar contains a tree view with 'Configuration' expanded, showing 'Interfaces', 'System', 'User Management', 'Base Group', 'Groups', 'Users', 'Policy Management', and 'Tunneling and Security'. The 'Users' link is selected. The main content area is titled 'Configuration | User Management | Users | Add'. It contains a message: 'This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.' Below this is a tabbed interface with 'Identity' selected. The 'Identity Parameters' table is shown below:

Attribute	Value	Description
Username	SSLUser	Enter a unique username.
Password	XXXXXXXXXX	Enter the user's password. The password must satisfy the group password requirements.
Verify	XXXXXXXXXX	Verify the user's password.
Group	SSLGroup	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

At the bottom of the form are 'Add' and 'Cancel' buttons.

6. Since the VPN concentrator can assign IP addresses to VPN client, this section shows how to enable this feature and create an address pool on the concentrator.

- Select **Configuration → System → Address Management → Assignment**
- Click **Use Address Pools**
- Click **Apply**

The screenshot shows the 'Configuration | System | Address Management | Assignment' page. It contains a message: 'This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.' Below this are several options with checkboxes:

- Use Client Address** ☐ Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
- Use Address from Authentication Server** ☐ Check to use an IP address retrieved from an authentication server for the client.
- Use DHCP** ☐ Check to use DHCP to obtain an IP address for the client.
- Use Address Pools** ☒ Check to use internal address pool configuration to obtain an IP address for the client.

Below these options is the **IP Reuse Delay** field, which is a text box containing '0'. The description for this field is: 'Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.'

At the bottom of the form are 'Apply' and 'Cancel' buttons.

- Select **Configuration → System → Address Management → Pools → Add**
- Click **Add**

Configuration | System | Address Management | Pools

This section lets you configure IP Address Pools.

Click the **Add** button to add a pool entry, or select a pool and click **Modify**, **Delete** or **Move**.

IP Pool Entry	Actions
— Empty —	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/>

- Enter the IP address range and subnet mask as shown below.
- Click **Apply**

Configuration | System | Address Management | Pools | Modify

Modify an address pool.

Range Start Enter the start of the IP pool address range.

Range End Enter the end of the IP pool address range.

Subnet Mask Enter the subnet mask of the IP pool address range.
Enter 0.0.0.0 to use default behavior.

7. Configure system default gateway in order to ensure the VPN concentrator has all necessary routes available.

- Select **Configuration → System → IP Routing → Default Gateway**
- Enter information as shown below. The 130.2.2.1 is the next router interface connected to its public interface.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway	<input type="text" value="130.2.2.1"/>	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.
Metric	<input type="text" value="1"/>	Enter the metric, from 1 to 16.
Tunnel Default Gateway	<input type="text" value="0.0.0.0"/>	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.
Override Default Gateway	<input type="checkbox"/>	Check to allow learned default gateways to override the configured default gateway.

8. Use this step to bind the SSL certificate with Cisco VPN Concentrator's interface
In this configuration, the concentrator uses its public interface to terminate the SSL VPN Client connection. This interface needs a SSL certificate associated with it to verify the Clients' credentials.
 - Click **Administration** → **Certificate Management** to confirm that SSL certificates are generated for the interfaces.
 - Click **Generate** button from the options under Actions in the SSL Certificates box for the respective interface if the certificates are not generated.

Administration | Certificate Management
Monday, 21 January 2008 13:44:30
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator. Installation of a CA certificate is required before identity and SSL certificates can be installed.

- [Click here to install a CA certificate](#)
- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 0, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
No Certificate Authorities				

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	No Certificate Installed.			Generate Enroll Import
Public	No Certificate Installed.			Generate Enroll Import

SSH Host Key

Key Size	Key Type	Date Generated	Actions
1024 bits	RSA	01/15/2008	Generate

Enrollment Status [[Remove All](#): [Errored](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#)] (current: 0 available: 20)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

- Enter public interface's IP address **130.2.2.2** in the **Common Name** field and select **1024-bits**, in this example, as **RAS KEY Size**.
- Leave other fields as default.
- Click **Generate**.

Administration | Certificate Management | Generate SSL Certificate

You are about to generate a certificate for the Public Interface. The certificate will have the following DN for both Subject and Issuer.

The certificate will be valid for 3 years from yesterday.

Common Name (CN) Enter the Common Name, usually the IP or DNS address of this interface.

