Avaya Solution & Interoperability Test Lab

Application Notes for WEBTEXT Contact Center Messaging v1.0 with Avaya Aura® Contact Center R7.1 and Avaya Aura® Communication Manager R8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate WEBTEXT Contact Center Messaging (CCM) with Avaya Aura® Contact Center and Avaya Aura® Communication Manager to allow SMS messages get passed from the customer to Avaya Agent Desktop for Avaya Aura® Contact Center and from Avaya Agent Desktop to the customer.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to integrate WEBTEXT Contact Center Messaging (CCM) v1.0 with Avaya Aura® Contact Center R7.1 and Avaya Aura® Communication Manager R8.1 in order to pass SMS messages from the customer to Avaya Agent Desktop for Avaya Aura® Contact Center and from Avaya Agent Desktop to the customer.

These Application Notes focus on the connection from WEBTEXT Contact Center Messaging to Avaya Aura® Contact Center 7.1 using the Aura® Contact Center Enterprise Web Chat Software Development Kit (SDK) running on the Contact Center Multimedia Module (CCMM) of Avaya Aura® Contact Center (AACC) and on the ability to create a screen pop when a voice call is presented to Agent Desktop. In addition, Agent Desktop gets passed a URL allowing text/SMS messages to be sent.

Enterprise Web Chat (EWC) delivers the next generation of Web Chat in Contact Center (AACC/ACCS) 7.1. It is offered as a licensed alternative to the traditional web chat providing a secure and high-capacity chat solution. Enterprise Web Chat is rich in agent, supervisor and customer features, provided via new customer facing and agent facing set of APIs and reference implementations.

The solution uses an embedded XMPP server to host the conversations within Contact Center. In EWC, customer and agent controllers are used to request a chat and to pass messages into the desired chat room. Transcripts are kept for each chat and persisted in the Contact Center database allowing for each chat to be logged for further analysis. A notification identifying which user is typing is also included, as well as both comfort and on hold messages for the customer when the agent is slow to react to new chats. In addition, supervisors are granted the ability to observe other agents and even barge in when they are not performing adequately, these actions are guided by intrinsic data such as number of messages sent, time since last message, number of unanswered messages etc. EWC contacts can be monitored via Contact Center Real time and historical reporting. EWC is supported on AACC 7.x Avaya Aura platforms and ACCS 7.1.

WEBTEXT have developed 3 capabilities to allow Avaya Aura® Contact Center agents to receive and respond to SMS massages sent by the customer.

1. Voice Agent Messaging - to send information to voice callers or in an after-call mode.
2. Chat Agent Messaging - reply to incoming messages and have an ongoing interaction by SMS text message.
3. Call Deflection – the ability for a caller to deflection from a voice call (queue) to and SMS chat interaction.

The first two capabilities were tested as part of the compliance testing - Voice Agent Messaging and Chat Agent Messaging.

The Enterprise Web Chat SDK and reference implementation has not undergone extensive security and vulnerability assessment. It is recommended that developers and system integrators perform a full security review prior to implementing the solution.

2. General Test Approach and Test Results

The general test approach focuses on two services offered by WEBTEXT Contact Center Messaging.

1. The ability to include an SMS message to the customer while on a call to that same customer.
2. The ability of the customer to initiate an SMS chat session with a Contact Center agent.

Due to the nature of the testing where WEBTEXT Contact Center Messaging resides in the public domain, there is a Firewall in place between the Enterprise side (Avaya Aura® Contact Center and core telephony) and the cloud (WEBTEXT Contact Center Messaging). There is also an Avaya Session Border Controller for Enterprise used as a "reverse proxy" that acts as an additional Firewall in the DMZ. The connection from WEBTEXT Contact Center Messaging is to the Avaya Session Border Controller which in turn passes the messages onto AACC. This setup is clearly outlined in **Section 3**. Port 8445 was used for the secure WebSocket (WSS) and port 8081 for the WebSocket (WS). Both ports were opened on the Avaya Firewall to allow the connections take place.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and WEBTEXT Contact Center Messaging made use of a secure link using Secure Web Socket WSS. The same connection using an unsecure Web Socket was also tested.

2.1. Interoperability Compliance Testing

The testing focused on the following areas:
Avaya Aura® Contact Center Agent includes an SMS message to the customer while on a call to that same customer. For example, a call comes in, the agent wants to send a message to the caller while talking to them, perhaps confirming a delivery address or reference code, so the caller doesn't need to find a pen and write it down.

- A voice call is presented to the agent and the agent answers it.
- A screen pop 'pops' up on the Agent Desktop.
- The 'Number' field is auto populated with the caller id of the voice caller.
- The agent wants to send a message to the caller while talking to them, perhaps confirming a delivery address or reference code.
- The agent enters the required text and clicks 'Send SMS' as above.
- Message history for this caller appears on the right-hand side of the screen pop.

Customer initiates an SMS chat session with an Avaya Aura® Contact Center Agent.

- A customer sends an SMS to the enterprise, that SMS is received in the Agent Desktop web chat. Responses from the agent go back as SMS to the customer.
- WEBTEXT connects to the Enterprise Web Chat SDK using the Avaya Session Border Controller for Enterprise.
- Messages to/from web chat are routed through this ASBCE connection.
- Incoming text message triggers a web chat event, opening web chat tab for agent.
- Agent replies to text messages in the web chat window, messages from the customer also appear in the same window.

2.2. Test Results

All test cases were executed and passed with the following exceptions, issues and observations.

1. There is an issue when the link is broken between the Avaya solution and WEBTEXT that warrants a reset on the WEBTEXT side before a new SMS can be received from that same number again.
2. The ‘less than’ < and ‘more than’ > characters are not recognised by AACC Web Chat and therefore cannot be sent by the agent to the customer and when received by the agent the < character appears as < and the > character appears as >. This appears to be a limitation on AACC.
3. Testing was carried out using a secure connection to the Enterprise Web Chat using Secure WebSocket (WSS) connecting to the Avaya Session Border Controller, which was being used as a proxy server.

2.3. Support

Support for WEBTEXT Contact Center Messaging can be obtained as follows:
Website: www.webtext.com
Email: support@webtext.com

3. Reference Configuration

The configuration in **Figure 1** will be used to compliance test WEBTEXT Cloud Messaging with Avaya Aura® Contact Center utilising the Enterprise Web Chat Software Development Kit to pass SMS messages to Agents on Contact Center. An Avaya Session Border Controller for Enterprise is used as a proxy.

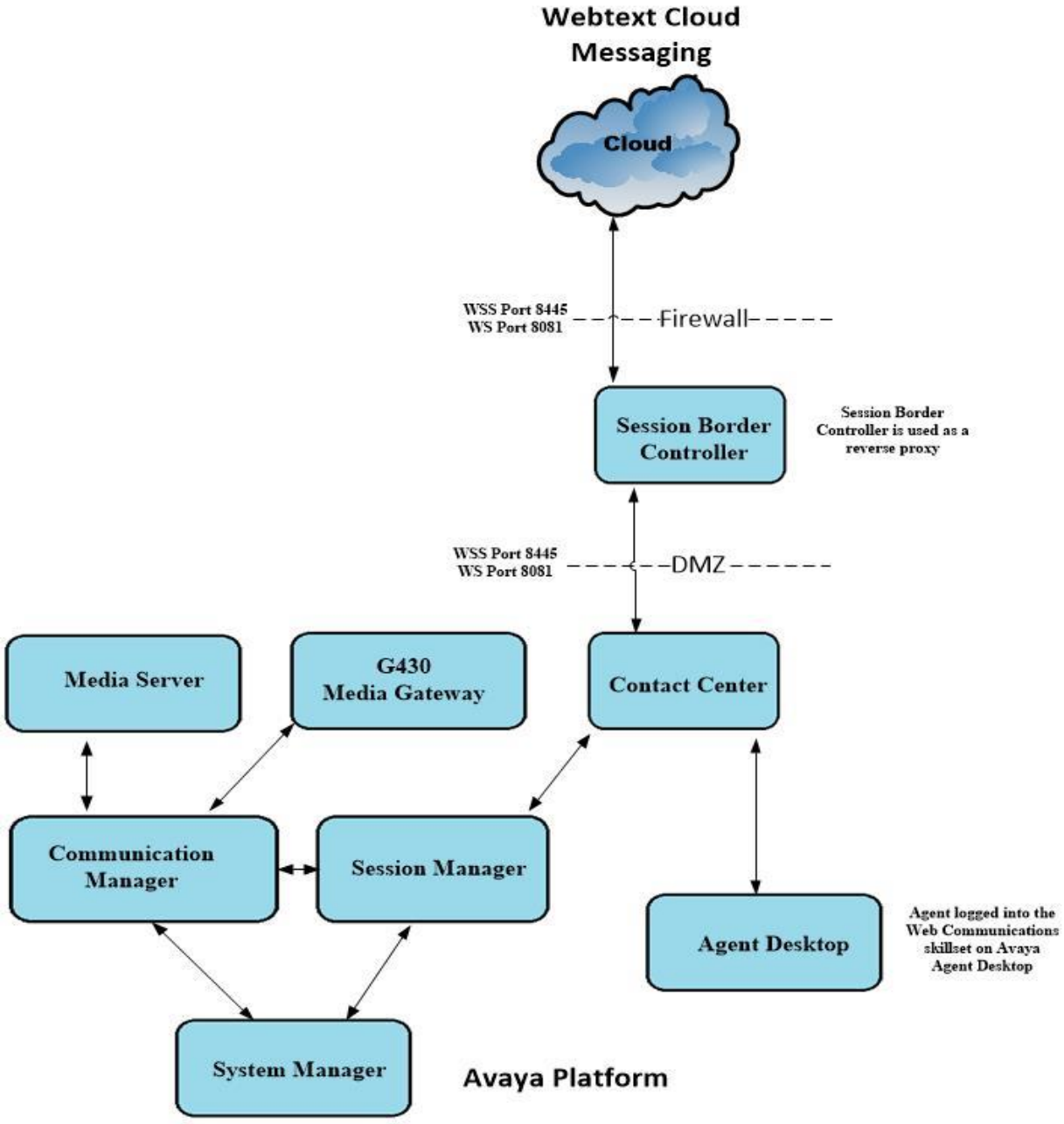


Figure 1: Connection of WEBTEXT Cloud Messaging with Avaya Aura® Contact Center R7.1

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager running on a virtual server	8.1.3.2 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.2.1012646 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	8.1.3.2 Build No. – 8.1.3.2.813207
Avaya Aura® Communication Manager running on a virtual server	8.1.3.2 – FP3SP2 R018x.01.0.890.0 Update ID 01.0.890.0-26989
Avaya Aura® Application Enablement Services running on a virtual server	8.1.3.2 Build 8.1.3.2.0.4-0
Avaya Aura® Contact Center	7.1.2
Avaya Agent Desktop running on Windows 10 PC	7.1.2
Avaya Aura® Media Server	8.0.2.184
Avaya G430 Media Gateway	41.16.0/1
WEBTEXT Contact Center Messaging	V1.0

5. Configuration of Avaya Aura® Contact Center

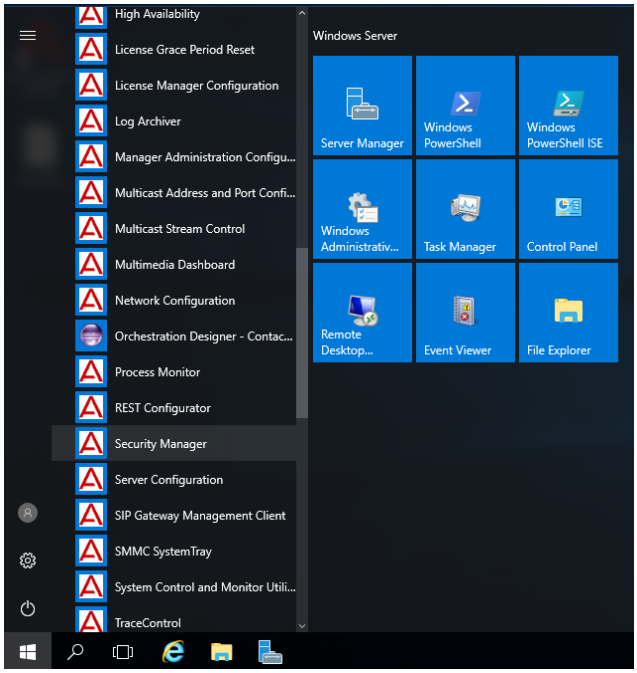
It is assumed that a fully working contact center is already in place with call routing and skillsets configured. The configuration of Contact Center for this solution focuses on the following:

1. Configure Secure and Unsecure Web Services.
2. Configure Enterprise Web Chat.
3. Configure Avaya Agent Desktop.

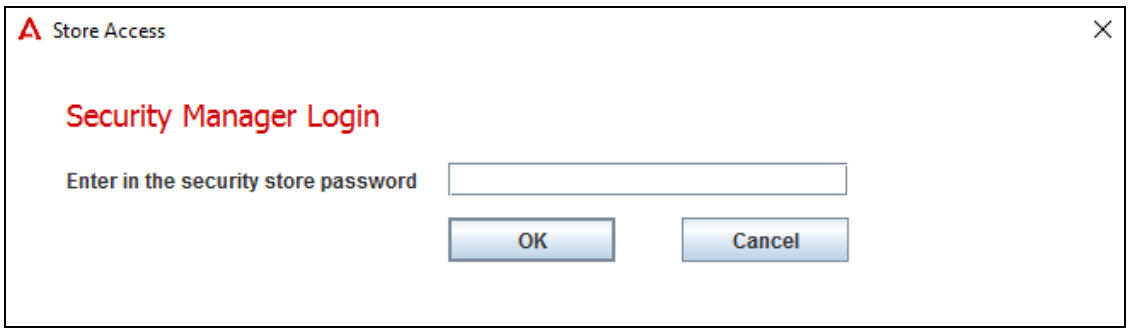
5.1. Configure Secure and Unsecure Web Services

Web services are configured to allow either secure or unsecure access, if a secure link is to be used then this must be set under Security Manager and vice versa for the unsecured link.

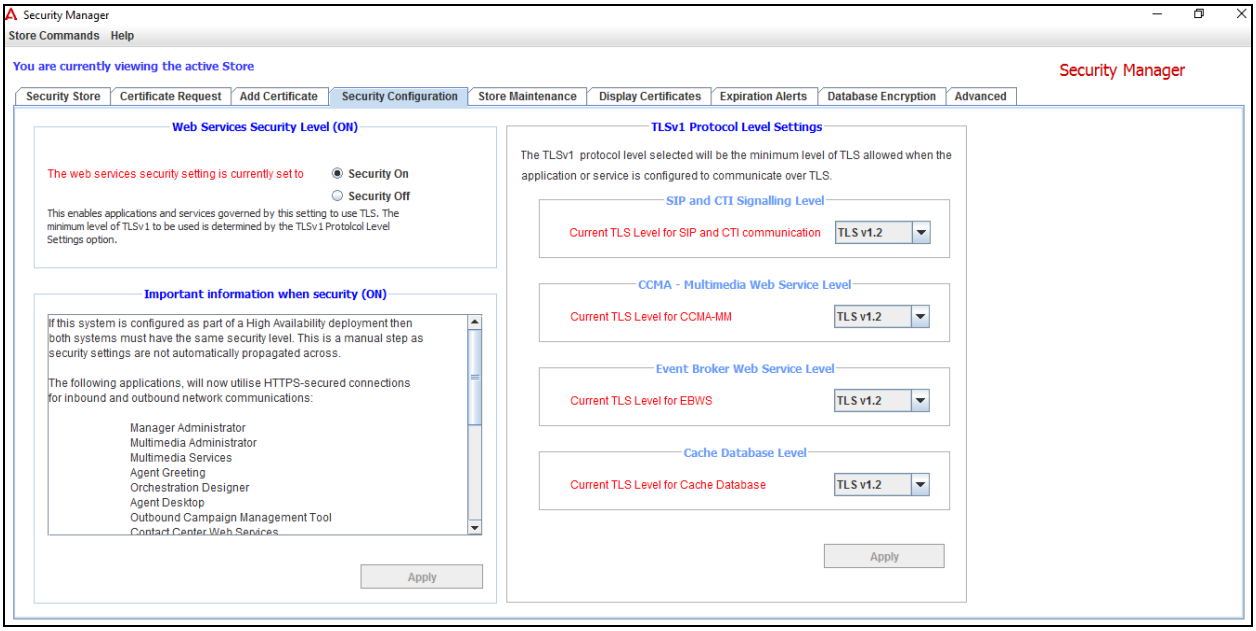
Log into AACC **Security Manager** from the AACC server as shown below.



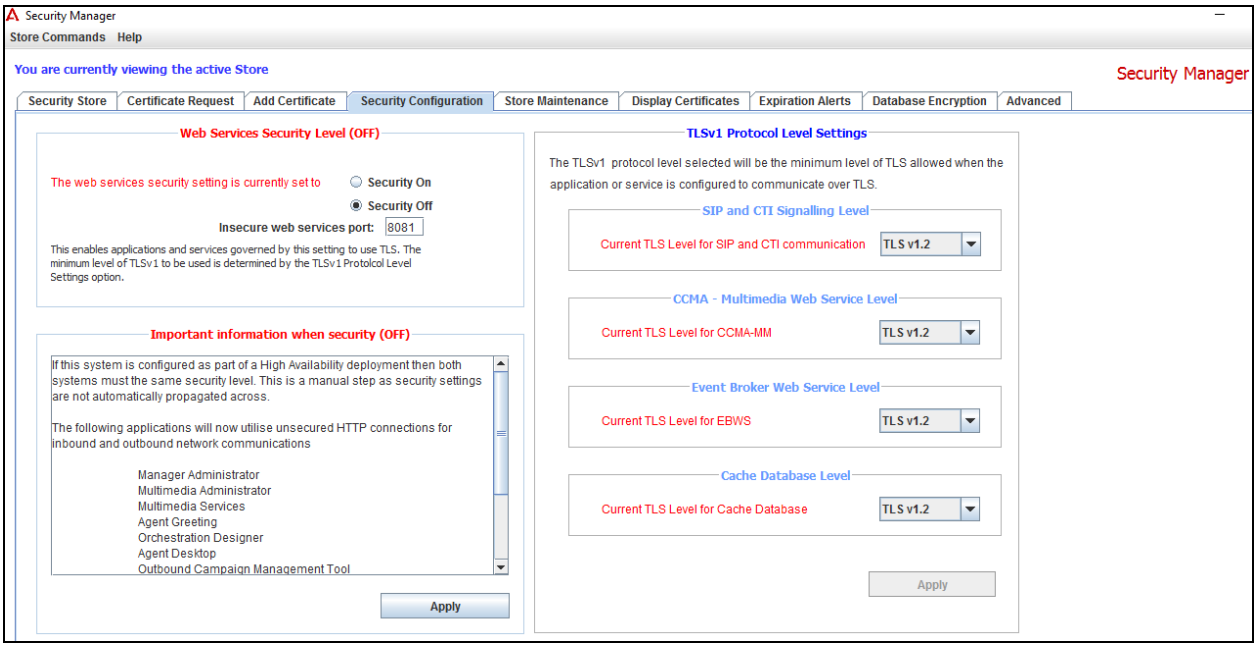
Enter the **security store password** and click **OK**.



Navigate to the **Security Configuration** tab, there are two options in the left windows under **Web Services Security Level**, **Security On** or **Security Off**. Compliance testing was carried out for both; however, it would be advised to have this set to **Security On** as shown below.

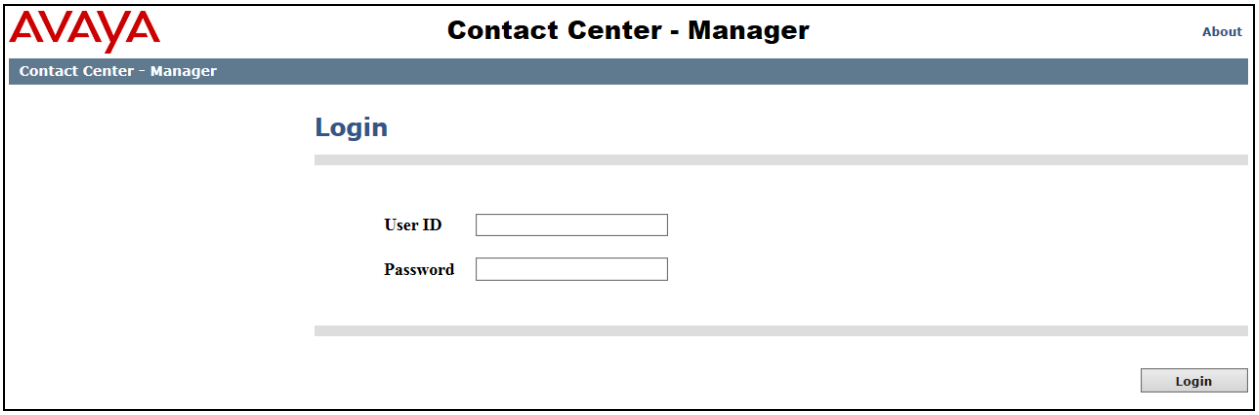


The below screenshot shows the setting for **Security Off**, and the **Insecure web services port** can be seen here as **8081**. Note that the secure port for Enterprise Web Chat is 8445.