Organizational Unit (OU) Enter the department.

Organization (O) Enter the Organization or company.

Locality (L) Enter the city or town.

State/Province (SP) Enter the State or Province.

Country (C) Enter the two-letter country abbreviation (e.g. United States = US).

RSA Key Size Select the key size for the generated RSA key pair.

Click **View** (under **SSL Certificates**) to display the certificate.

Administration | Certificate Management Monday, 21 January 2008 13:51:53
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator. Installation of a CA certificate is required before identity and SSL certificates can be installed.

- [Click here to install a CA certificate](#)
- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 0, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
No Certificate Authorities				

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	No Certificate Installed.			Generate Enroll Import
Public	130.2.2.2 at Cisco Systems, Inc.	130.2.2.2 at Cisco Systems, Inc.	01/19/2011	View Renew Delete Export Generate Enroll Import

SSH Host Key

Key Size	Key Type	Date Generated	Actions
1024 bits	RSA	01/15/2008	Generate

Enrollment Status [[Remove All: Errored](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#)] (current: 0 available: 20)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

The certificate is as shown below.

Administration Certificate Management View	
Subject CN=130.2.2.2 OU=VPN 3000 Concentrator O=Cisco Systems, Inc. L=Franklin SP=Massachusetts C=US	Issuer CN=130.2.2.2 OU=VPN 3000 Concentrator O=Cisco Systems, Inc. L=Franklin SP=Massachusetts C=US

Serial Number 47939849
Signing Algorithm MD5WithRSA
Public Key Type RSA (1024 bits)
MD5 Thumbprint A5:37:FC:BB:67:8A:99:96:C4:67:DA:42:3A:D3:37:C2
SHA1 Thumbprint 18:9C:CE:84:9E:31:CA:F6:DC:FE:0A:3E:7D:67:64:54:62:32:83:F7
Validity 1/20/2008 at 13:51:53 to 1/19/2011 at 13:51:53

[Back](#)

9. Choose an interface to specifically allow the HTTPS session on the interface that terminates the SSL VPN Client.
 - Select **Configuration → Interfaces**
 - Click **Ethernet 2 (Public)**

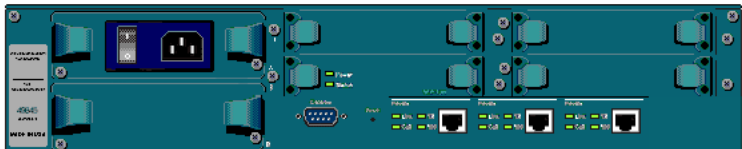
Configuration | Interfaces Wednesday, 16 January 2008 14:30:33
Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.1.198	255.255.255.0	00.03.A0.8A.63.0E	
Ethernet 2 (Public)	UP	130.2.2.2	255.255.255.252	00.03.A0.8A.63.0F	130.2.2.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

• [Power Supplies](#)



- Check both boxes: **Allow WebVPN HTTPS sessions** and **Redirect HTTP to HTTPS**.
- Click **Apply**.

Configuration | Interfaces | Ethernet 2

Configuring Ethernet Interface 2 (Public).

General | RIP | OSPF | Bandwidth | **WebVPN**

WebVPN Parameters		
Attribute	Value	Description
Allow Management HTTPS sessions	<input type="checkbox"/>	Check to enable management HTTP and HTTPS sessions on this interface. Disabling will prevent managing the device through a web browser on this interface.
Allow WebVPN HTTPS sessions	<input checked="" type="checkbox"/>	Check to enable WebVPN HTTPS sessions on this interface.
Redirect HTTP to HTTPS	<input checked="" type="checkbox"/>	Check to force any connections coming in as HTTP to be redirected to HTTPS. This provides additional security. Unencrypted HTTP sessions will no longer be allowed on this interface.
Allow POP3S sessions	<input type="checkbox"/>	Check to enable POP3S e-mail sessions on this interface using an e-mail program.
Allow IMAP4S sessions	<input type="checkbox"/>	Check to enable IMAP4S e-mail sessions on this interface using an e-mail program.
Allow SMTPS sessions	<input type="checkbox"/>	Check to enable SMTPS e-mail sessions on this interface using an e-mail program.

4.1. Install WebVPN Client Software for Remote Client

Upon the first time the client computer connects to the VPN concentrator, the VPN concentrator will automatically push the VPN client software to the PC after it authenticates the user login credentials.