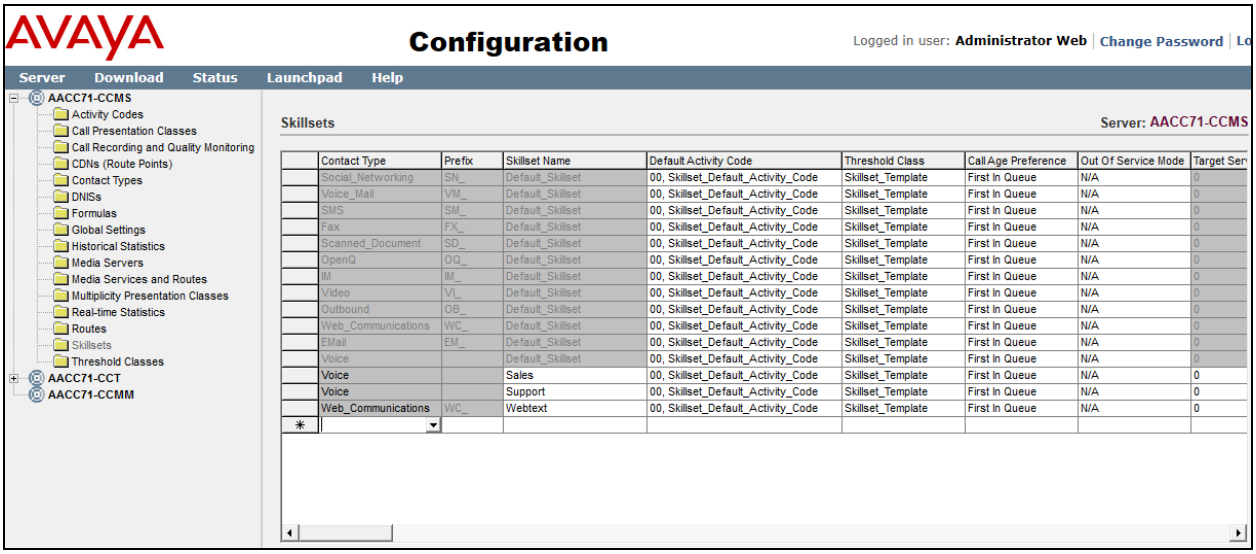
5.2. Configure Enterprise Web Chat

The remaining configuration for Contact Center is carried out using a web session to the Contact Center server. Open a web session to the Contact Center server and log in with the appropriate credentials as shown below

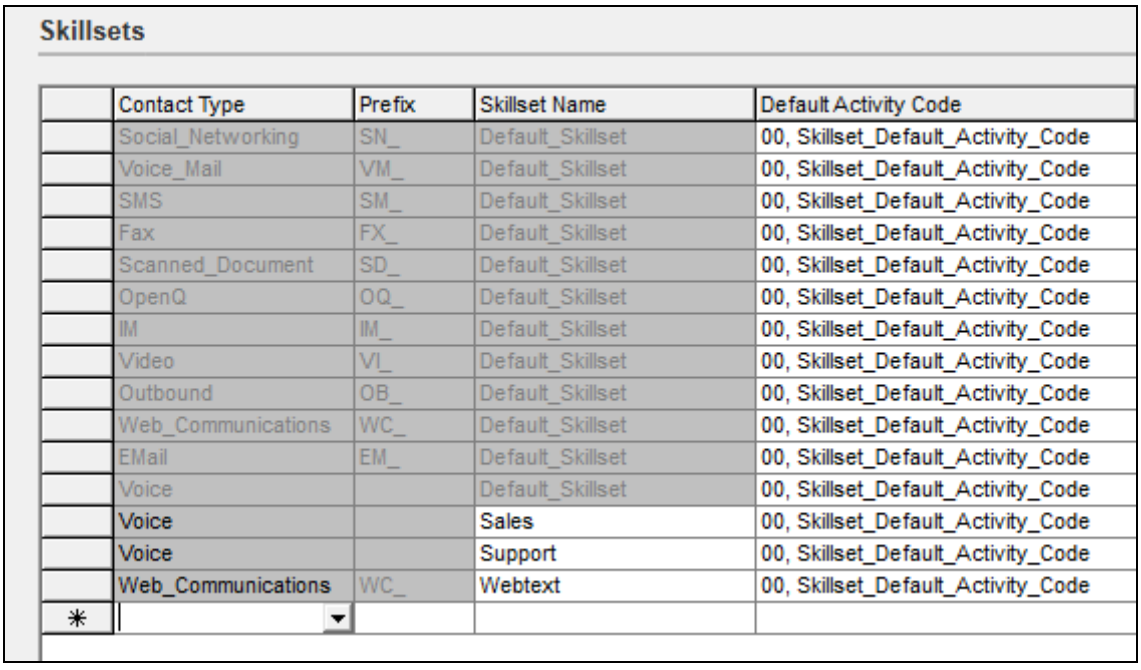


Before EWC is configured the correct skillset must be present, typically the Default Skillset is present for each contact type, however it is useful to know where to add more skillsets should this be required. From the main **Launchpad**, click on **Configuration** as shown below.

Expand the CCMS menu in the left window and click on **Skillsets**.

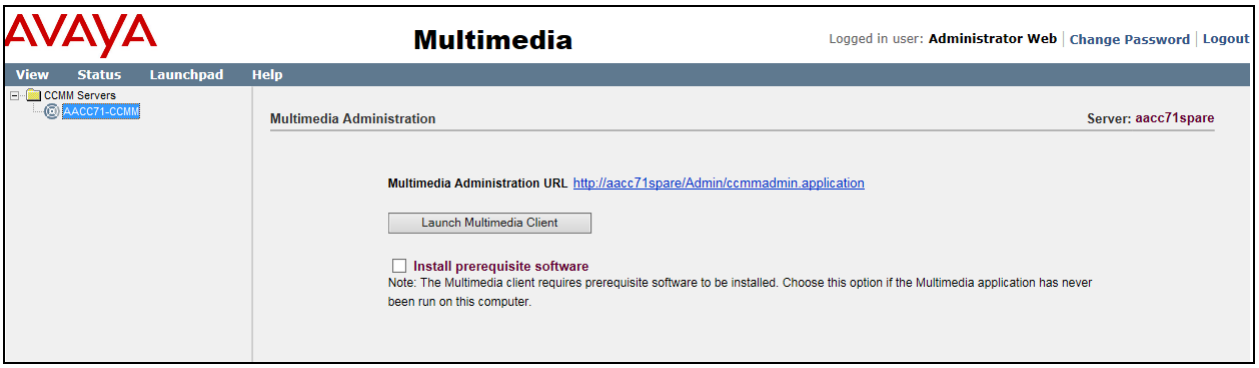


The Contact Type for an EWC skillset is **Web_Communications**, so if a new skillset was to be added for EWC then this would be of type Web_Communications. A new Skillset called **Webtext** was added for compliance testing; however, the Default Skillset called **WC_Default_Skillset** could be used also. As long as the agent in question has these skillsets assigned, then the call should route to that agent.



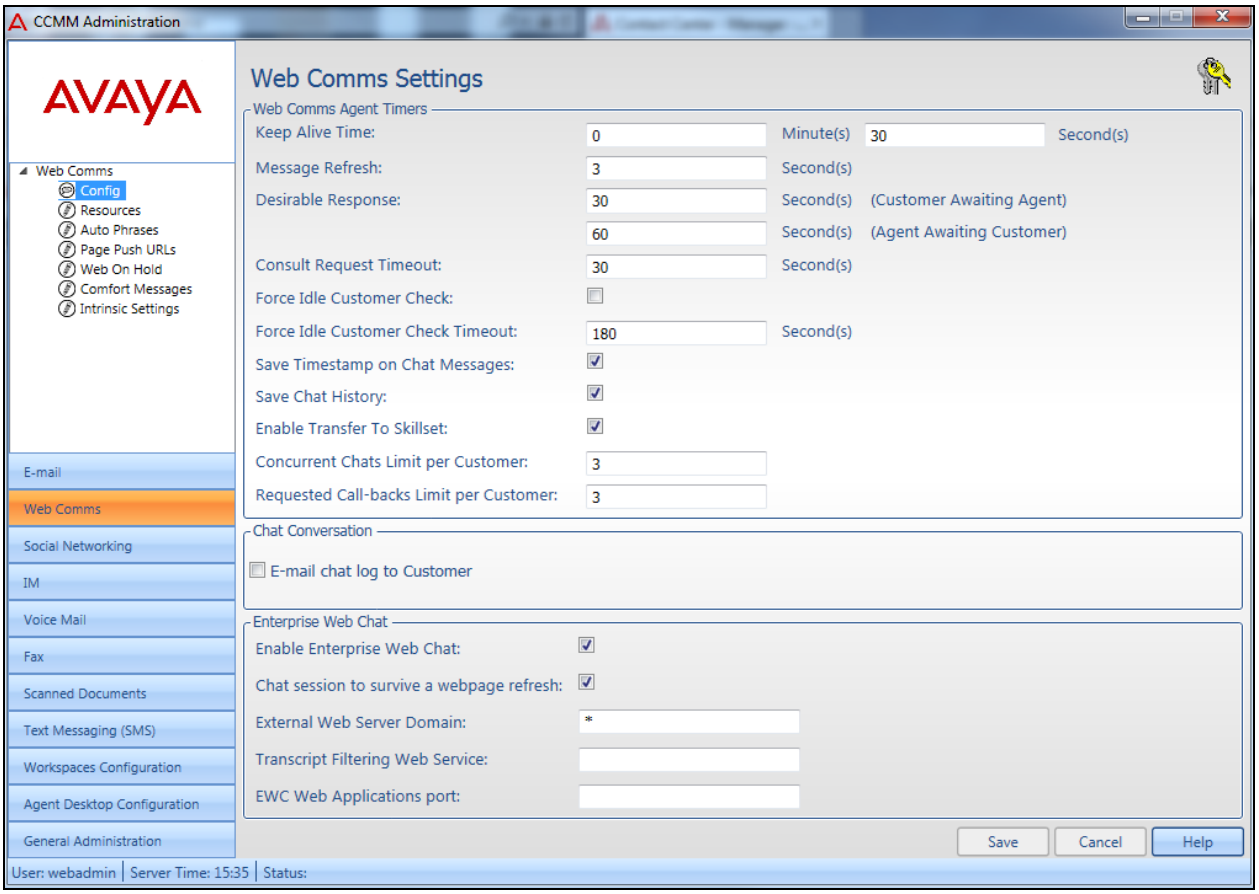
Settings for Enterprise Web Chat (EWC) are carried out from the Multimedia section. From the **Launchpad** page, click on **Multimedia**.

Click on **Launch Multimedia Client**.

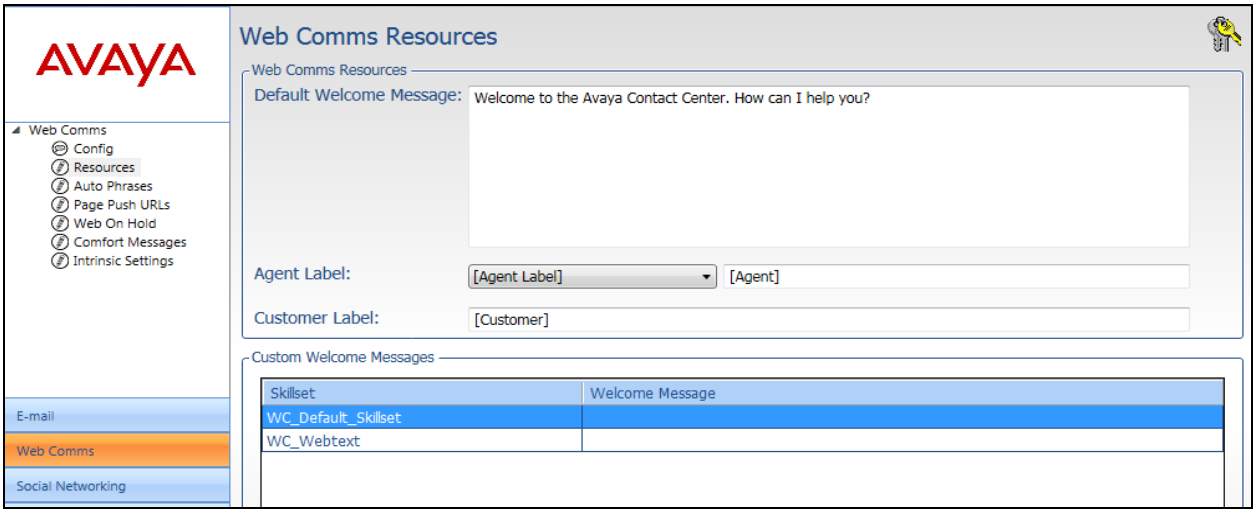


The **CCMM Administration** page is opened. Click on **Web Comms** in the left window and under config the following below are shown.

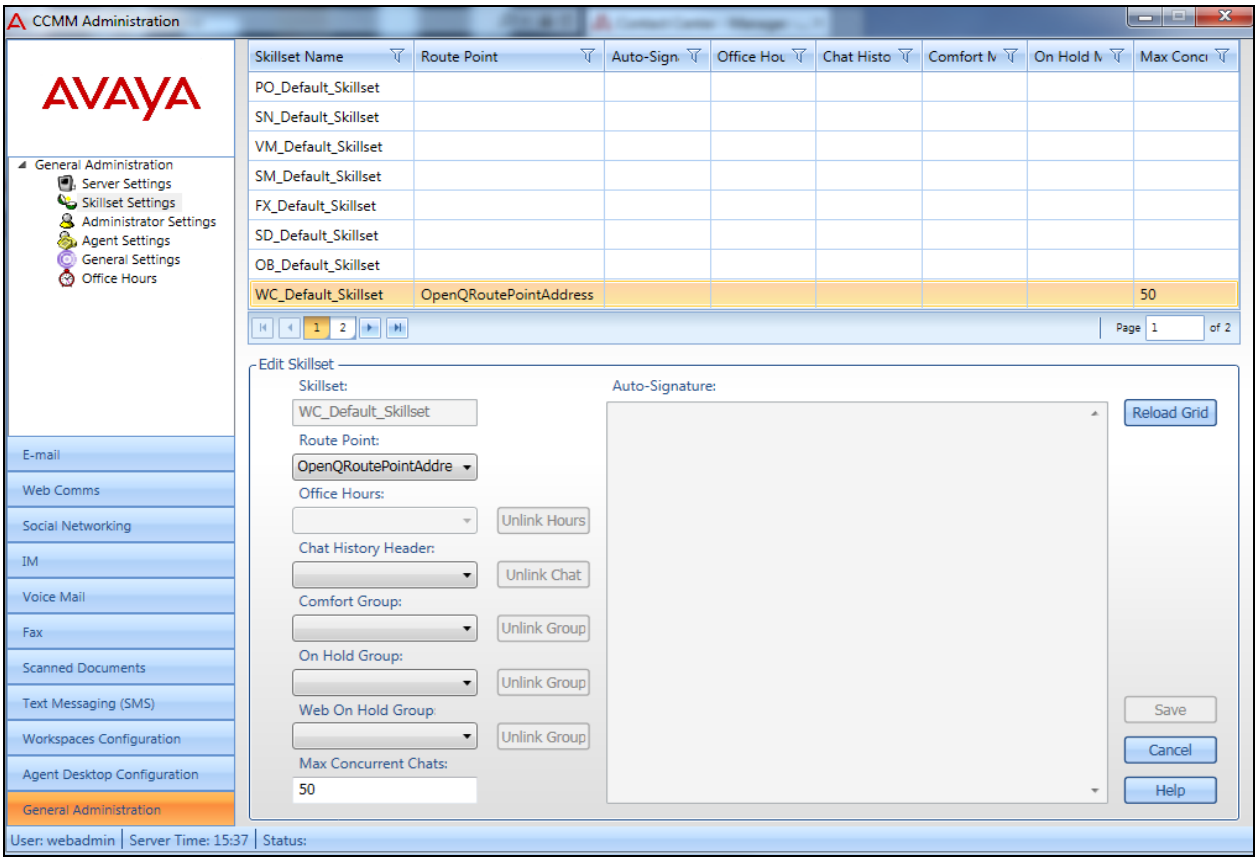
Towards the bottom of the screen the settings for **Enterprise Web Chat** are found. Ensure that both **Enable Enterprise Web Chat** and **Chat Session to survive a webpage refresh** are ticked. An asterisk (*****) is added for the **External Web Server Domain** and everything else was left as shown below.



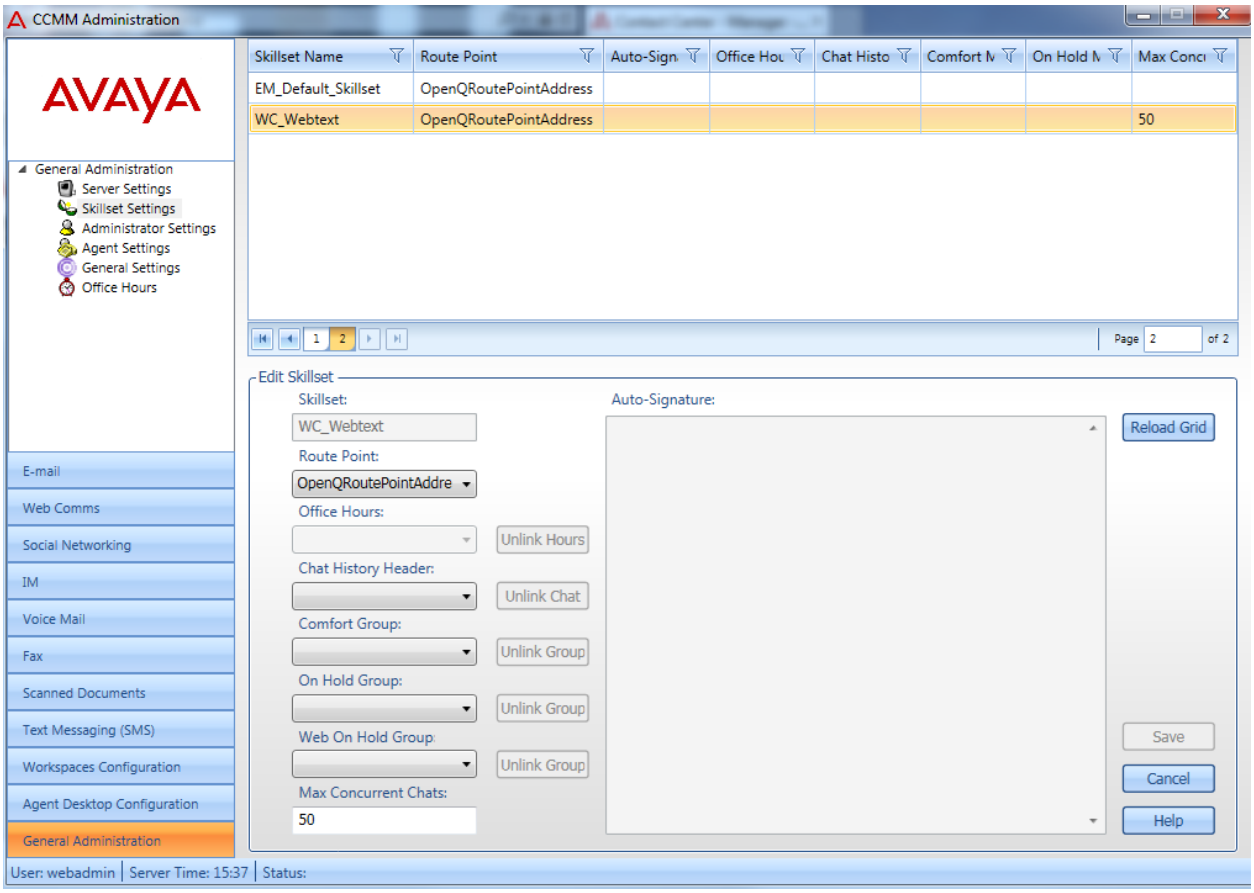
Under **Resources**, the skillsets for Contact Type Web_Communications are present, where a **Welcome Message** can be configured for each skillset, and this will be presented to the customer after the incoming SMS is received by the agent.



Click in the **General Administration** tab, as the bottom left of the screen and under **Skillset Settings**, ensure that **OpenQRoutePointAddress** is selected for the Route Point for the skillset in question.