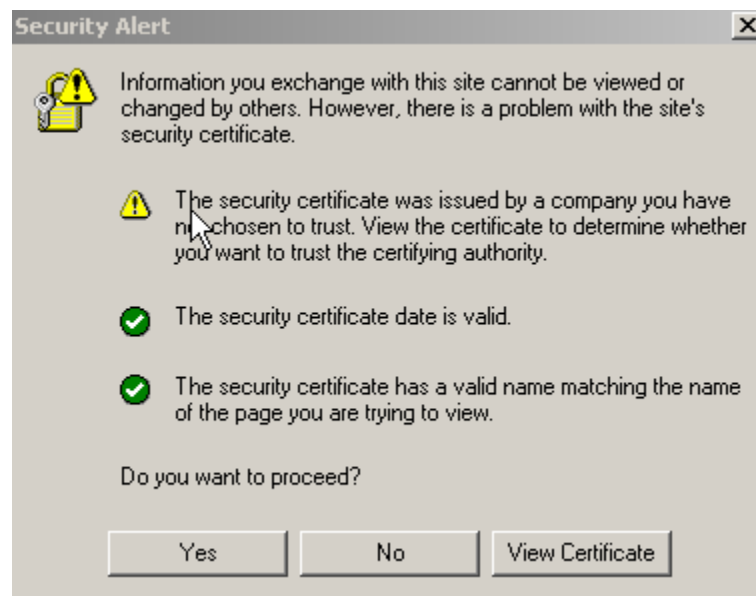
- Open the Web browser on the Client PC that is going to connect to the VPN Concentrator and enter <https://130.2.2.2>.
- At the login prompt, enter the user credentials created earlier and select **Login**.



The screenshot shows the Cisco Systems WebVPN Services login interface. At the top, there is a header with the Cisco Systems logo and the text "WebVPN Services". Below this, there is a "Login" section with a purple background. It contains the text "Please enter your username and password." followed by two input fields: "Username" with the value "SSLUser" and "Password" with masked characters "•••••". Below the input fields are two buttons: "Login" and "Clear".

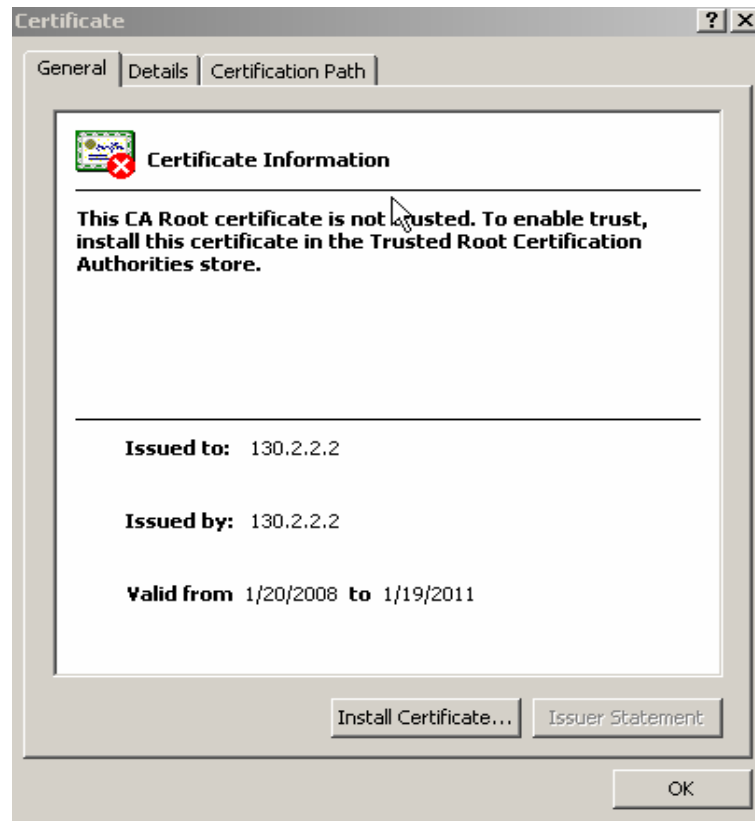
After login, the certificate alert appears.

- Click **View Certificate** to view the certificate.



Since this is the first time the client logs in, the certificate has not been installed on the PC yet.