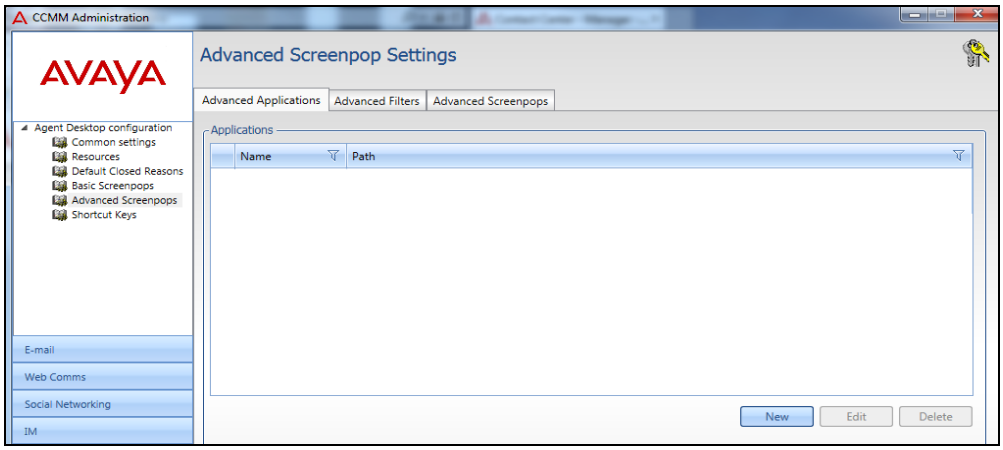
This should be the same for the added skillset **WC_Webtext**, ensure that **OpenQRoutePointAddress** is selected for the Route Point for the skillset.



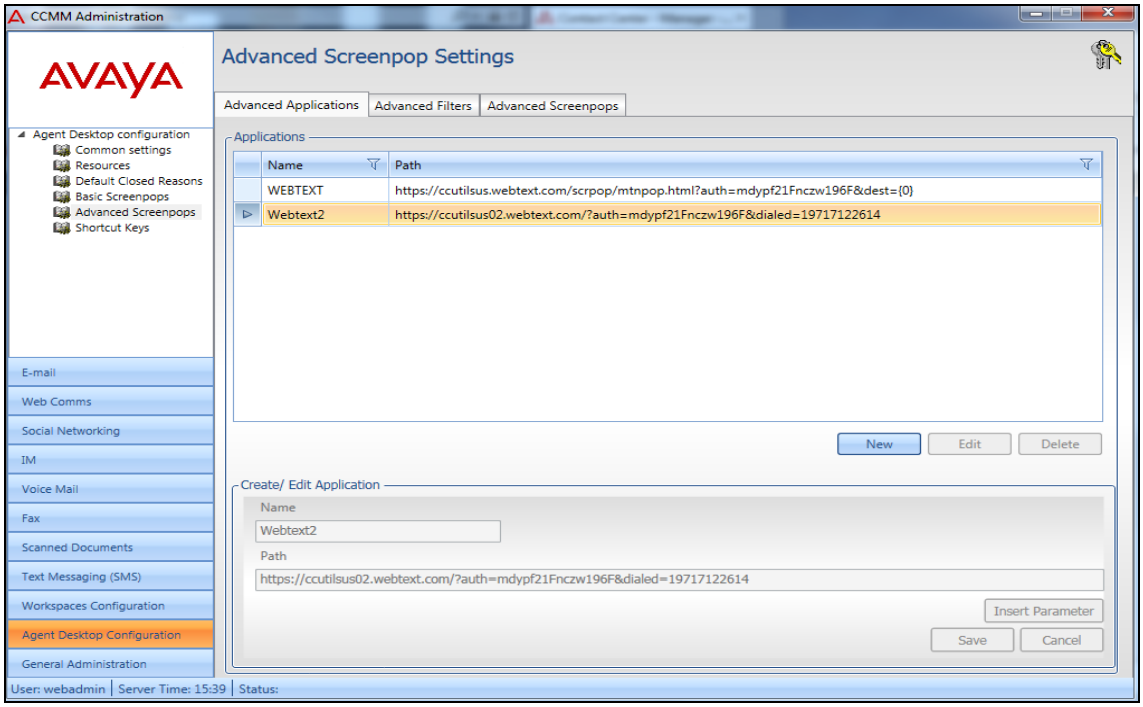
5.3. Configure Avaya Agent Desktop

The following is configured on the Agent Desktop to allow a screen pop from the WEBTEXT Cloud service, which in turn will allow the agent to send SMS messages from this resulting URL.

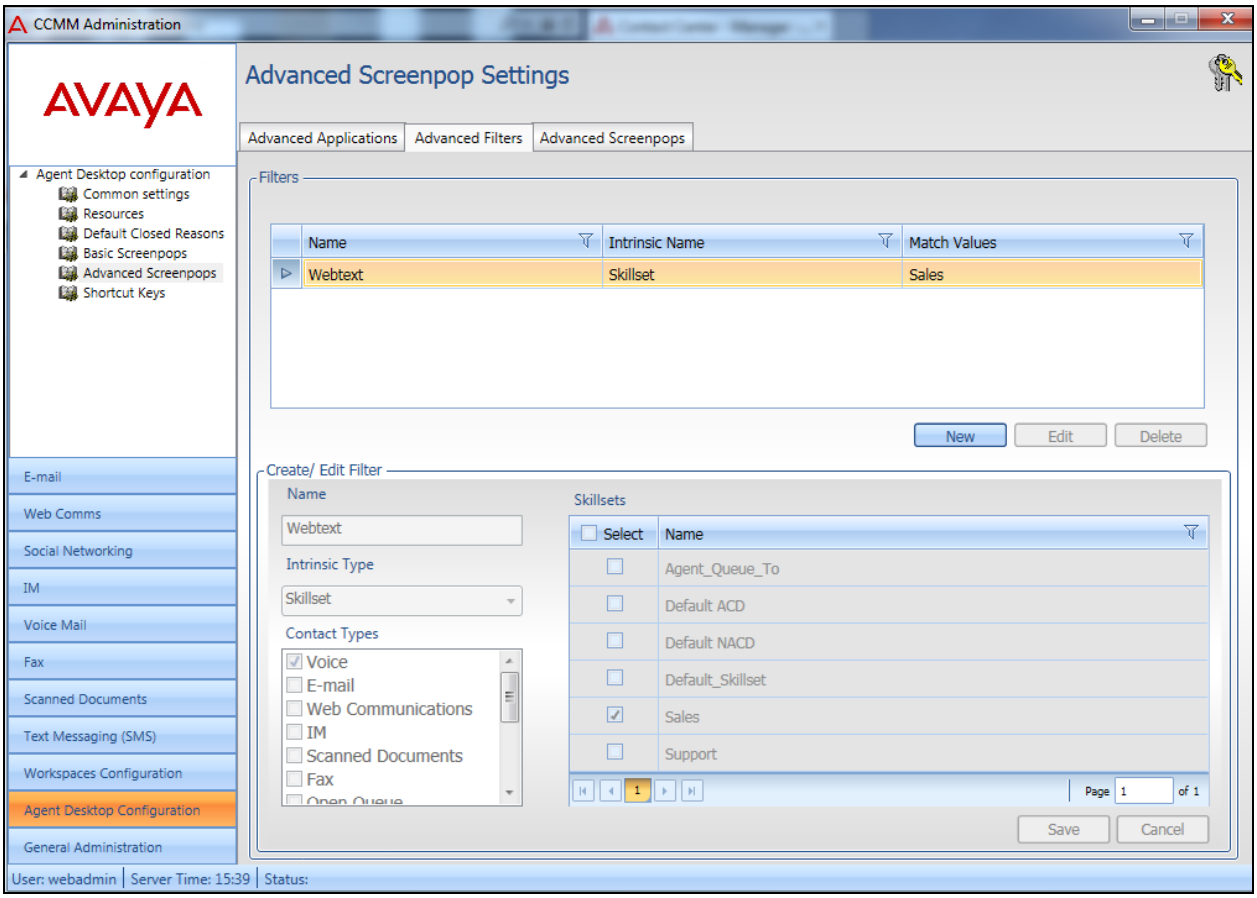
Click on **Agent Desktop Configuration** at the bottom of the left window and select **Advanced Screenpops** in the left window. From the main window click on the **Advanced Applications** tab and click on **New**.



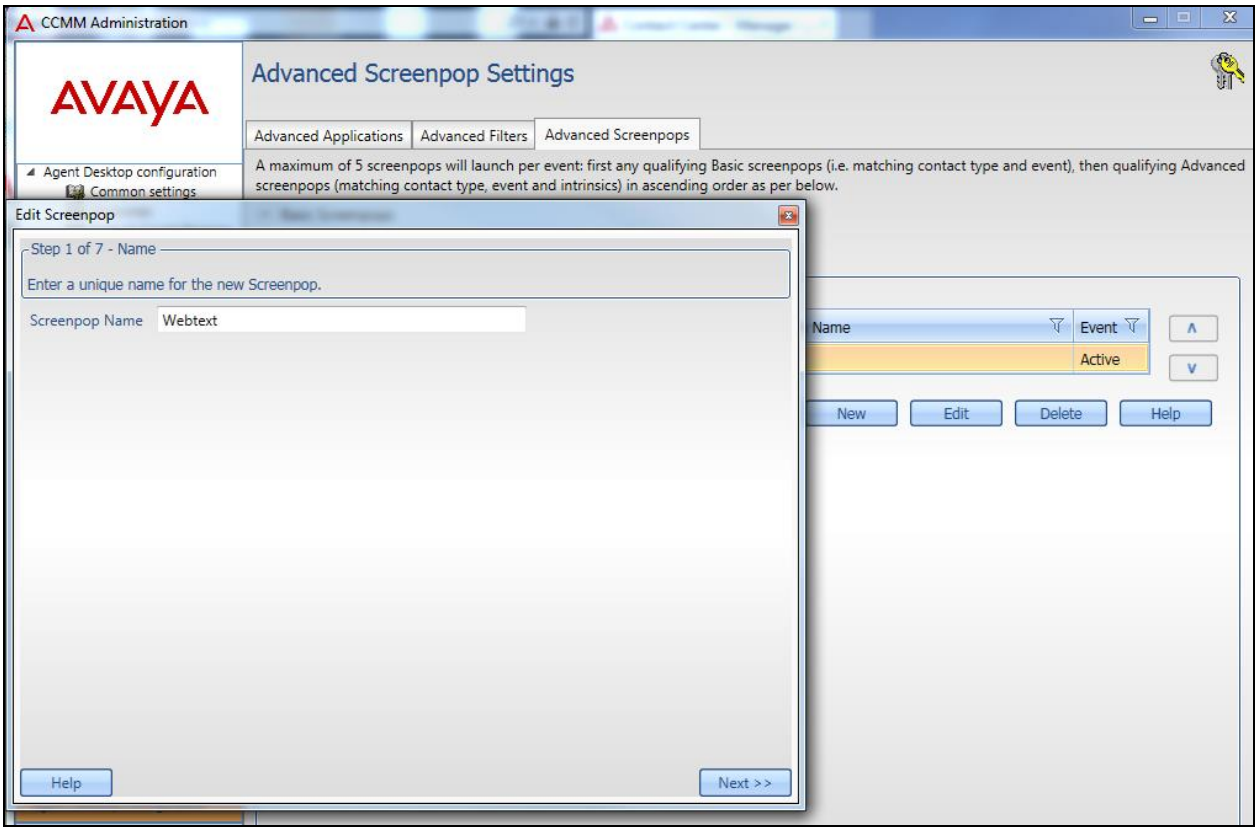
Webtext2 below is the updated version that was used for compliance testing. The information contained in the **Path** is provided directly be WEBTEXT and contains customer specific information unique to each connection.



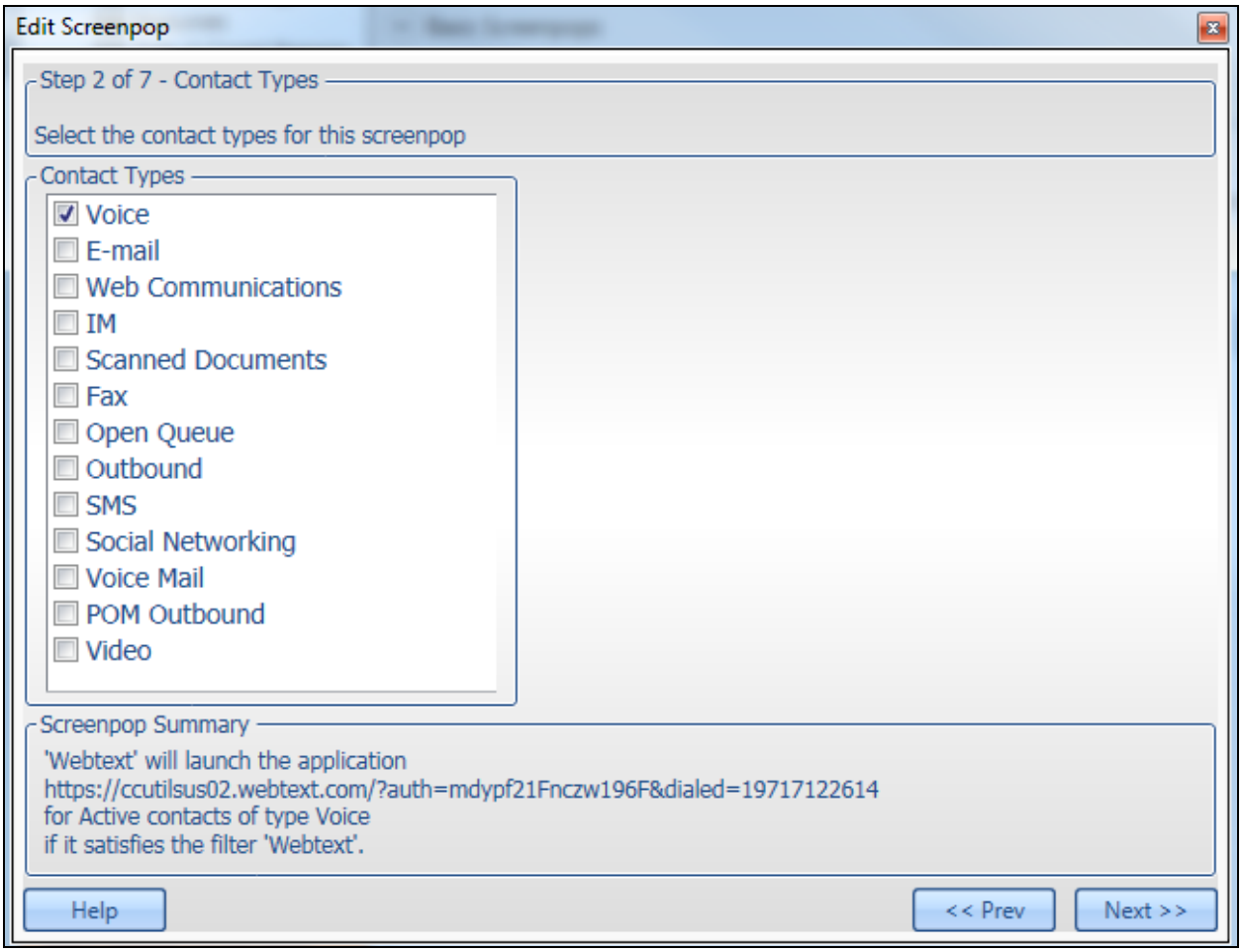
Click on the **Advanced Filters** tab and click on **New**. Below shows the configuration of the filter called **Webtext**, which was used for compliance testing. Note that the skillset **Sales** was selected which is a **Contact Type** called **Voice**. Basically, this means that these screen pops will only occur for voice calls to the skillset Sales.



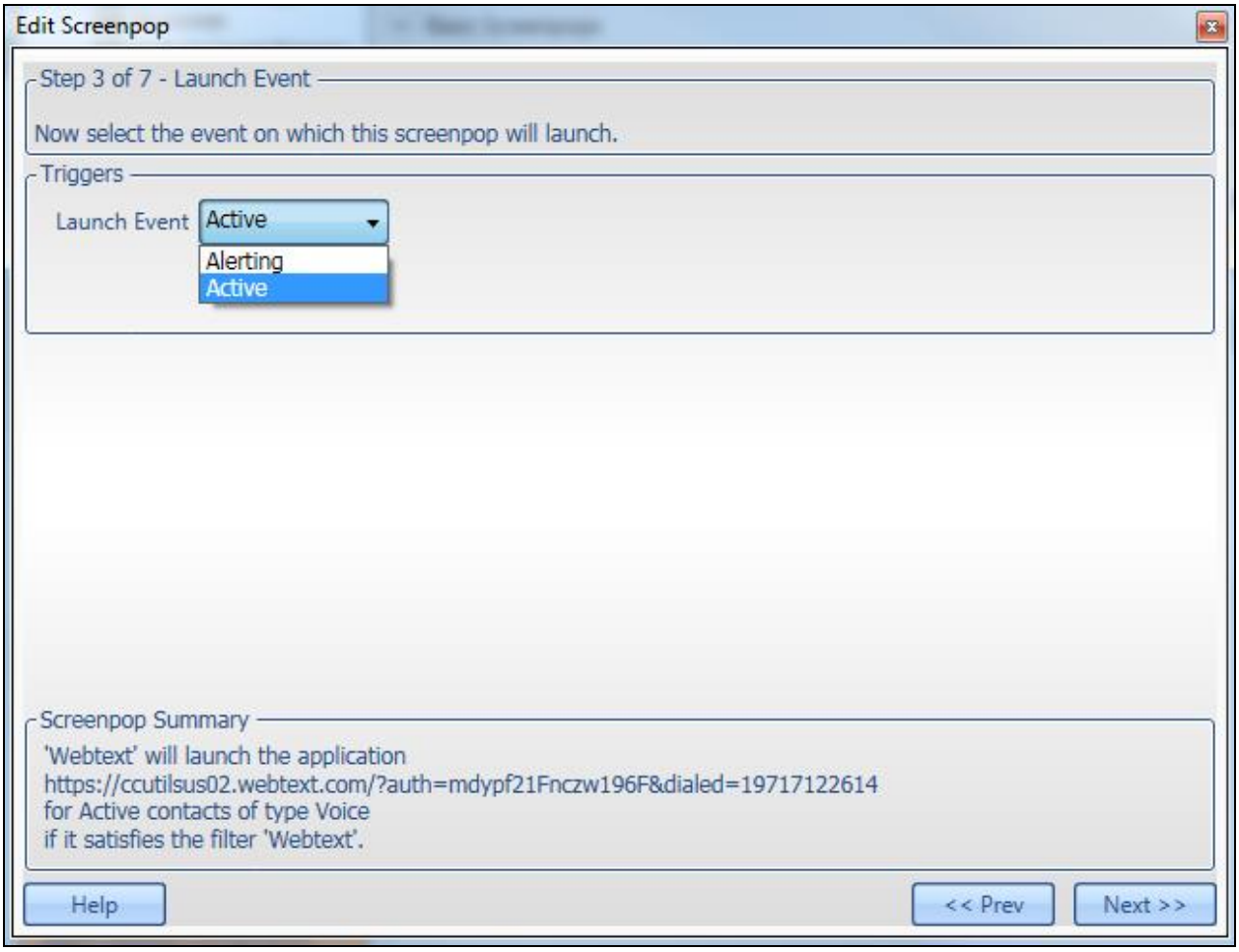
Click on the **Advanced Screenpops** tab and click on **New** in the main window. A new window opens, enter a suitable name for the screen pop and click on **Next**.



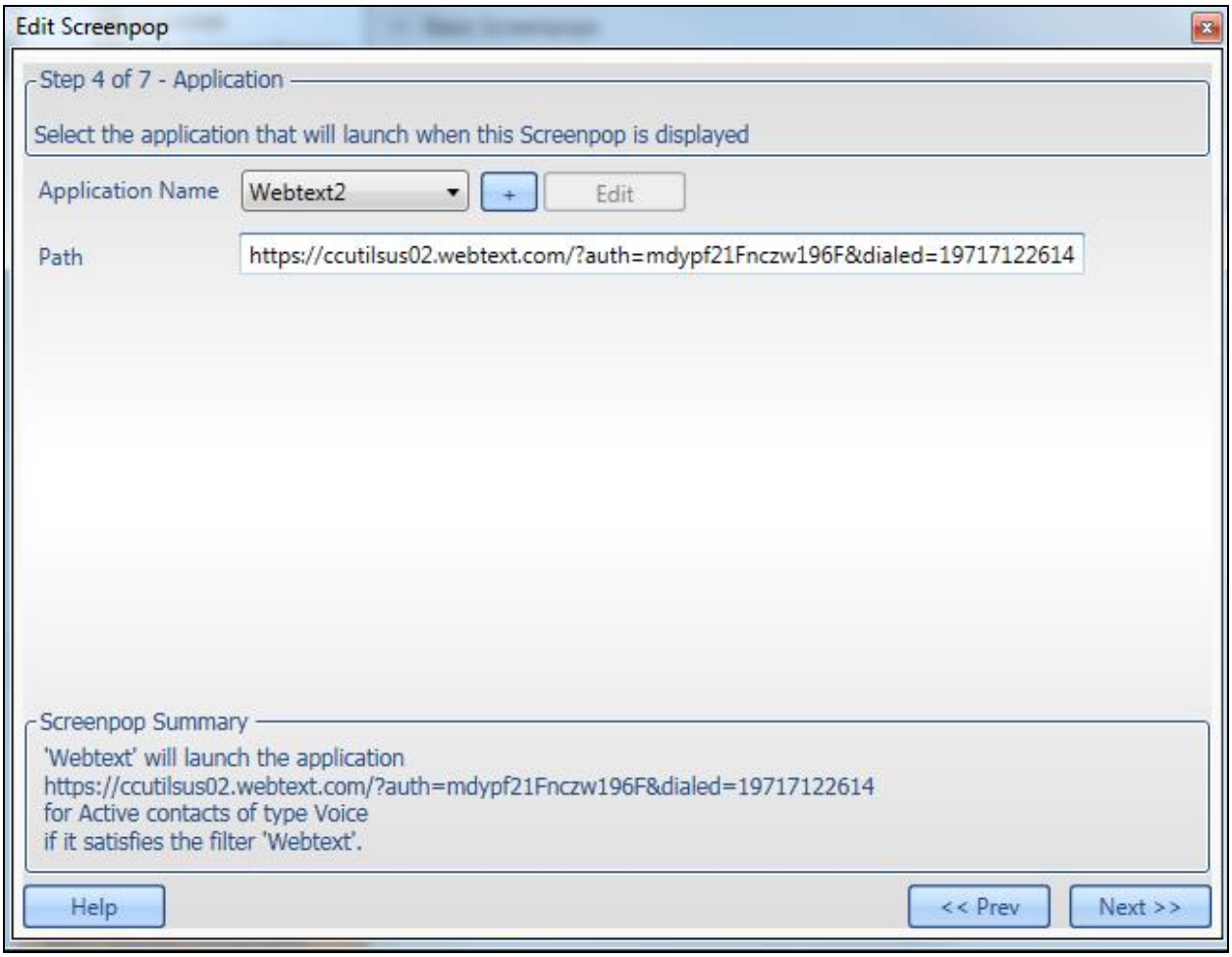
Select the correct **Contact Type**, the example below a **Voice** contact is chosen, this may vary depending on the contact type that initiates the screen pop. Click on **Next** to continue.



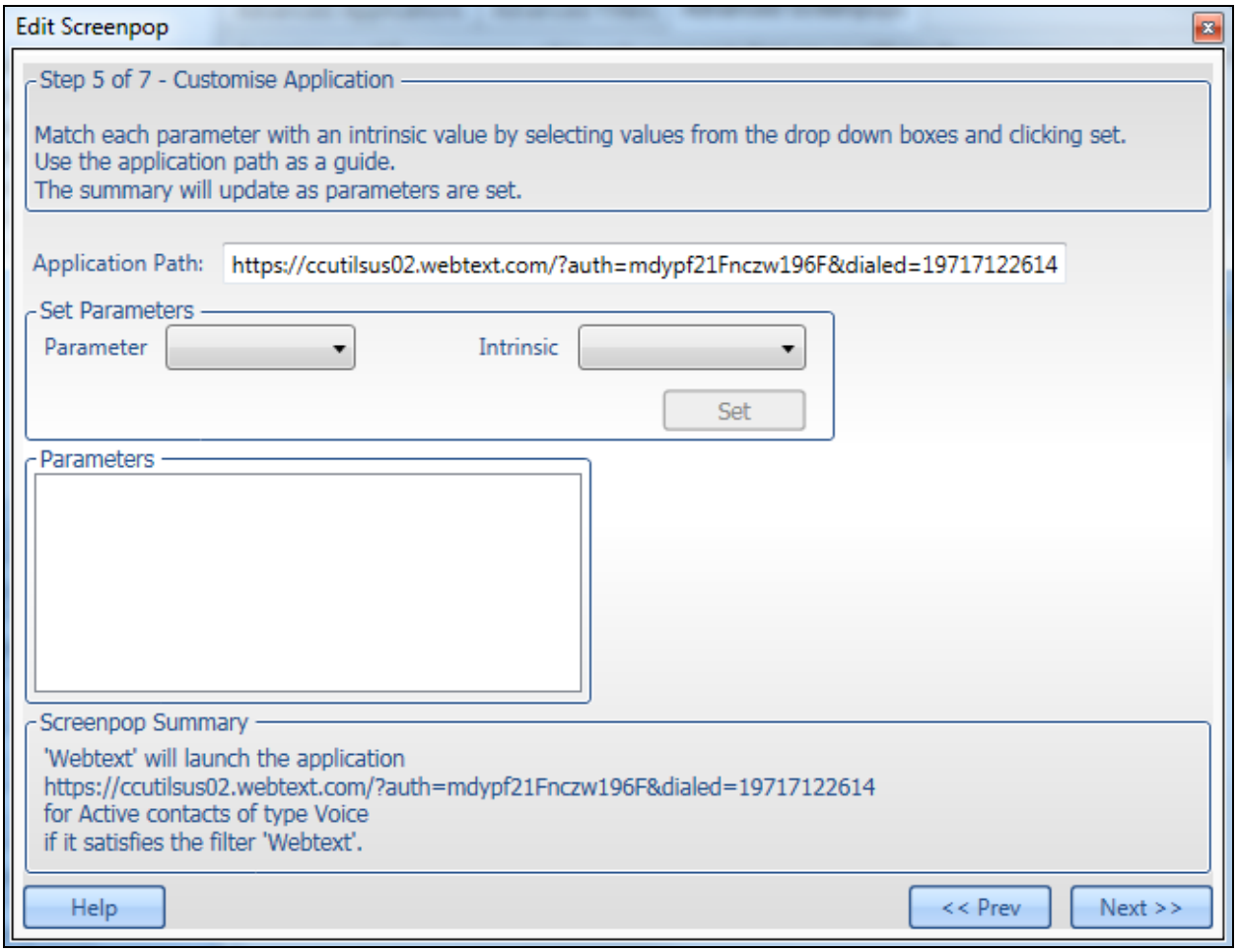
Select a suitable trigger to initiate the screen pop, in the example below **Active** is chosen to initiate the screen pop, so when a voice call is answered by the agent the screen pop is initiated. Click on **Next** to continue.



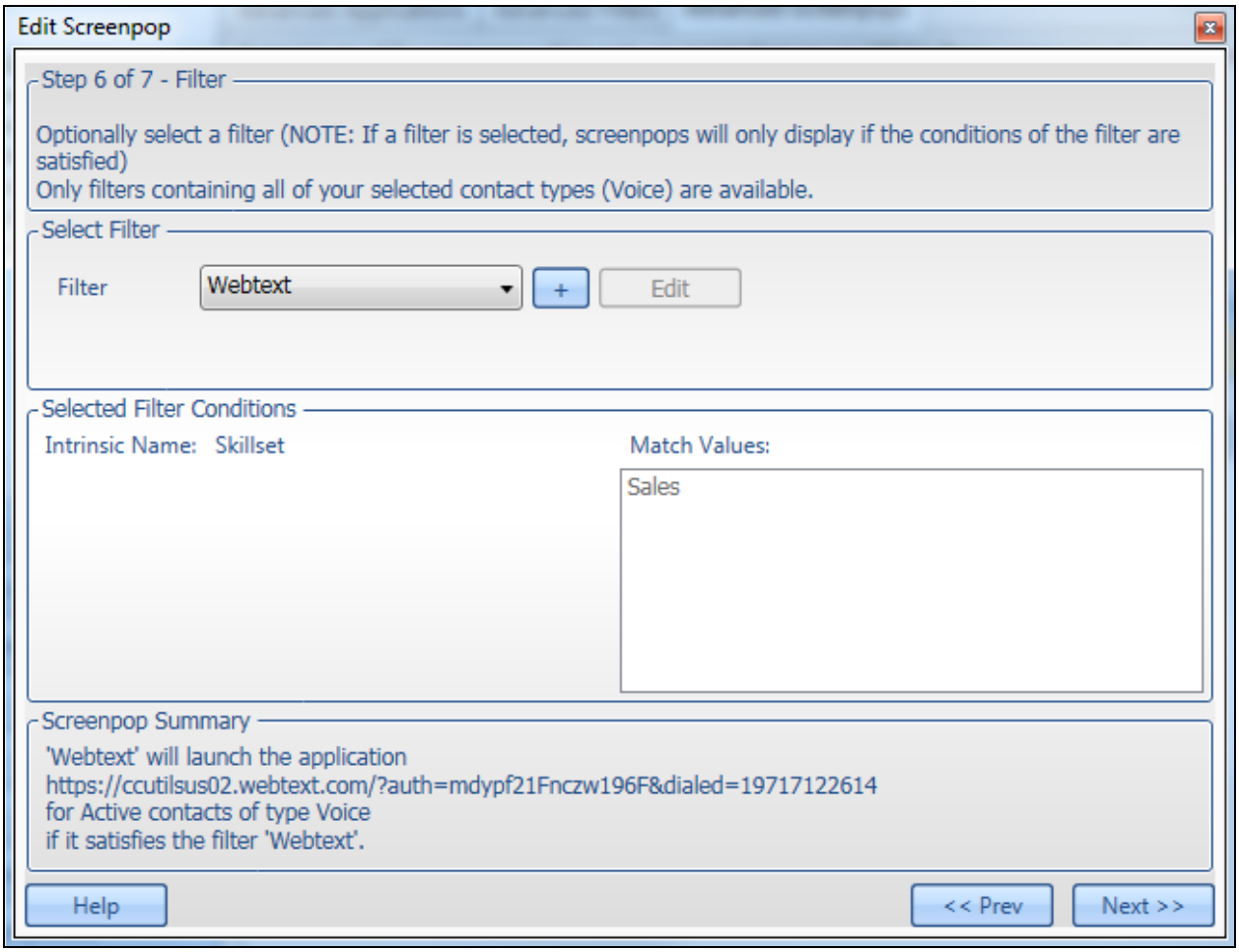
Select the **Application Name** that was created earlier from the drop-down menu and click on **Next** to continue.



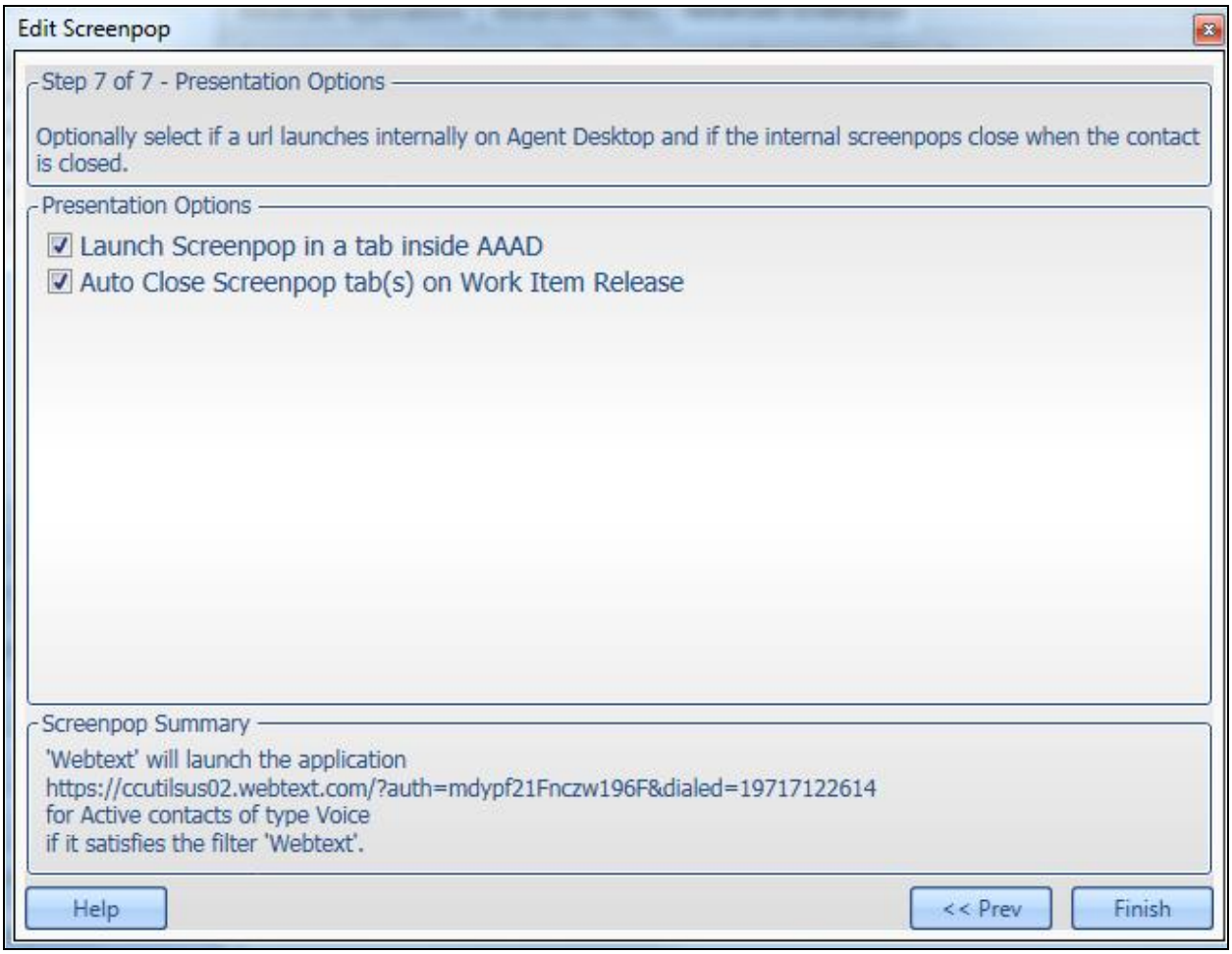
Certain **Intrinsics** can be set here but none were used for compliance testing, click on **Next** to continue.



Select the **Filter** that was created earlier from the drop-down menu and again click on **Next** to continue.



Tick the **Launch Screenpop in a tab inside AAAD** box and click on **Finish**.

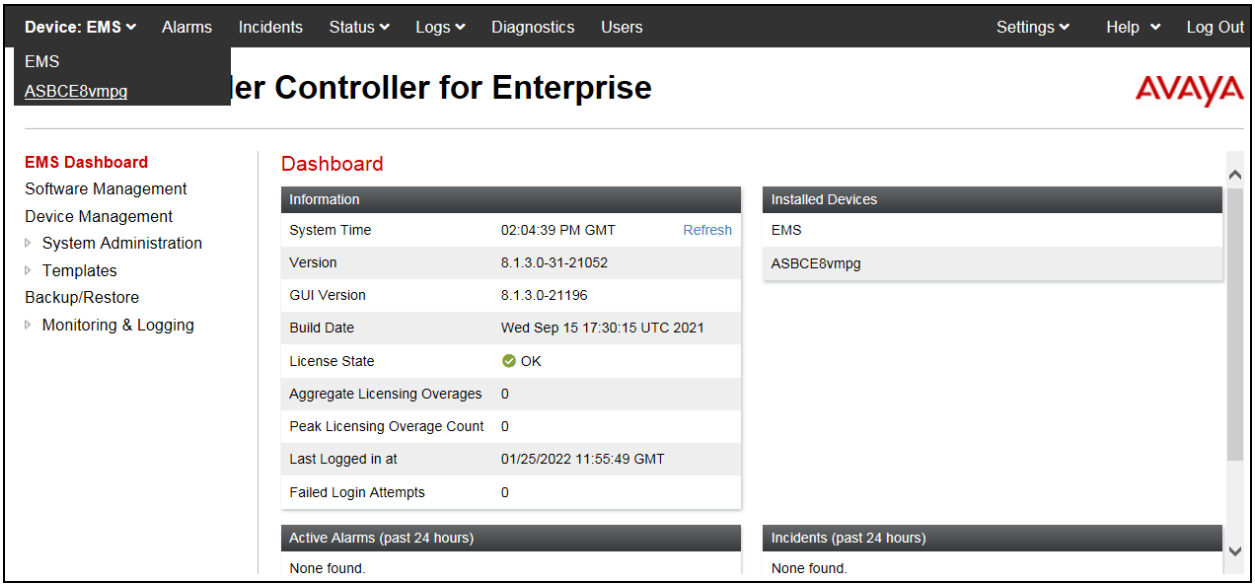


6. Configure Avaya Session Border Controller for Enterprise

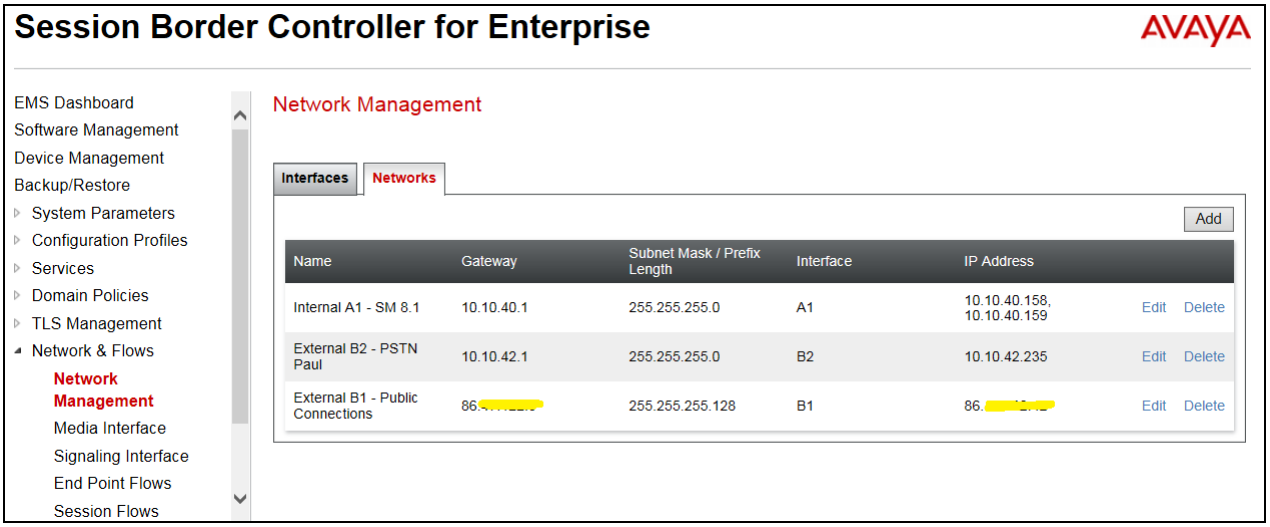
Although third parties could connect directly to Contact Center, it is strongly recommended to use some kind of proxy server to do so, and one such solution would be to use the Avaya Session Border Controller for Enterprise and its Reverse Proxy configuration. This section goes through the setup that was configured for compliance testing and may be of some use when setting up something similar.

Open a URL to the SBCE and log in with the appropriate credentials.

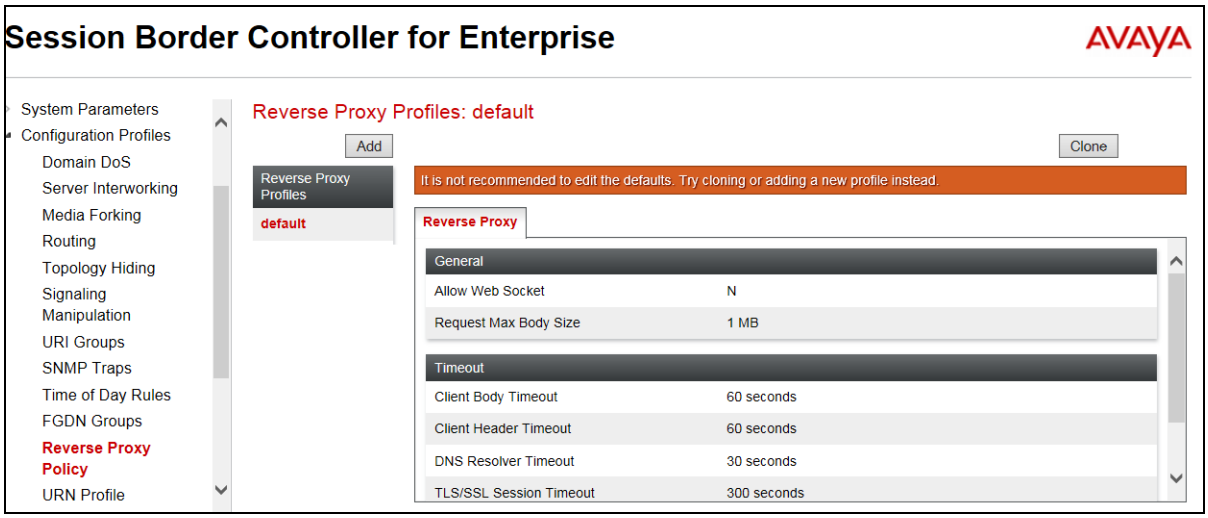
From the top left of the screen, select the SBCE from the **Device** drop-down menu.