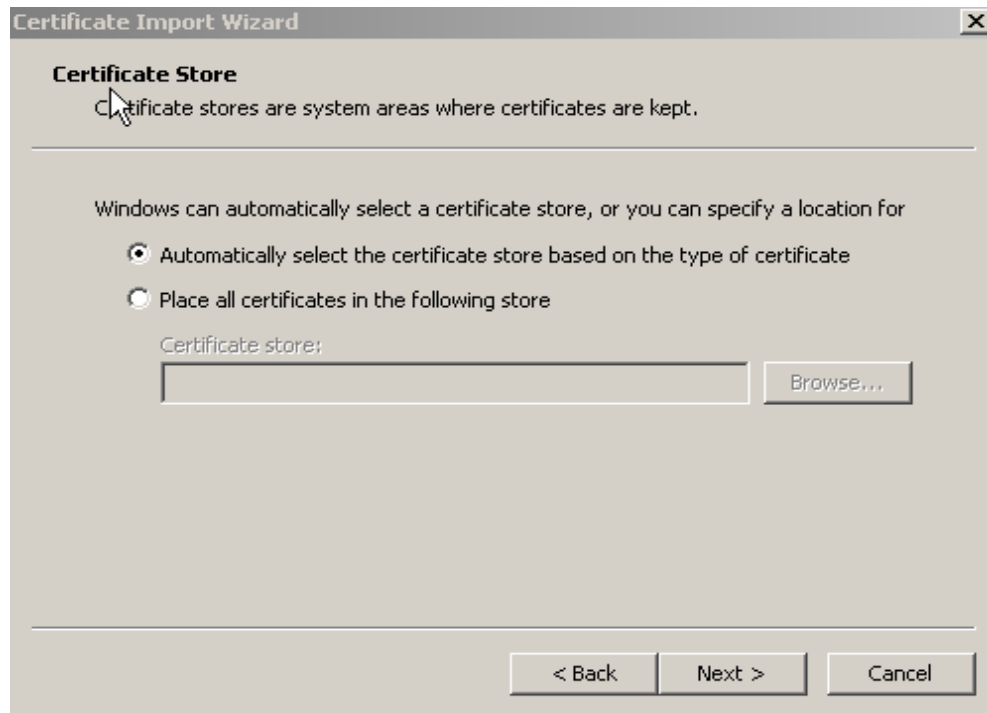
- Click **Install Certificate**



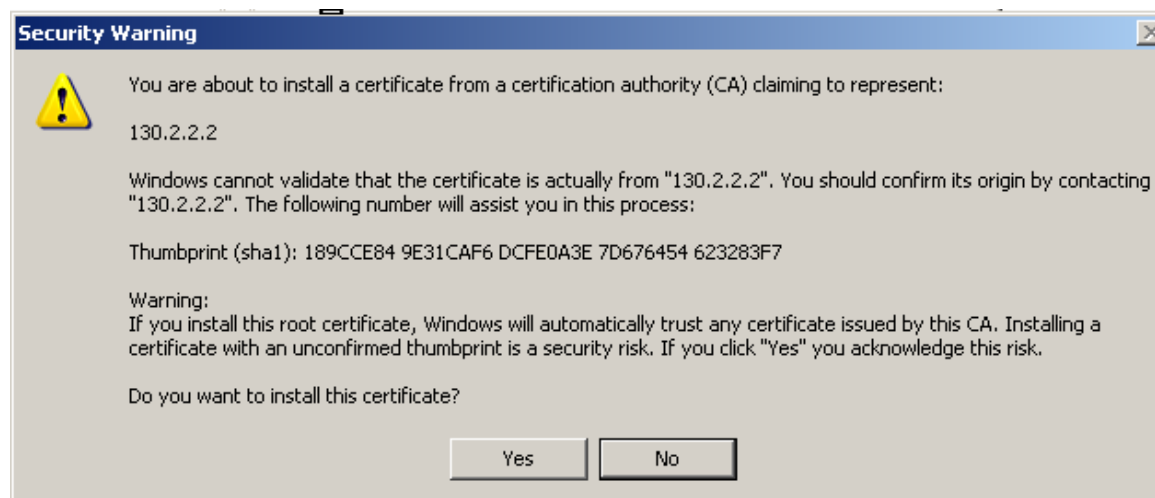
- Click **Next**



- Select **Automatically select a certificate store based on the type of certificate**
- Click **Next**



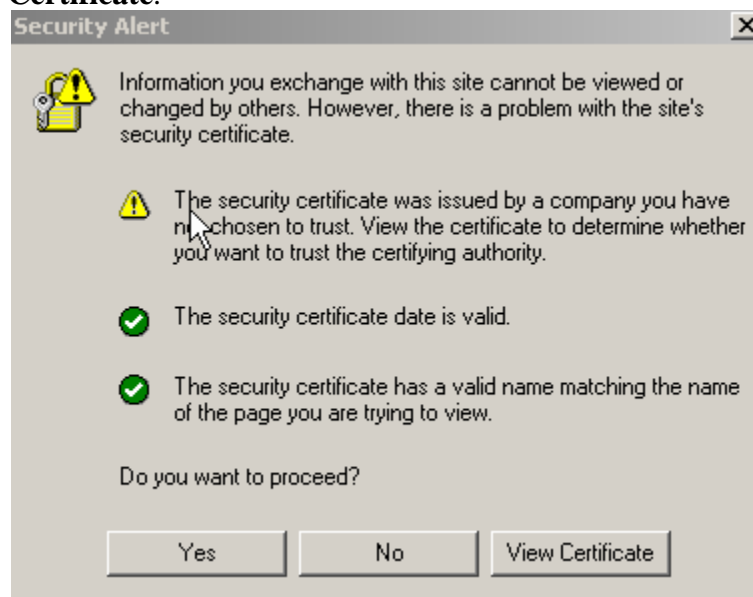
- Click **Yes**.



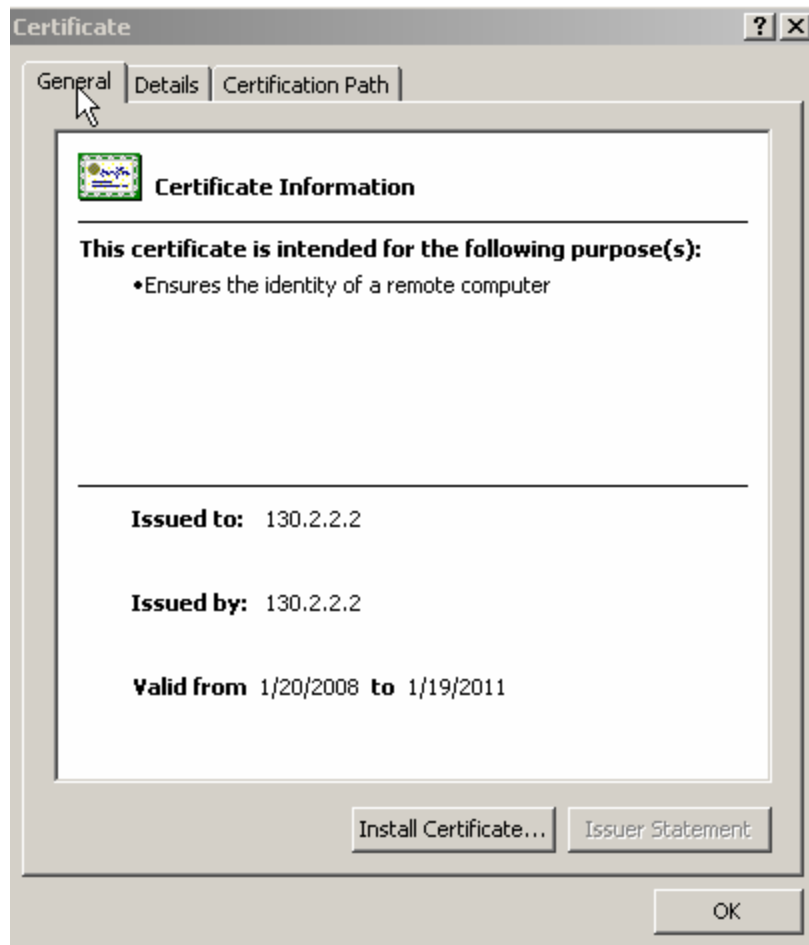
- Click **Finish**.




- Click **View Certificate**.



The **Certificate** screen shows a validated certificate.



- Click **OK**

After clicking **OK**, the SSL VPN Client is installed on the client PC. The WebVPN connection is automated as well. Once the tunnel is established, the Key icon  appears on the Windows taskbar.