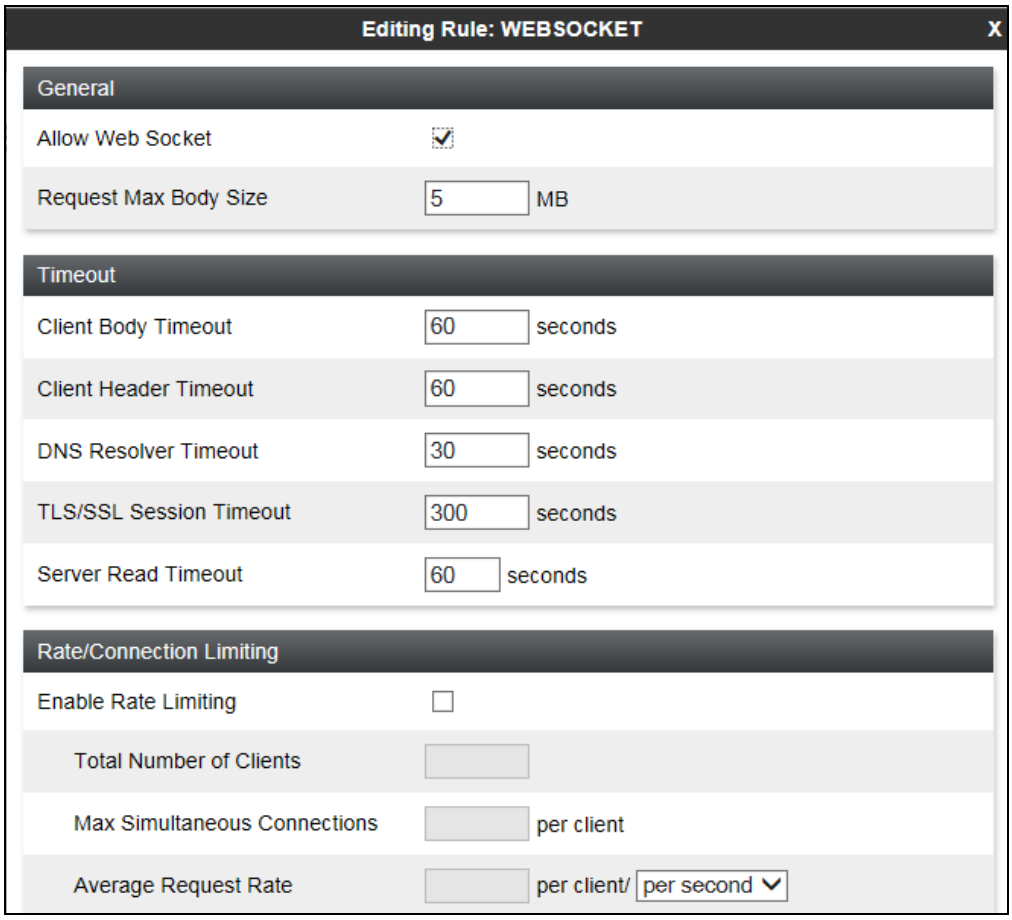
Note the IP address setup for this SBCE as it will be used in Reverse Proxy setup later. Navigate to **Network & Flows** and then **Network Management** in the left window. There are two tabs, **Interfaces** and **Networks**, and both should be noted as they are referenced in the setup later. The Networks tab below shows the **IP address**, **Subnet Mask** and **Gateway** information for each Interface that was enabled. The **Internal A1** interface contains an IP address on the same subnet as Session Manager, Communication Manager and Contact Center. The **External B1** interface contains a public IP address to allow a connection to the outside world. These are the interfaces that will be used later in this section for the setup of the Reverse Proxy services.



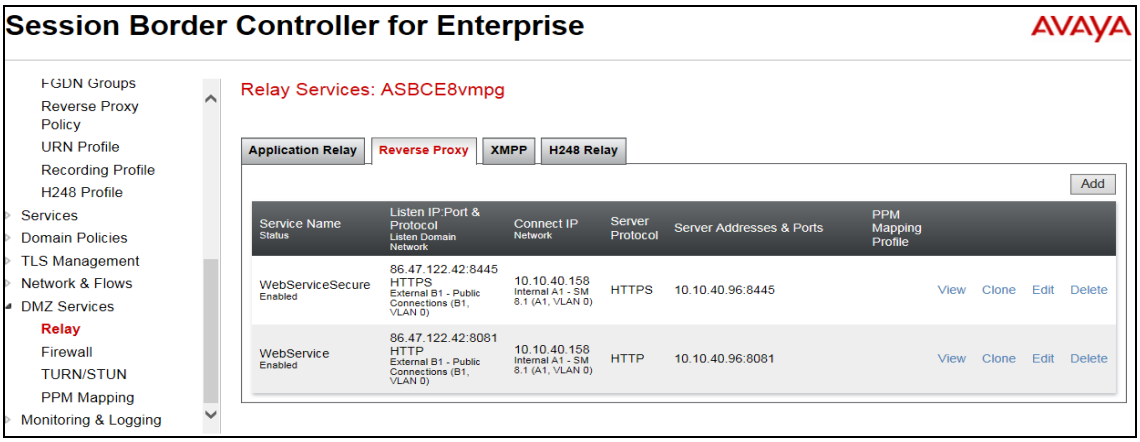
Navigate to **Configuration Profiles → Reverse Proxy Policy** in the left window and add a new Reverse Proxy by either cloning the default one present or clicking **Add**.



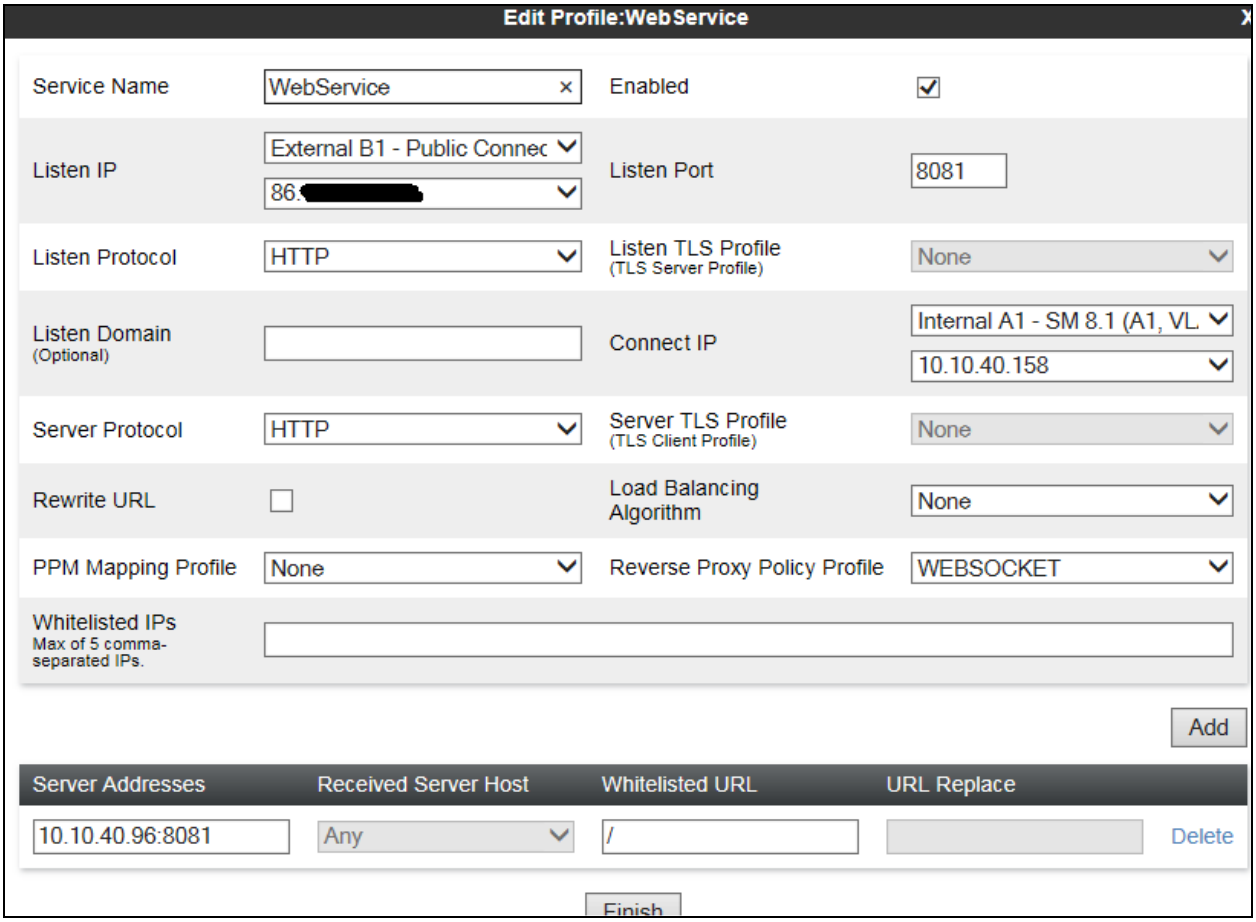
Ensure that **Allow Web Socket** is ticked, and the **Request Max Body Size** was increased to **5MB**.



Navigate to **DMZ Services → Relay** in the left window and select the **Reverse Proxy** tab in the main window. The two existing services are shown below, one for the secure port **8445** and another for the unsecure port **8081**, both were added for compliance testing as both were tested. To setup a new service, click on **Add** to the right of the page.

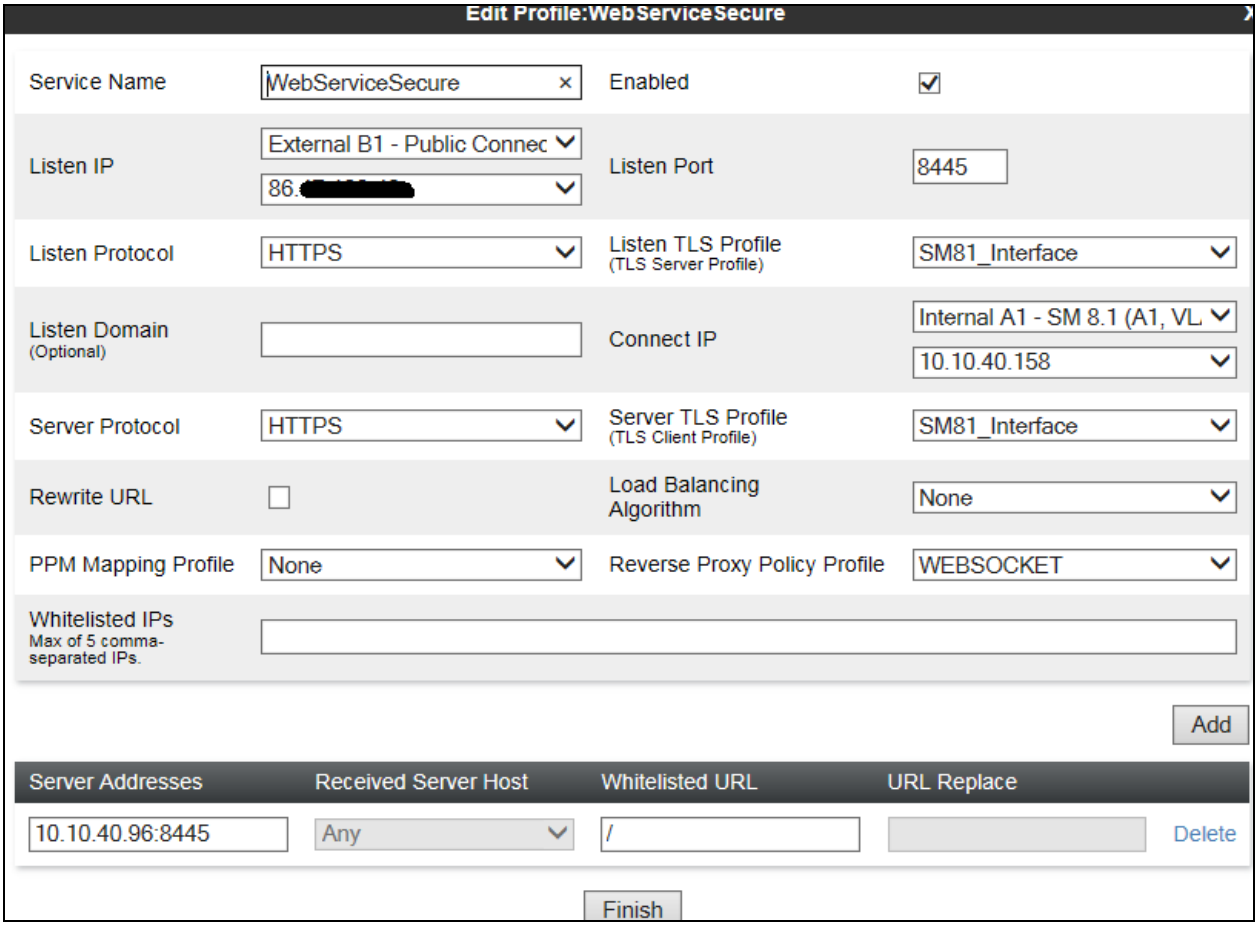


The following setup shows the service added for the unsecure connection over port **8081**. The **Listen IP** will be the external or public IP address and the **Connect IP** will be the inside or Enterprise IP address. The protocol used here is **HTTP** and not https. The **Reverse Proxy Policy Profile** used is that created earlier. The IP address of the Contact Center or CCMM including the correct port is added to the **Server Addresses** at the bottom of the screen and click on **Finish**.



A similar setup is used for the secure connection. Here, port **8445** is used instead of 8081 and **HTTPS** is used instead of http. The same **Listen IP** and **Connect IP** are used for the unsecure connection, however there are some extras needed for a secure connection such as TLS Profiles that allow the exchange of certificates. There is a **Listen TLS Profile** that is used for a certificate exchange between the SBCE and the third party on the public side, and there is a **Server TLS Profile** that is used for a certificate exchange between the SBCE and Session Manager for the enterprise side. The same **Reverse Proxy Policy Profile** is used, and the same Contact Center IP address was added but note the port is now **8445** instead of 8081 that was used on the previous page.

Note: The setup and configuration of the TLS profiles are outside the scope of these Application Notes, however an example of such a setup is included in the **Appendix** as a reference to help explain the setup of such profiles.



7. Configure WEBTEXT Contact Center Messaging (CCM)

All configurations of WEBTEXT Contact Center Messaging are performed by a WEBTEXT engineer and are outside the scope of these Application Notes.

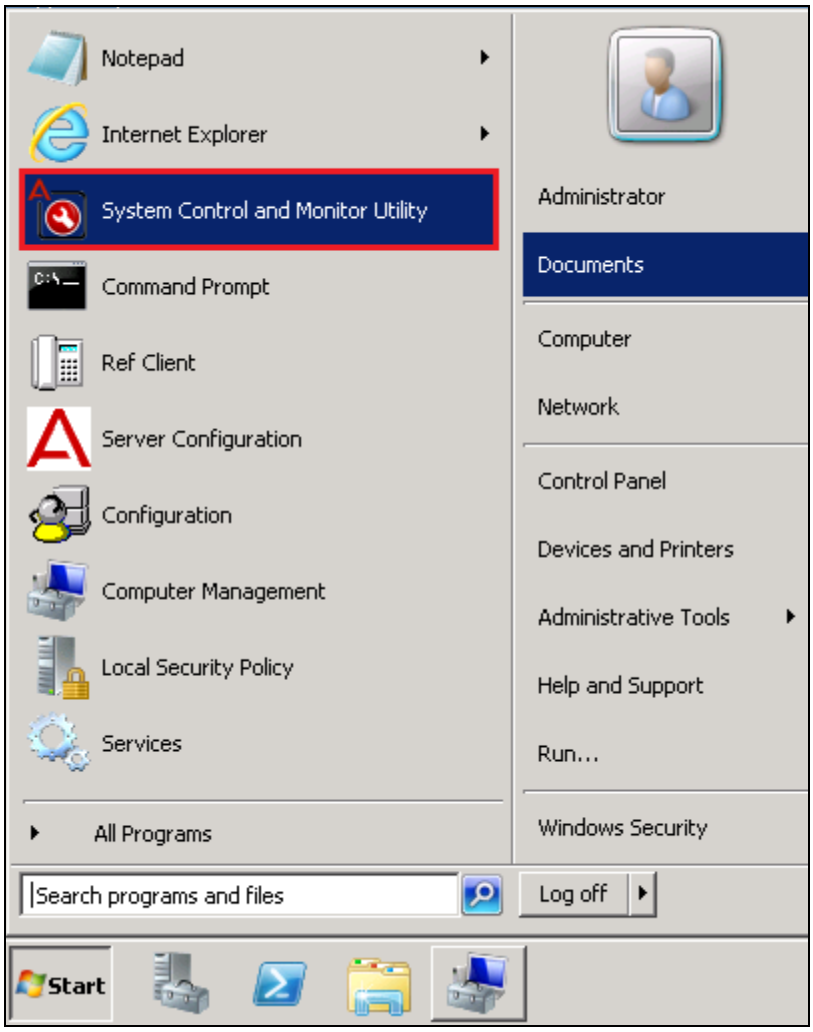
Please note that information such as, the public routable FQDN and port for the EWC service, skillset names and associated numbers, and any certificates required for TLS communication, will need to be shared with WEBTEXT.

8. Verification Steps

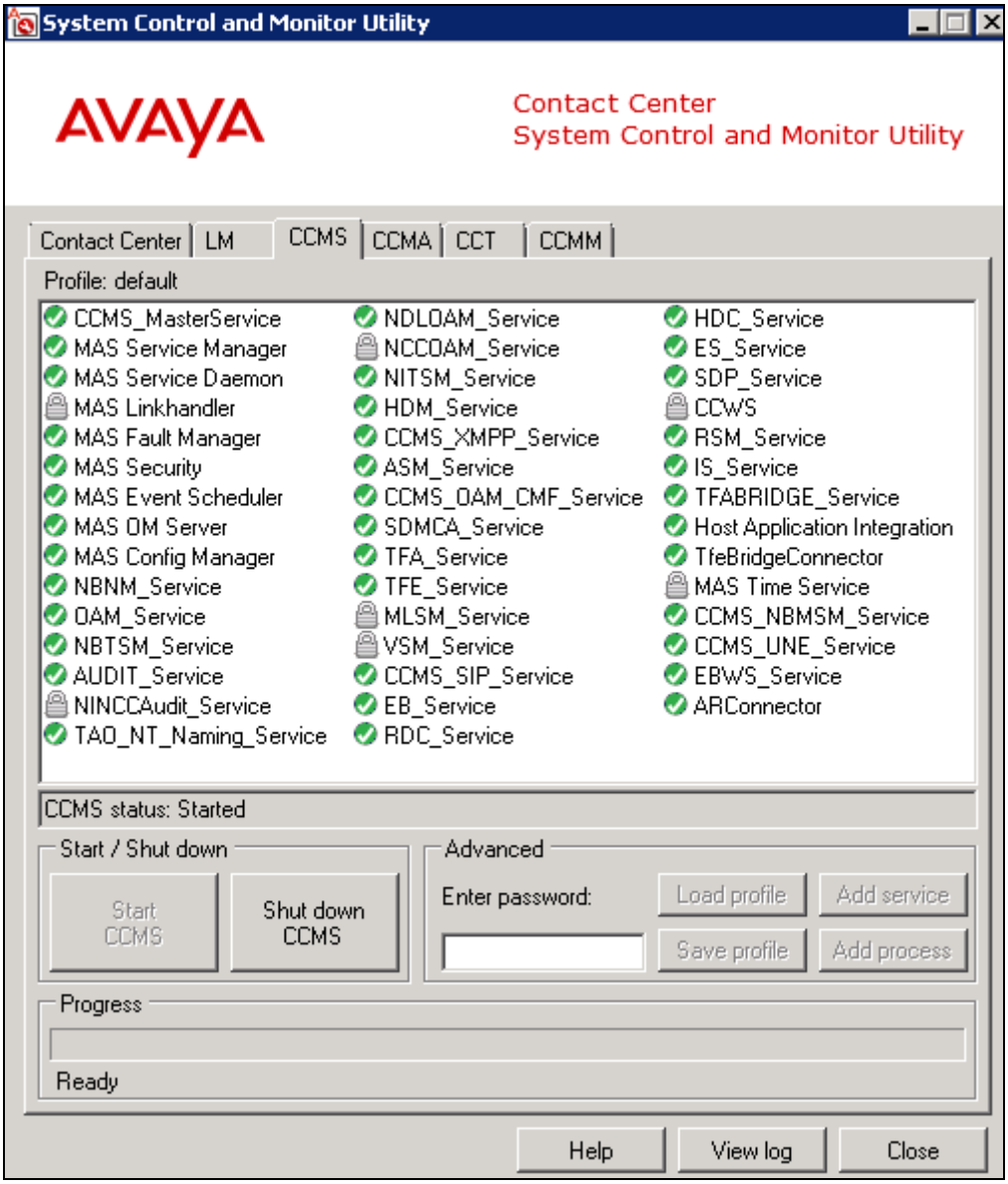
This section provides the tests that can be performed to verify correct configuration of WEBTEXT Contact Center Messaging with Avaya Aura® Contact Center.

8.1. Verify Avaya Aura® Contact Center Services

From the Contact Center Server, open **System Control and Monitor Utility**.