5. Avaya Communication Manager Configuration

All the commands discussed in this section are executed on Avaya Communication Manager using the System Access Terminal (SAT). This section assumes that basic configuration on Avaya Communication Manager has already been completed.

The Telephones in corporate network are in IP Network Region 1 and use codec G.711 (not shown). The Avaya IP Softphones are assigned to IP Network Region 2 using the IP address range of the VPN Client IP Address Pool. IP Network Region 2 is then assigned to a codec set configured with the G.729 codec.

5.1. IP Softphone Administration

An Avaya IP Softphone is administered similar to other IP telephones within Avaya Communication Manager. Note that the IP SoftPhone field needs to be set to **y**. Following screen shows how to add an extension 333-1666 on Avaya Communication Manager.

add station 3331666		Page 1 of 5
STATION		
Extension: 333-1666	Lock Messages? n	BCC: 0
Type: 4620	Security Code: *	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: IP-Softphone	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 333-1888	
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 Softphone? n	

add station 3331666		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		
Multimedia Mode: enhanced		
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: 333-1666	Always Use? n	IP Audio Hairpinning? n

For additional information regarding the administration of Avaya Communication Manager, see reference [3].

5.2. IP Codec Sets Configuration

Use the **change ip-codec-set n** command to configure IP Codec Set parameters where n is the IP Codec Set number.

1. Use the **change ip-codec-set 2** command to define a codec set for the G.729 codec as shown below.

```
change ip-codec-set 2                                     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:

Media Encryption
1: none
2:
```

5.3. IP Network Regions Configuration

Use the **change ip-network-region n** command to configure IP Network Region parameters where n is the IP Network Region number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

1. **Intra-region** and **Inter-region IP-IP Direct Audio** determines the flow of RTP audio packets. Setting these fields to **yes** enable direct audio between the IP endpoints. **Codec Set 2** is used for IP Network Region 2 as described in **Section 5.2**.

```
change ip-network-region 2                               Page 1 of 19

                                IP NETWORK REGION
Region: 2
Location:      Authoritative Domain: avaya.com
Name:
MEDIA PARAMETERS                                Intra-region IP-IP Direct Audio: yes
Codec Set: 2                                Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                IP Audio Hairpinning? y
UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS                        RTCP Reporting Enabled? y
Call Control PHB Value: 26                    RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46                            Use Default Server Parameters? y
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 3
Audio 802.1p Priority: 5
Video 802.1p Priority: 5                    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5 IP NETWORK REGION
```

Page 3 of the IP-Network-Region form, shown below, defines the codec set to use for intra-region and inter-region calls. Note that the calls between region 2 and region 1 will use codec set 2 for audio.

change ip-network-region 2										Page 3 of 19	
Inter Network Region Connection Management											
src	dst	codec	direct	WAN-BW-limits		Video			Dyn		
rgn	rgn	set	WAN	Units	Total	Norm	Prio	Shr	Intervening-regions	CAC	IGAR
2	1	2	y	NoLimit							n
2	2	2									
2	3										

Use the **change ip-network-map** command to map all IP Softphones to IP Network Region 2, which is using G.729 codec.


change ip-network-map										Page 1	
IP ADDRESS MAPPING											
From IP Address		(To IP Address		Subnet		Region	VLAN	Emergency			
		or Mask)						Location			
192.168.1	.1	192	.168.1	.254	24	1	n	Extension			
10	.10	.50	.230	10	.50	.50	.250	24	2	n	

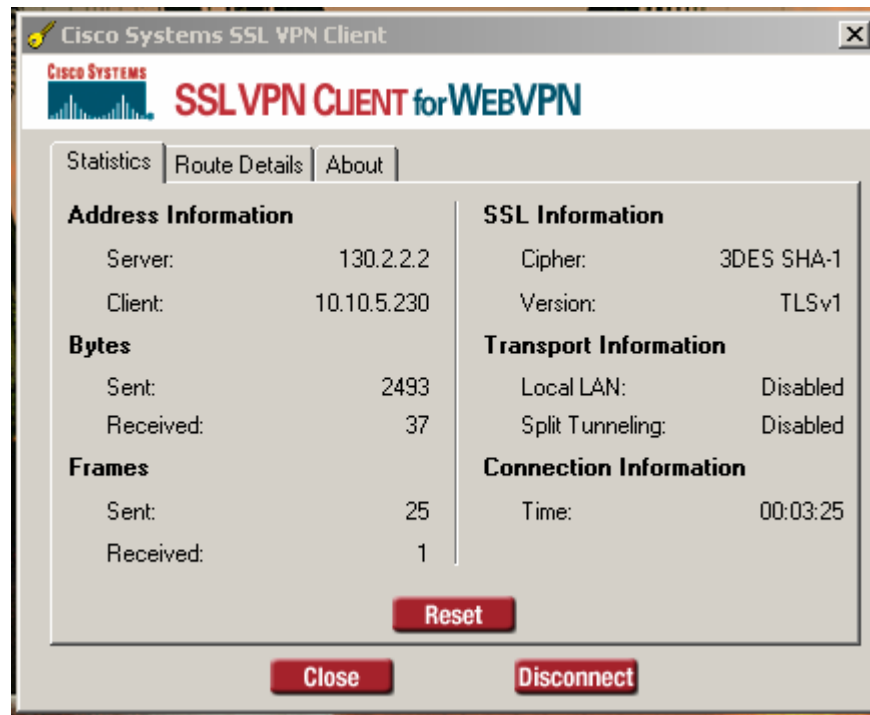
6. Verification

6.1. Cisco SSL VPN Client Status

At client PC, open command window and type **ipconfig** to verify that the IP address **10.10.5.230** from the address pool has been assigned to client Ethernet adapter.

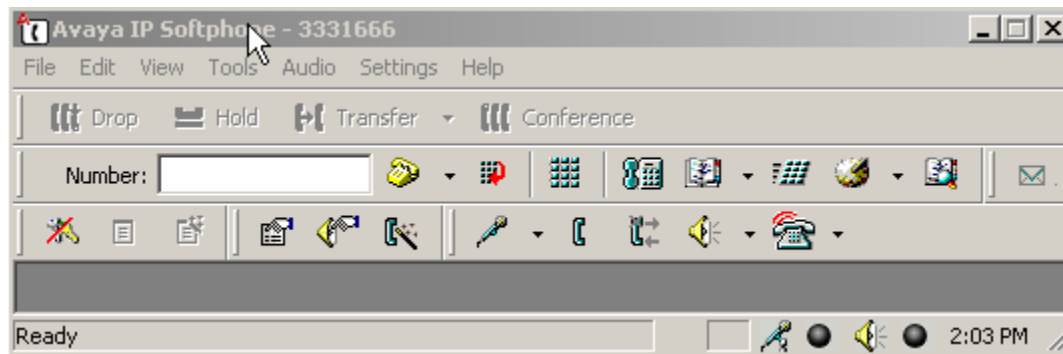
Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. C:\Documents and Settings\Administrator>ipconfig											
Windows IP Configuration											
Ethernet adapter Local Area Connection:											
Connection-specific DNS Suffix . :											
IP Address. : 172.16.2.101											
Subnet Mask : 255.255.255.0											
Default Gateway : 172.16.2.1											
Ethernet adapter Local Area Connection 3:											
Connection-specific DNS Suffix . :											
IP Address. : 10.10.5.230											
Subnet Mask : 255.255.255.0											
Default Gateway : 10.10.5.230											

Click the client icon  on the Windows taskbar to display the client status.



6.2. Avaya IP Softphone Statistics

On client PC, ping the Cisco 3020 VPN Concentrator public interface IP address to verify the connectivity before launching the VPN client. Once the Cisco VPN Client establishes an IPsec tunnel with the Concentrator, launch a ping from the client PC to C-LAN and verify that the ping is successful. Start the Avaya IP Softphone from the client PC 1 and verify that the IP Softphone is registered with Avaya Communication Manager and becomes functional. The screen capture below shows the status of the IP Softphone station 3331666.



From the Avaya Communication Manager SAT terminal, use the command **list registered-ip-stations** to show both IP Softphones are registered on Avaya Communication Manager with their inner IP addresses assigned from the address pool on Cisco 3020 VPN Concentrator.