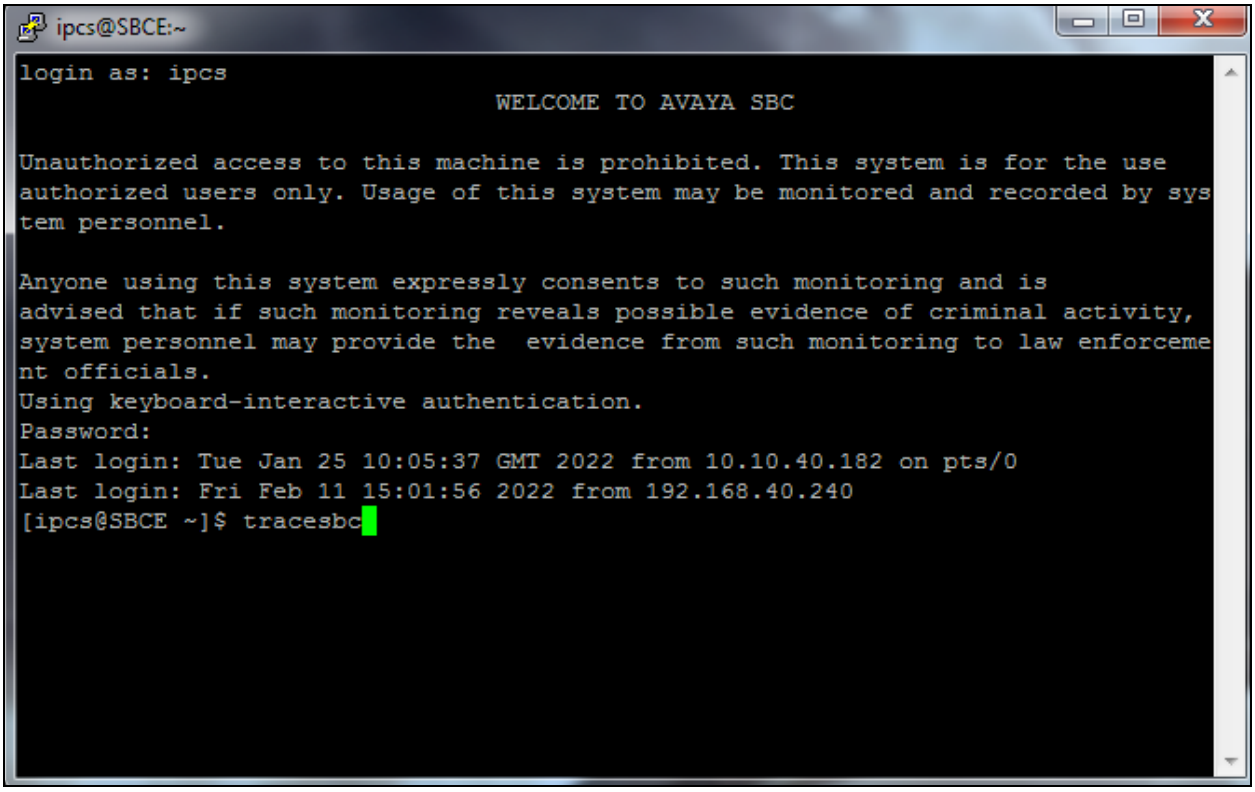
Navigate across each of the tabs, paying special attention to any service that may not be running. The **CCMS** services are all showing green below which indicates that the Contact Center Manager Server is fully operational. Check this the case for all services on all tabs.



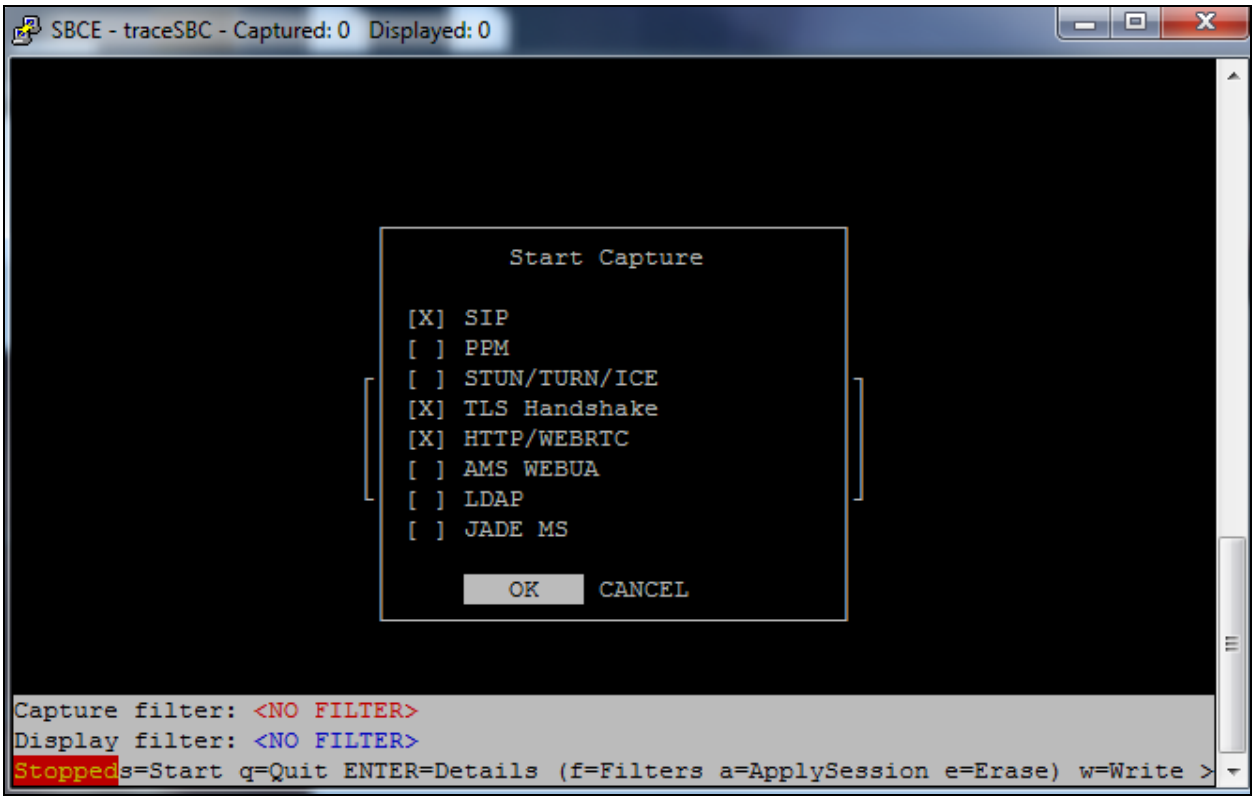
8.2. Verify Connection between Contact Center Messaging and Enterprise Web Chat

The “tracesbc” facility on the Session Border Controller for Enterprise shows all connections that pass through the SBCE including the Reverse Proxy connections. Before an SMS is sent to the number associated with the SMS service to the Agent Desktop, open the tracesbc and once the SMS is sent the messaging on the SBCE can be observed and scrutinized.

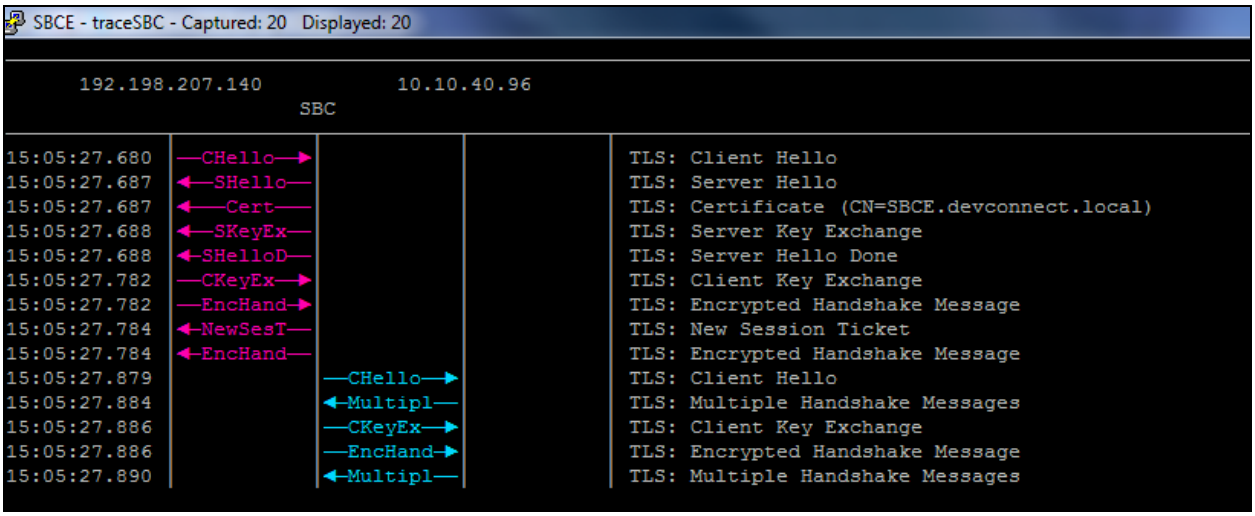
Open an SSH session to the SBCE via PuTTY or some other suitable application and type in tracesbc as shown below. The following trace shows an example of such messaging.



Once the trace window opens, the amount of information to capture can be selected. **HTTP/WEBRTC** as well as **SIP** and **TLS Handshake** are chosen.

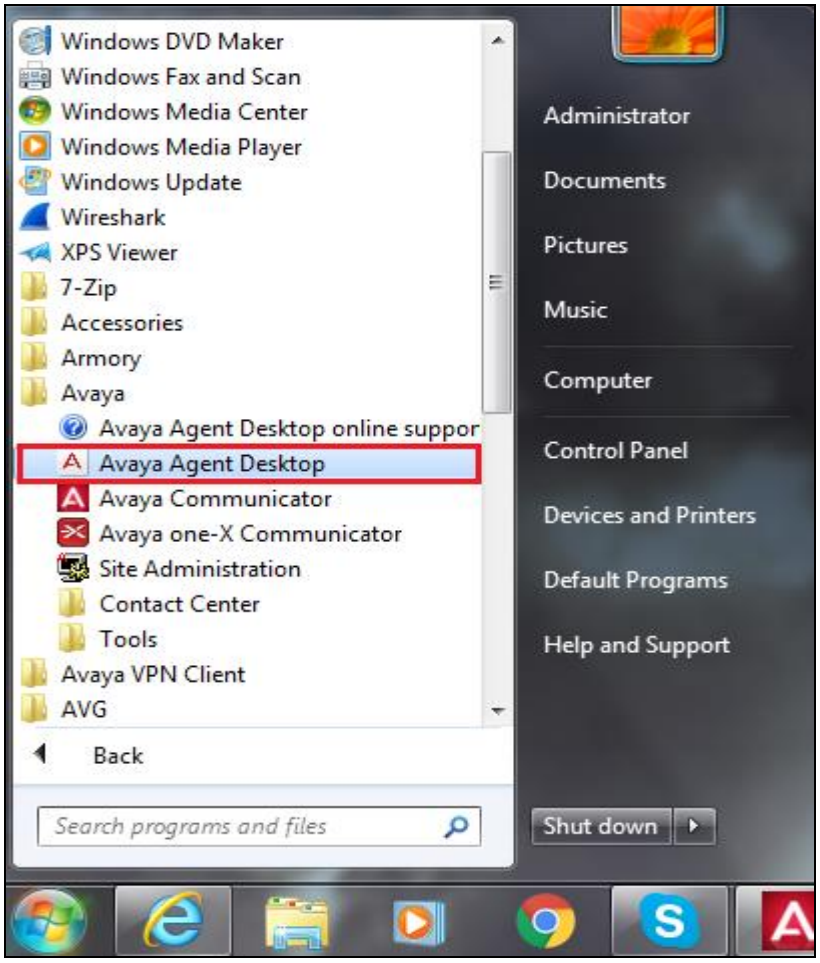


The exchange below shows the certificate exchange between WEBTEXT and AACC was successful.

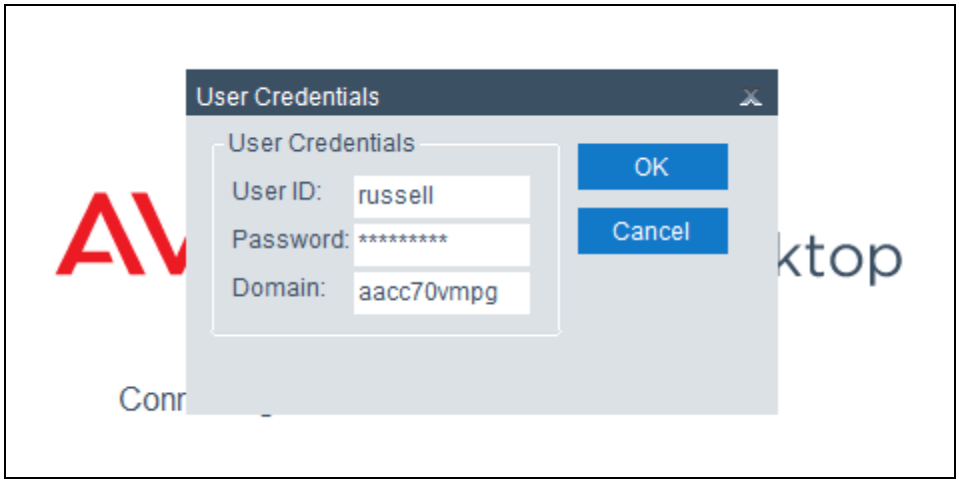


8.3. Verify SMS Sent/Received on Avaya Agent Desktop

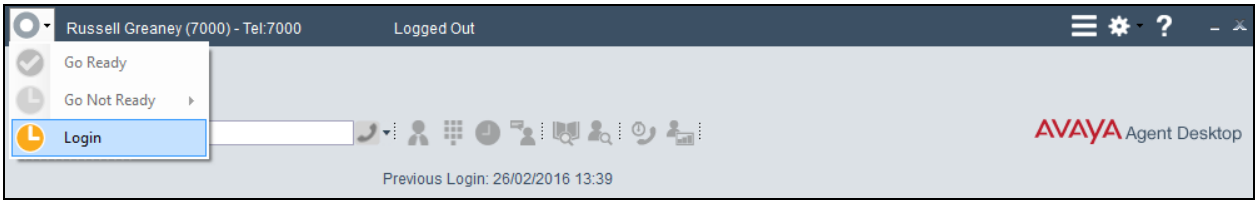
From a client PC where AAAD is installed, open **Avaya Agent Desktop**.



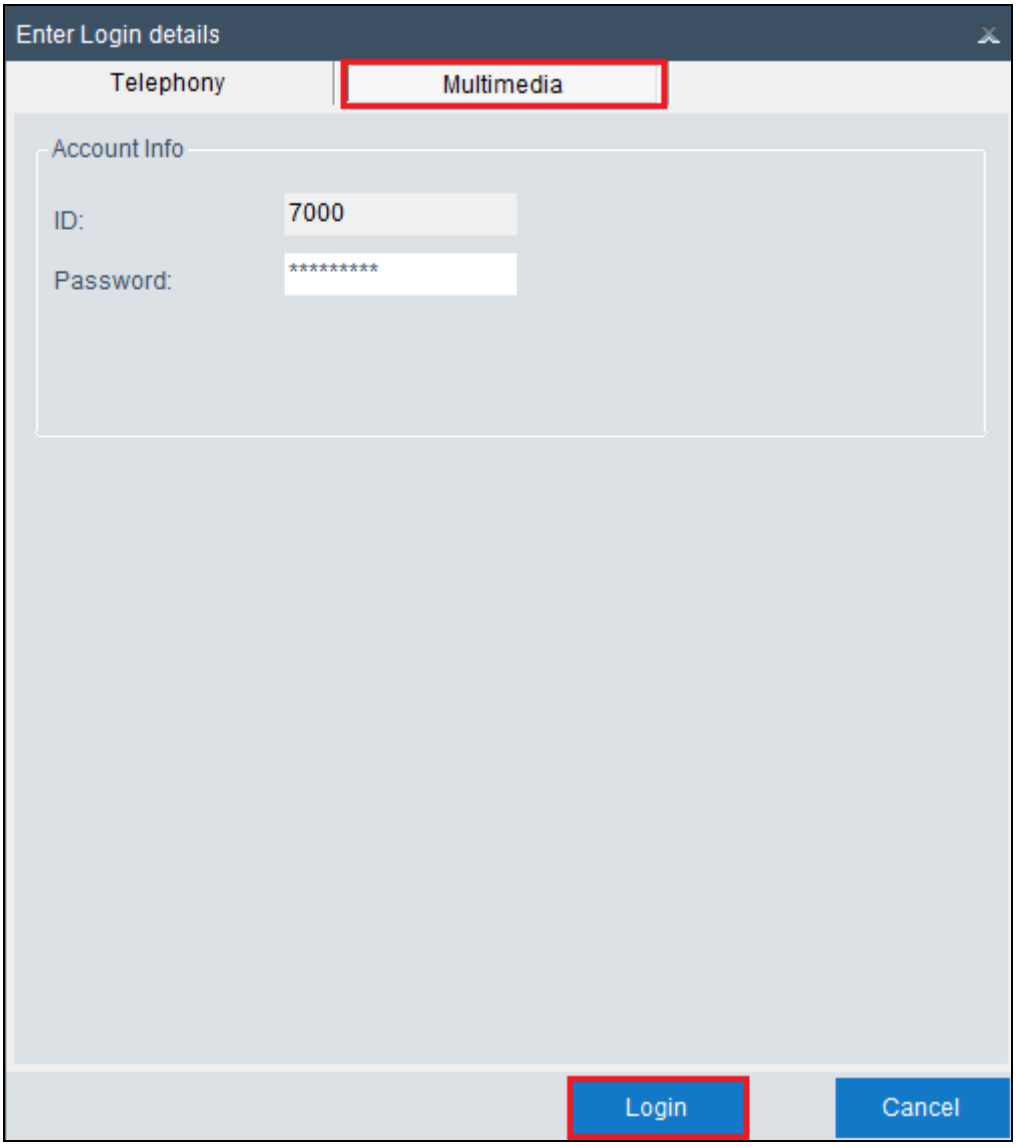
Enter the appropriate credentials and click on **OK**.



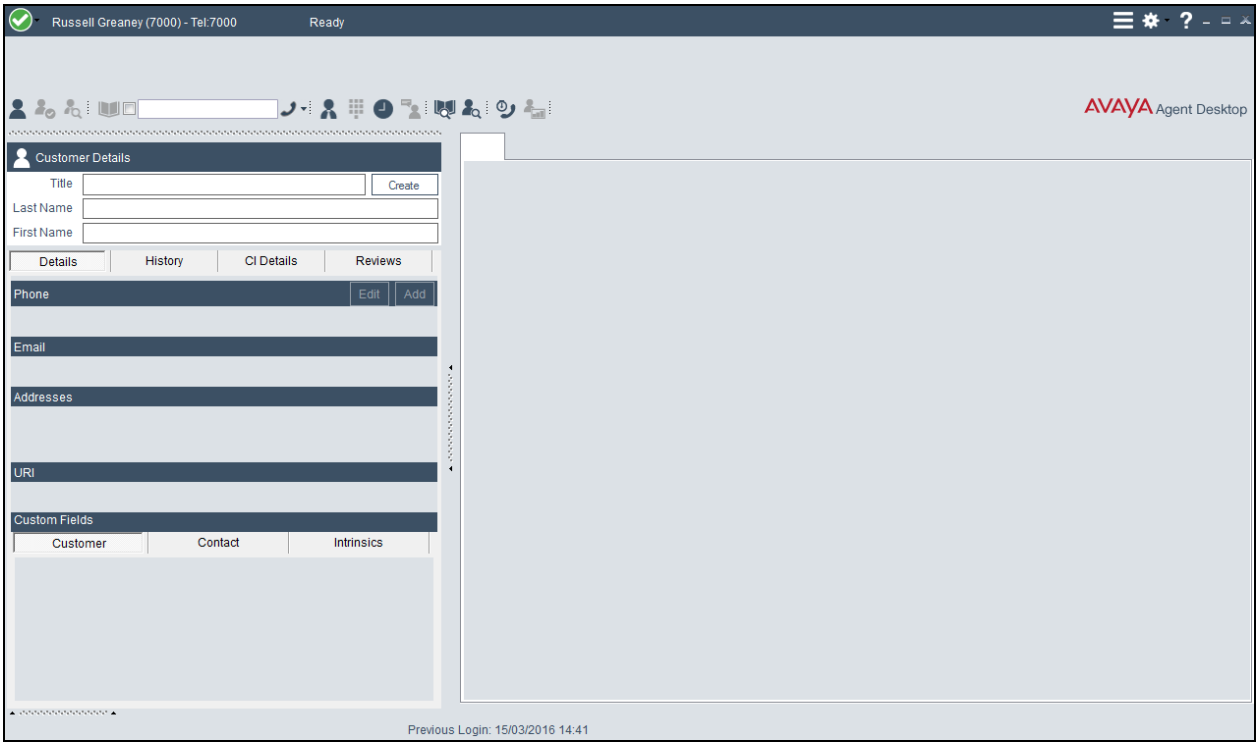
Once the Desktop opens click on **Login** as shown below.



Log into Contact Center Multimedia, under the **Multimedia** tab, and click on **Login**.

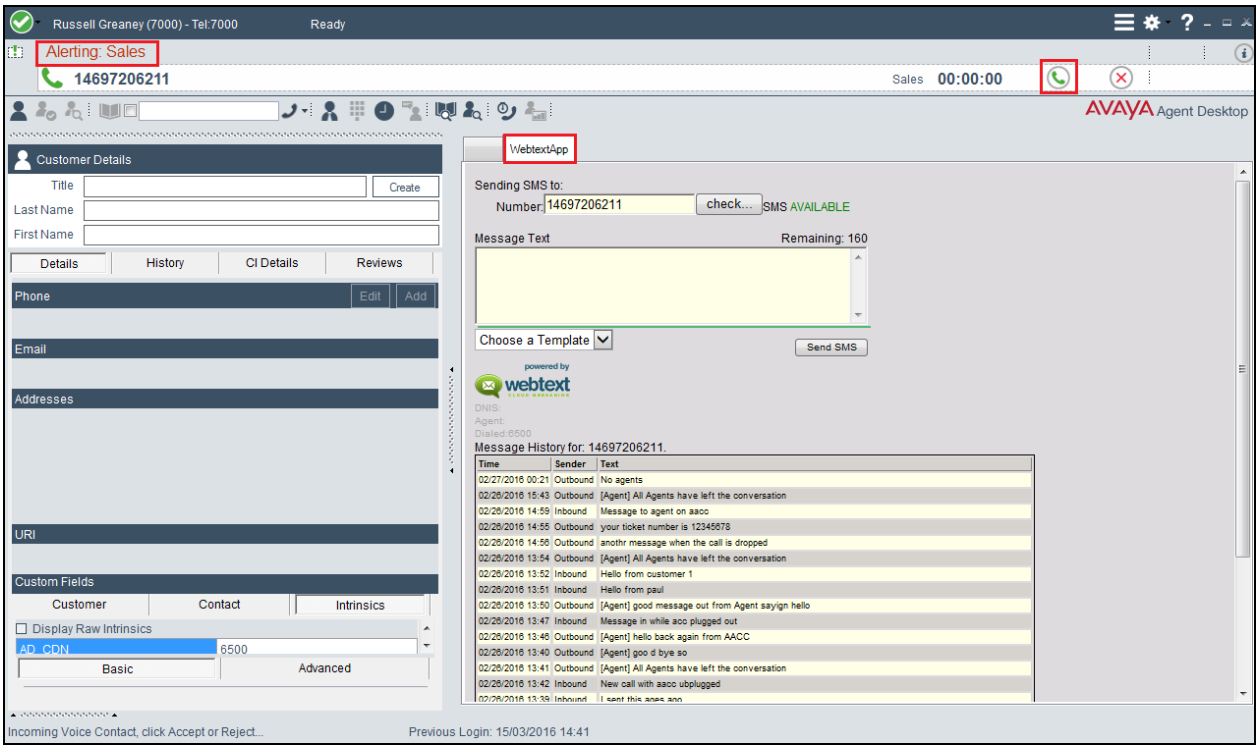


The following screen appears showing the agent logged in and **Ready**.

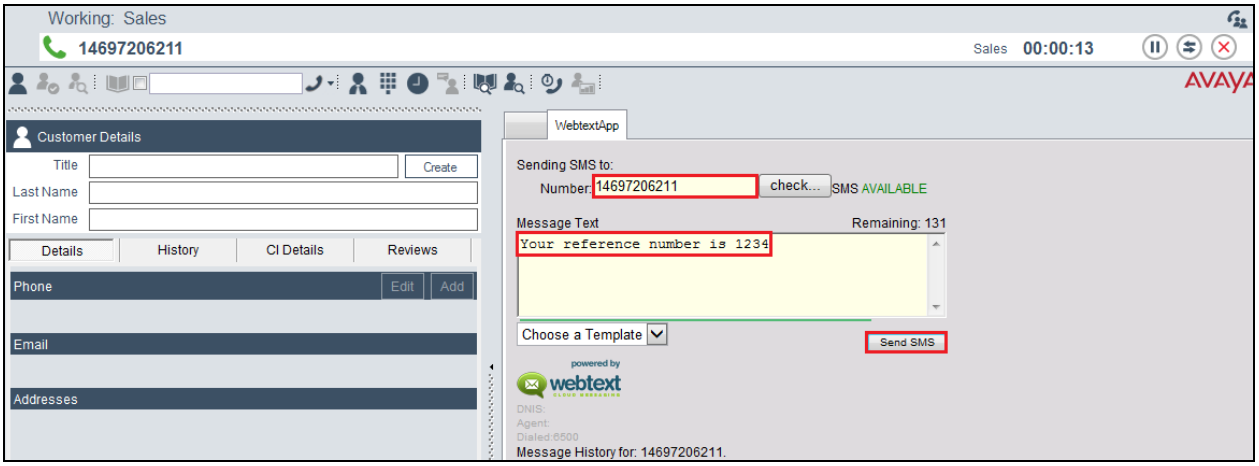


8.3.1. Verify the Ability to Include an SMS Message to the Customer while on a Call to that Same Customer

A voice call is made to the **Sales** CDN in order to present a call to the Contact Center agent. When the call is presented to the agent's desktop display the screen will display **Alerting** as shown below and because this screen pop is setup to trigger on alerting the **WEBTEXTApp** screen pop is displayed. The agent answers the call by pressing the answer icon highlighted.

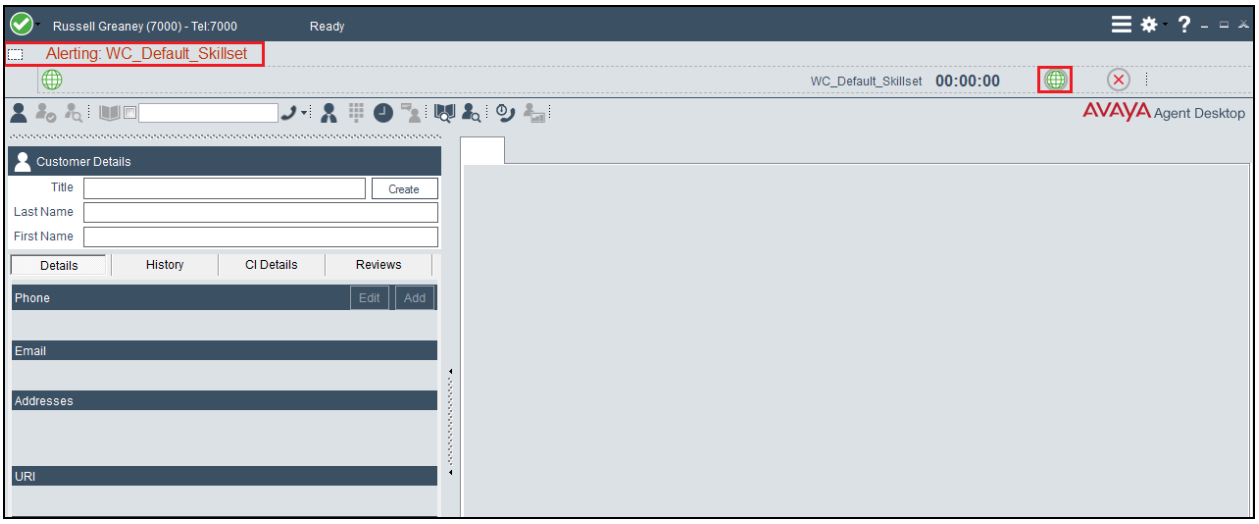


The **Number** is automatically populated with the CLID of the caller and the agent can simply enter the SMS message that needs to be sent and the **Send SMS** button is pressed. This will send a text message to the phone number highlighted below.

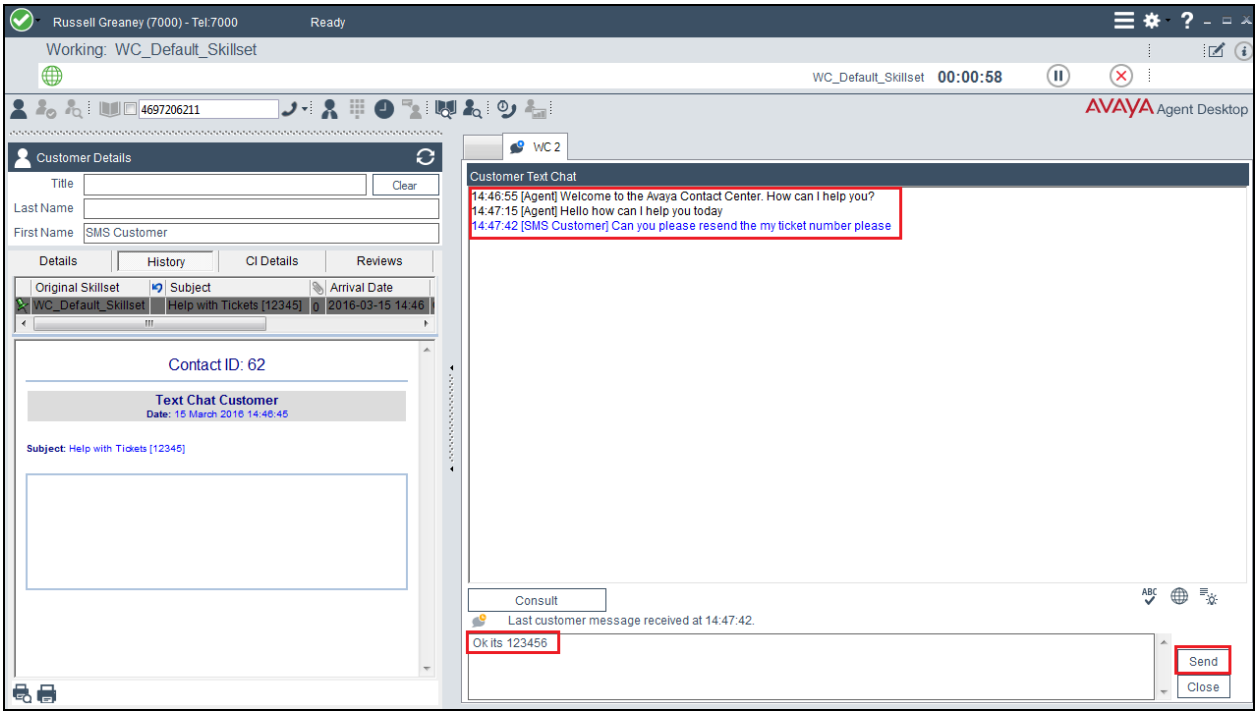


8.4. Verify the Ability of the Customer to Initiate an SMS Chat Session with a Contact Center Agent

A customer creates a new text/SMS message and sends this to the Contact Center SMS number. This will then be routed to the Web Chat skillset as shown below. The agent then answers the call by pressing on the answer icon highlighted at the top right of the screen.



Once the call is answered the agent can send and receive SMS messages using the web chat window as shown below.



9. Conclusion

These Application Notes describe the configuration steps required to integrate WEBTEXT Contact Center Messaging (CCM) with Avaya Aura® Contact Center R7.1 and Avaya Aura® Communication Manager R7.1 in order to pass SMS messages from the customer to the Avaya Agent Desktop and from the agent to the customer. All test cases have passed with any issues and observations noted in **Section 2.2**.

10. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from *http://support.avaya.com* or from your Avaya representative.

[1] *Avaya Aura® Contact Center & Avaya Contact Center Select Enterprise Web Chat* Release 7.1 Issue 5.0 August 2019

[2] *Avaya Aura ® Contact Centre SIP Commissioning, Doc # NN44400-511, Release 7.1*

[3] *Avaya Aura® Contact Center Installation Release 7.1, NN44400-311, 05.02, Release 7.1*

[4] *Avaya Aura® Contact Center Commissioning Release 7.1, NN44400-312, 05.01, Release 7.1*

[5] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509

[6] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205

[7] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 8.1

Technical documentation for WEBTEXT Contact Center Messaging can be obtained as follows:
www.webtext.com
U.S. +1 (855)247 3232
Europe +353 1 2479000(IRL) +44 203 3285053(UK).

11. TLS Certificates Management

In the reference configuration, the Avaya SBCE uses TLS transport to securely communicate with Session Manager on the enterprise network, and with WEBTEXT Contact Center Messaging on the public network.

For TLS protocol usage, Avaya recommends using unique digital identity certificates, signed by a trusted Certificate Authority (CA). This section describes the procedures to install and configure TLS certificates on the Avaya SBCE public and private interfaces, using the Avaya System Manager built-in Certificate Authority to generate the identity certificates.

The following tasks are performed:

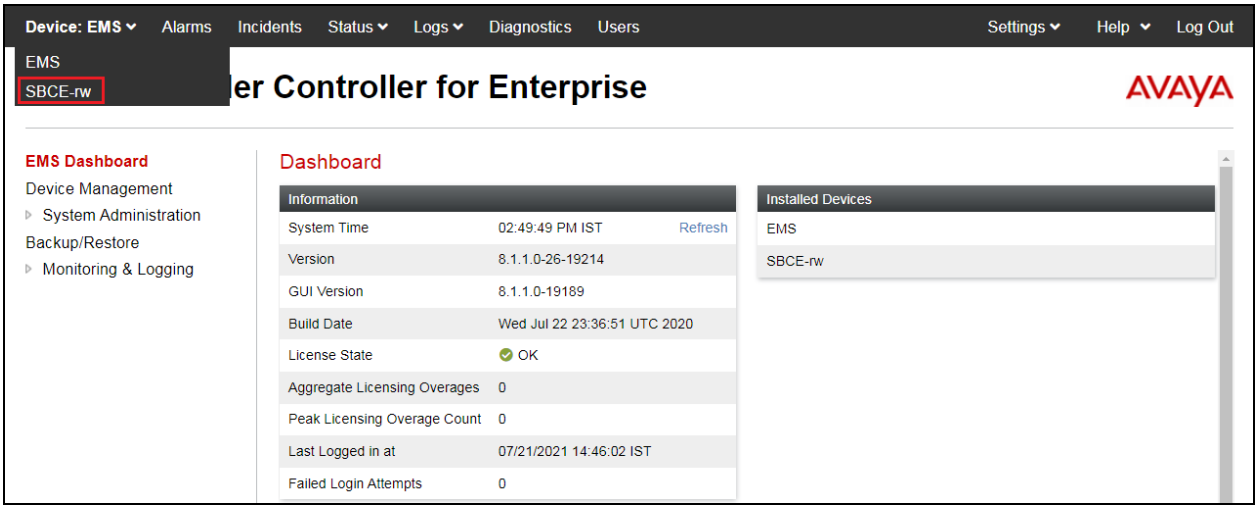
- Network Management
- Create Certificate Signing Requests in Avaya SBCE
- Install Identity Certificates issued by the System Manager CA in Avaya SBCE
- Install System Manager CA root certificate in Avaya SBCE
- Create TLS Client Profiles in Avaya SBCE
- Create TLS Server Profiles in Avaya SBCE

11.1. Network Management

Use a Web browser to access the Element Management Server (EMS) web interface and enter https://*ipaddress*/sbc in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE.

Log in using the appropriate credentials.

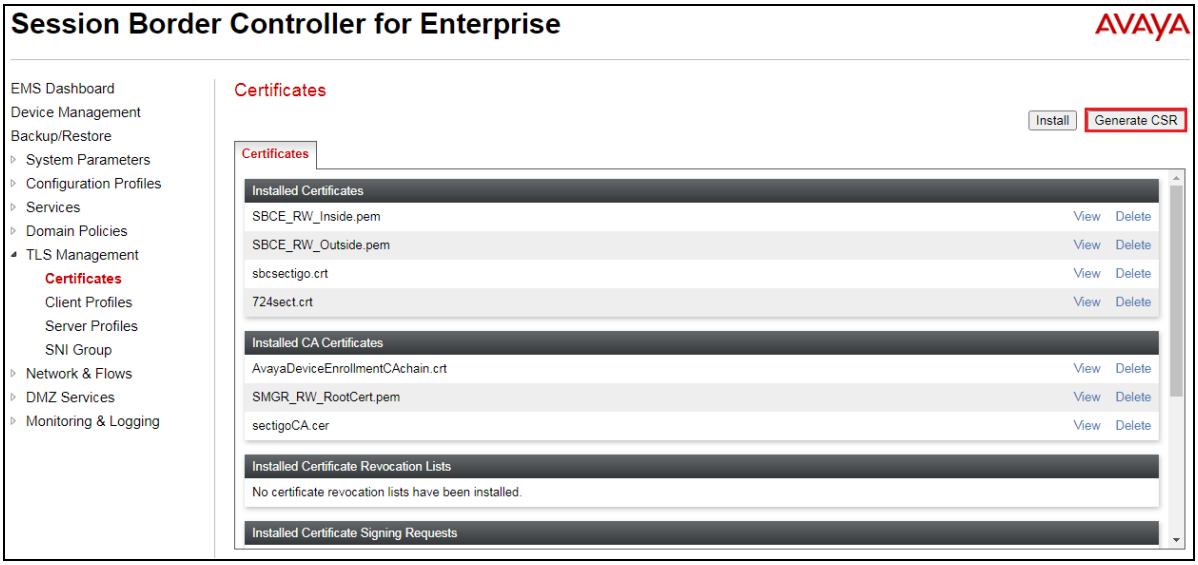
Once logged in, the following screen is presented, and the device must be set to the SBCE before any further configuration can take place.



11.2. Create Certificate Signing Requests for Avaya SBCE interfaces

Follow the steps in this section to create Certificates Signing Requests (CSR) for the Avaya SBCE external interface. This CSR will later be signed by the Avaya System Manager Certificate Authority.

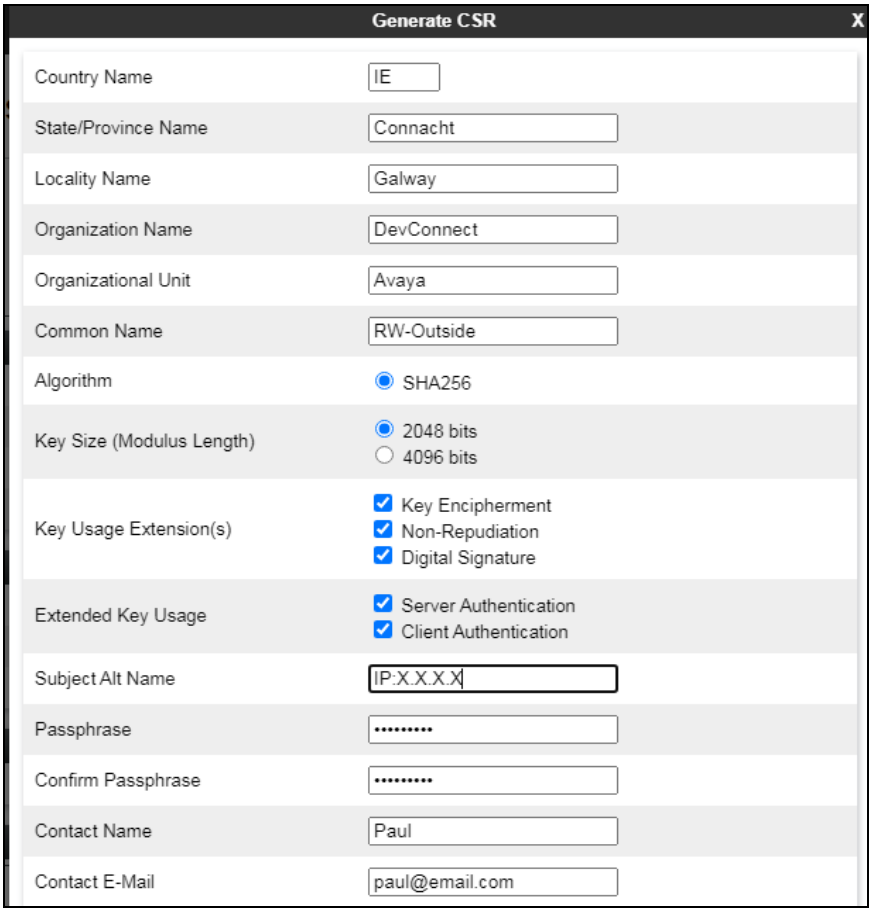
Navigate to **TLS Management → Certificates** and click the **Generate CSR** button. The screen below shows all the certificates that were configured and installed as part of the compliance testing. This section will run through the procedure to create a new CSR and install the resulting Identity Certificate as well as the Root Certificate.



On the **Generate CSR** form that appears, fill the information as required:

- Enter the information on the location and organization fields as appropriate.
- Under **Common Name**, enter a descriptive name, e.g., **RW-Outside**.
- **Algorithm**: **SHA256**.
- **Key Size**: **2048 bits**.
- **Key Usage Extension(s)** and **Extended Key Usage**: check all options.
- **Subject Alt Name**: using format **IP:<value>**, enter the IP addresses of the external interface of the Avaya SBCE used by Remote Workers for HTTPS and for SIP traffic.
- **Passphrase**: Enter a password, used to encrypt the private key.
- **Contact Name** and **Contact Email**: Enter information as appropriate.

The following screen illustrate the parameters used in the sample configuration. Click **Generate CSR**.