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

REGISTERED IP STATIONS

Station	Ext/Orig Port	Set Type	Product ID	Prod Rel	Station IP Address	Net Rgn	Gatekeeper IP Address	TCP Skt
50000		4621	IP_Phone	2.800	60.1.1.66	1	192.168.1.10	y
50008		4620	IP_Phone	1.500	60.1.1.67	1	192.168.1.10	y
333-1666		4620	IP_Soft	5.620	10.10.50.230	2	192.168.1.10	y
333-1667		4621	IP_Soft	5.242	10.10.50.231	2	192.168.1.10	y

Make a call from the IP Softphone (x333-1666) to IP Telephone (x50000) and verify the status of the IP Softphone as shown below. Notice on page 1, the IP Softphone Service State is **in-service/off-hook**.

```
status station 3331666
```

Page 1 of 7

GENERAL STATUS

Administered Type: 4620	Service State: in-service/off-hook
Connected Type: N/A	TCP Signal Status: connected
Extension: 333-1666	
Port: S00002	Parameter Download: complete
Call Parked? no	SAC Activated? no
Ring Cut Off Act? no	
Active Coverage Option: 1	
EC500 Status: N/A	Off-PBX Service State: N/A
Message Waiting:	
Connected Ports: S00020	

On page 3, the IP Softphone uses IP address **10.10.5.230**, which is assigned from the IP address pool defined on the Router.

status station 3331666			Page 3 of 7		
CALL CONTROL SIGNALING					
Port: S00002		Switch-End IP Signaling Loc: 01A0217		H.245 Port:	
IP Address		Port	Node Name		Rgn
Switch-End: 192.168. 1. 10		1720	c-lan		1
Set End: 10. 10. 5.230		23390			2
H.245 Near:					
H.245 Set:					

Page 4 shows this is an **ip-direct** call between IP Softphone and IP Telephone.

status station 3331666			Page 4 of 7		
AUDIO CHANNEL Port: S00002					
G.729A		Switch-End Audio Location:			
	IP Address	Port	Node Name	Rgn	
Other-End:	60. 1. 1. 66	12314		1	
Set-End:	10. 10. 5.230	2048		2	
Audio Connection Type: ip-direct					

Page 6 shows the g729a codec is used for this call.

status station 3331666		Page 6 of 7
SRC PORT TO DEST PORT TALKPATH		
src port: S00002		
S00002:TX:10.10.5.230:2048/g729a/20ms		
S00020:RX:60.1.1.66:10554/g729a/20ms		

6.3. Call Features

- Make a phone call between the two IP Softphones and verify that the call is successful and the call is IP-direct.
- While the call is up, conference the IP telephone x50008 and verify that all three parties are in conference call.

6.4. Cisco VPN Concentrator Logging

The Cisco VPN concentrator **Session Status** displays the current active session status. To display the status, select **Monitoring → Sessions → Encryption** and select the **SSLGroup** from the **Group** drag-down window.

The detailed session information is shown below.

Monitoring | Sessions | Encryption

Group SSLGroup

Active Sessions: 1

Total Sessions: 7

Encryption	Sessions		Percentage
Other	0		0.0%
None	0		0.0%
DES-56	0		0.0%
DES-40	0		0.0%
3DES-168	0		0.0%
RC4-40 Stateless	0		0.0%
RC4-40 Stateful	0		0.0%
RC4-128 Stateless	0		0.0%
RC4-128 Stateful	0		0.0%
AES-128	0		0.0%
AES-192	0		0.0%
AES-256	0		0.0%
DES-56 SSLv3	0		0.0%
3DES-168 SSLv3	0		0.0%
RC4-128 SSLv3	0		0.0%
DES-56 TLSv1	0		0.0%
3DES-168 TLSv1	1		100.0%
RC4-128 TLSv1	0		0.0%

- Select **Monitoring** → **Statistics** → **SSL** to see the SSL status.

Monitoring Statistics SSL		
	Inbound Octets	Outbound Octets
Unencrypted	17616127	18330496
Encrypted	25893168	26548316
	Sessions	
Total	156	
Active	4	
Max Active	7	

7. Conclusion

These Application Notes verify that Avaya IP Softphone can successfully interoperate with Cisco VPN concentrator and Cisco VPN client application. The Avaya IP Softphones can utilize the WebVPN established between the Cisco VPN concentrator and Cisco SSL VPN Client to provide a secure telephony communication for remote users over any broadband Internet connection.

8. References

- [1] *VPN Concentrator for WebVPN using the SSL VPN Client Configuration Example*, Doc ID: 67917 at <http://www.cisco.com/>
- [2] *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring, Release 4.7* at <http://www.cisco.com/>
- [3] *Administrators Guide for Avaya Communication Manager*, Doc ID: 03-300509, Issue 3.1, February 2007 at <http://www.avaya.com/>

©2008 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