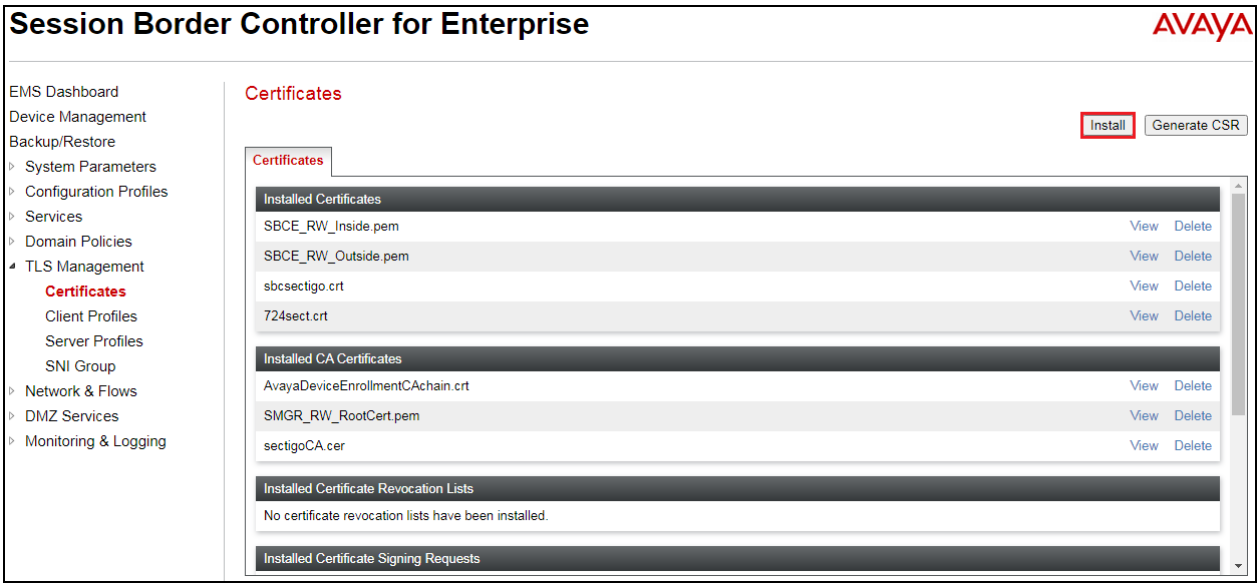
After clicking **Generate CSR**, a pop-up window showing the details of the CSR will appear (not shown). Click on **Download** to extract the CSR file from the Avaya SBCE. Save the generated CSR file, e.g., **SBCE_RW_Outside.req**, to the local PC. This will be used to generate the ID Certificate.

11.3. Install Identity Certificate on Avaya SBCE

Follow the steps in this section to install the identity certificate on the Avaya SBCE.

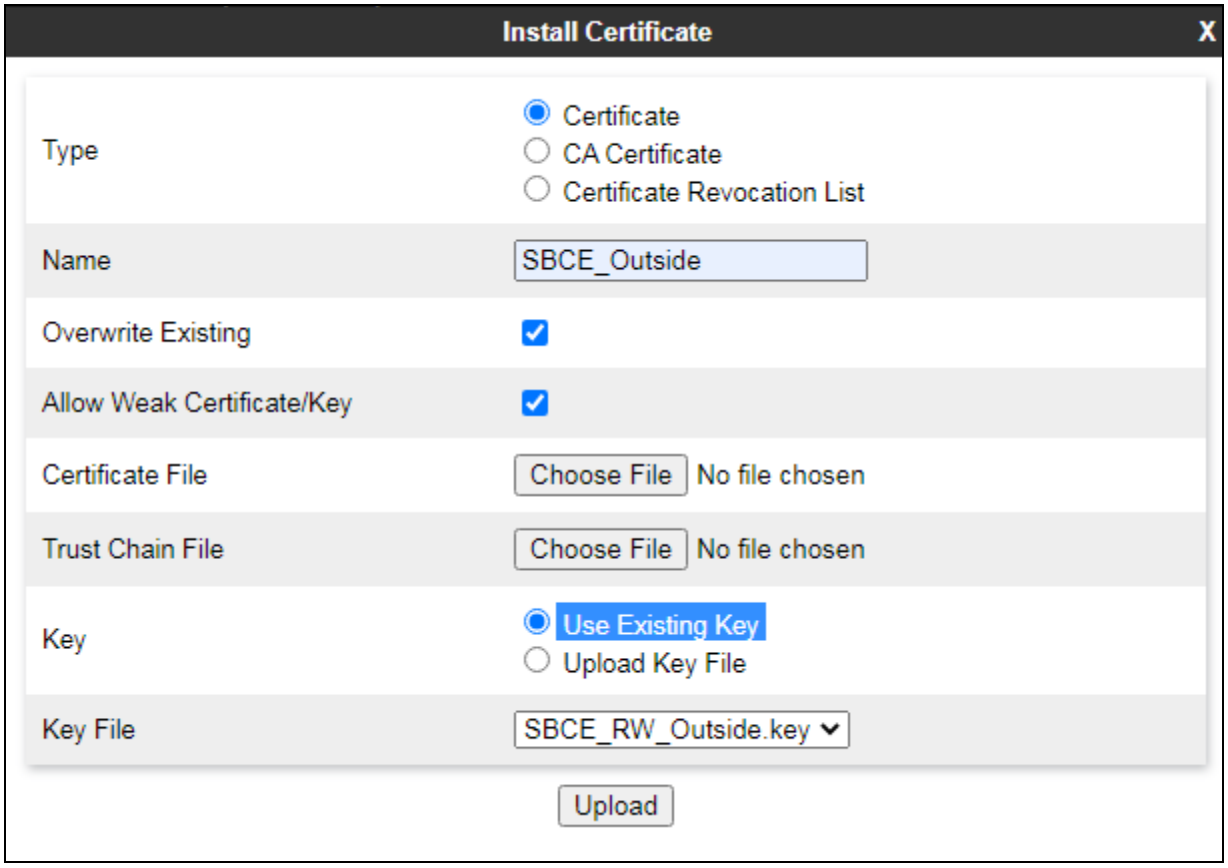
Note: The steps used to create the identity certificates are outside the scope of these Application Notes. System Manager was the CA used to create the identity certs for the profiles.

On the Avaya SBCE web interface, navigate to **TLS Management → Certificates** and click the **Install** button. The screen below shows all the certificates that were present for compliance testing.



In the **Install Certificate** screen, select the following:

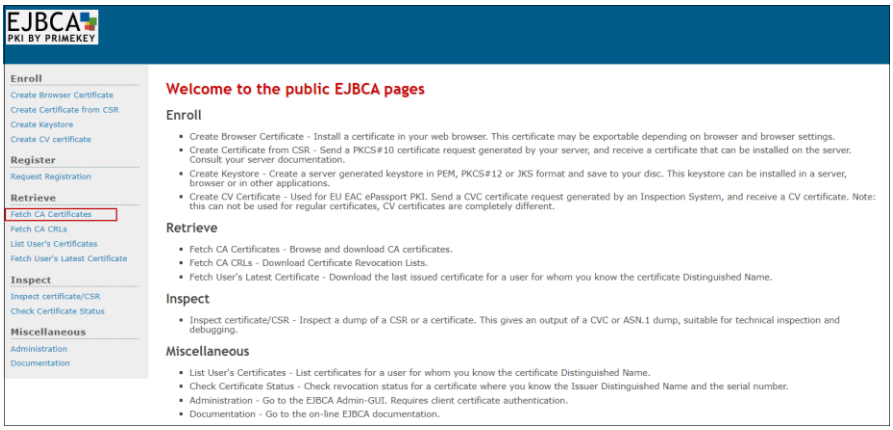
- **Type**: **Certificate**.
- **Name**: enter a descriptive name, e.g., **SBCE_Outside**.
- Check the boxes for **Overwrite Existing** and **Allow Weak Certificate/Key**.
- **Certificate File**: click **Browse** to select the identity certificate file previously saved on the local PC.
- **Key**: Select **Use Existing Key**, to use one of the key files automatically generated during the CSR creation.
- **Key File**: Select **SBCE_RW_Outside.key** from the drop-down menu.
- Click **Upload**.
- Click **Install** (not shown).



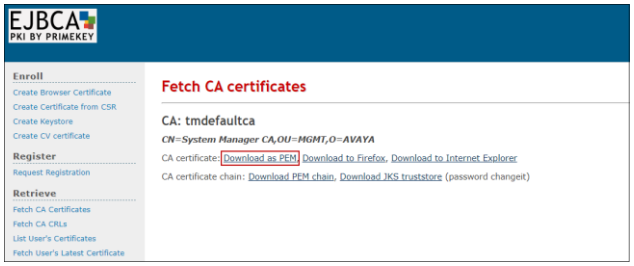
Note: The installation of the "Inside" identity certificate follows the same procedure, but uses the key generated for the inside cert instead.

11.4. Install System Manager CA Root Certificate

From the System Manager **Home** page, navigate to **Services → Security → Certificates → Authority**. Select **Public Web** (not shown). Select **Fetch CA Certificates**.



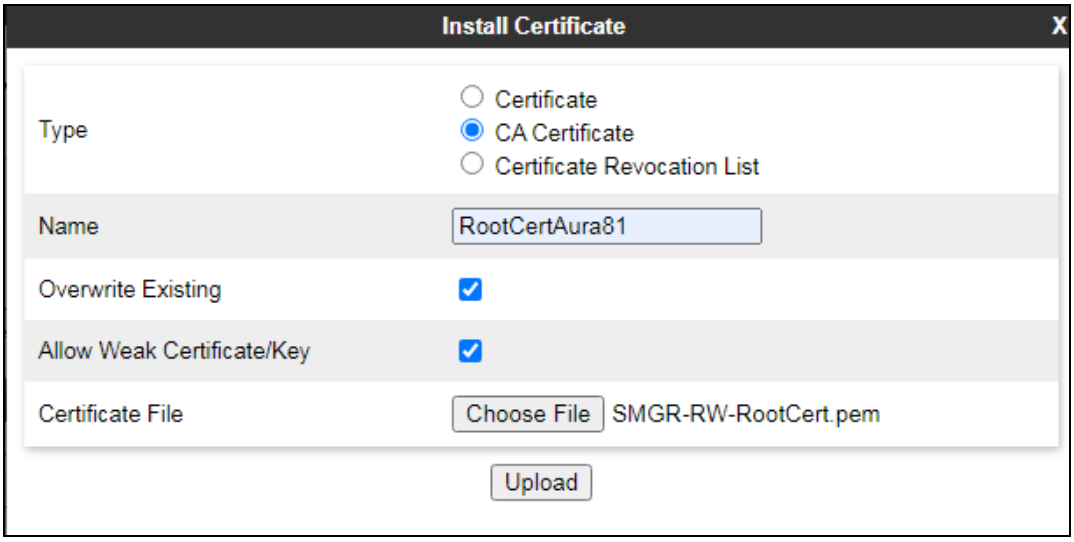
Click **Download as PEM**.



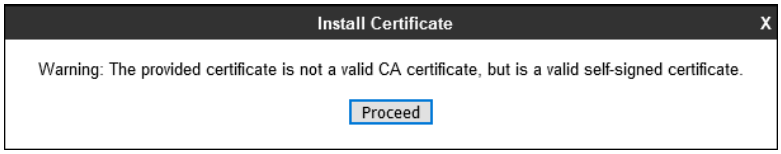
Save the .pem file to the local PC, e.g., **SystemManagerCA.pem** in the reference configuration.

On the Avaya SBCE web interface, navigate to **TLS Management → Certificates** and click the **Install** button (not shown). In the **Install Certificate** screen select the following:

- **Type**: **CA Certificate**.
- **Name**: enter a descriptive name, e.g., **RootCertAura81**.
- Check the boxes for **Overwrite Existing** and **Allow Weak Certificate/Key**.
- Click **Browse** to select the System Manager CA certificate previously downloaded, in this case **SMGR-RW-RootCert.pem**.
- Click **Upload**.



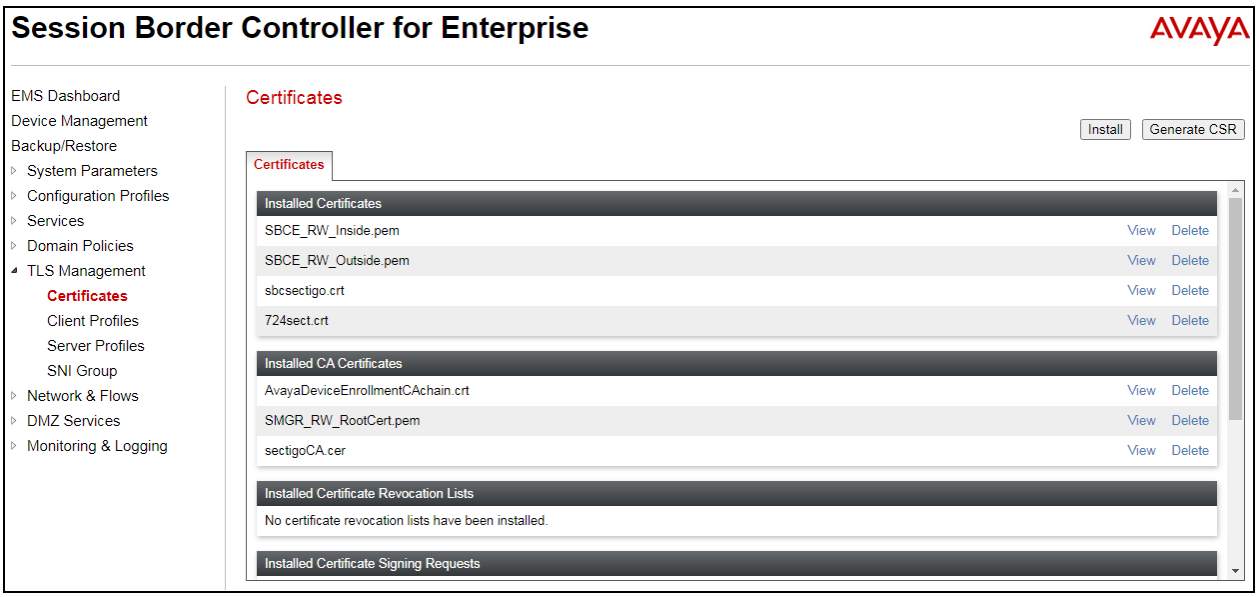
Select **Proceed** on the next screen.



Select **Install**.

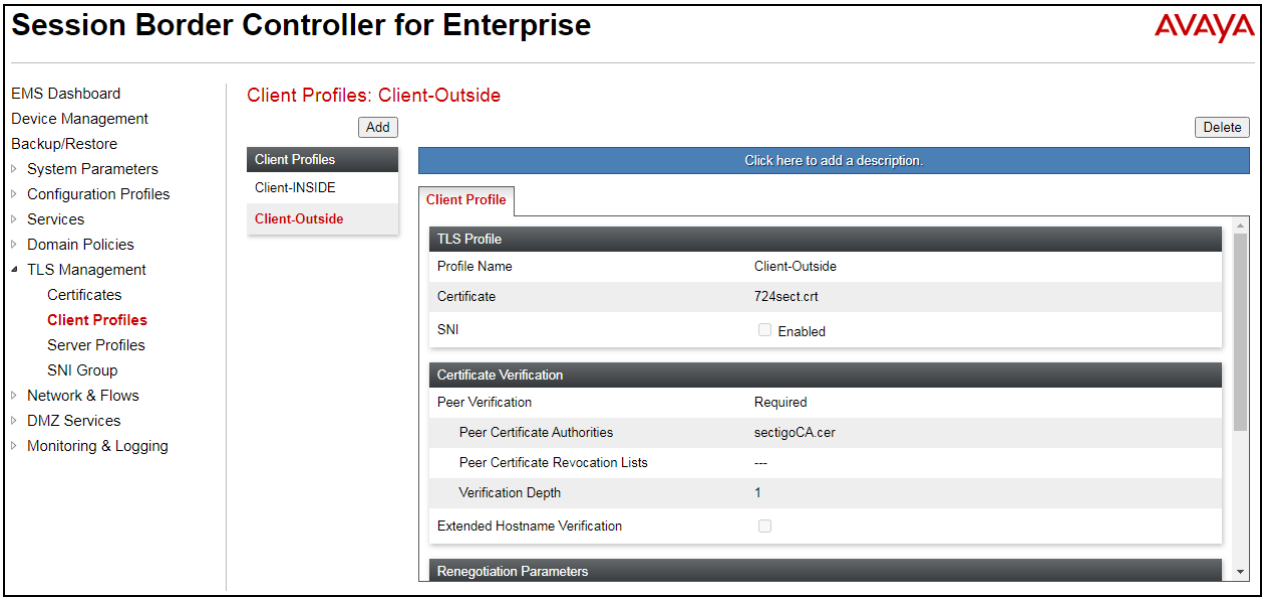
On the Avaya SBCE web interface, select **TLS Management → Certificates** from the left-hand menu. Verify the following:

- System Manager CA signed identity certificates are present in the **Installed Certificates** area.
- System Manager CA certificate is present in the **Installed CA Certificates** area.



11.5. Configure Avaya SBCE TLS Client Profiles

The screen below shows two Client Profiles. To add a new certificate, select TLS Management → Client Profiles from the left-hand menu to add the Avaya SBCE TLS Client Profiles. Click Add (shown above).



At the **Client Profiles** screen, select **Add** and enter the following:

- **Profile Name:** enter descriptive name, e.g., **Client-INSIDE**.
- **Certificate:** select the identity certificate, e.g., **SBCE_RW_Inside.pem**.
- **Peer Verification** is set to **Required** by default. Under **Peer Certificate Authorities** select the CA certificate installed previously, e.g., **SMGR_RW_RootCert.pem**. Set **Verification Depth** to **1**.
- Click **Next**.

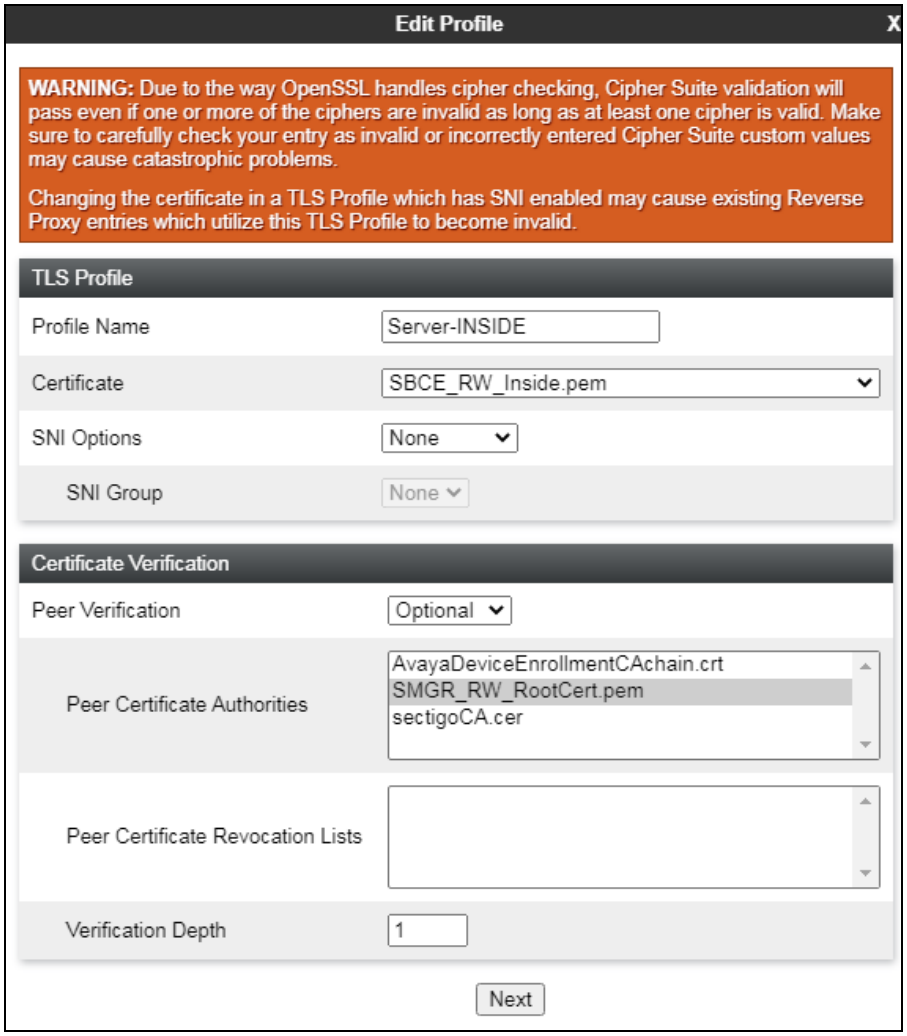
Accept default values for the next screen and click **Finish** (not shown).

11.6. Configure Avaya SBCE TLS Server Profiles

The screen below shows the two Server To add a new identity cert, select TLS Management → Server Profiles from the left-hand menu and click Add.

At the **Server Profiles** screen, select **Add** one more time and enter the following:

- **Profile Name:** enter descriptive name, e.g., **Server-INSIDE**.
- **Certificate:** select the identity certificate, e.g., **SBCE_RW_Inside.pem**, from the menu.
- **Peer Verification**: **Optional**.
- **Peer Verification Authorities**: Select the System Manager root certificate installed earlier, in this instance **SMGR_RW_RootCert.pem**.
- Click **Next**.



Accept default values for the next screen and click **Finish** (not shown).

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 DevConnect Program at devconnect@avaya.com.