



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 messages 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.

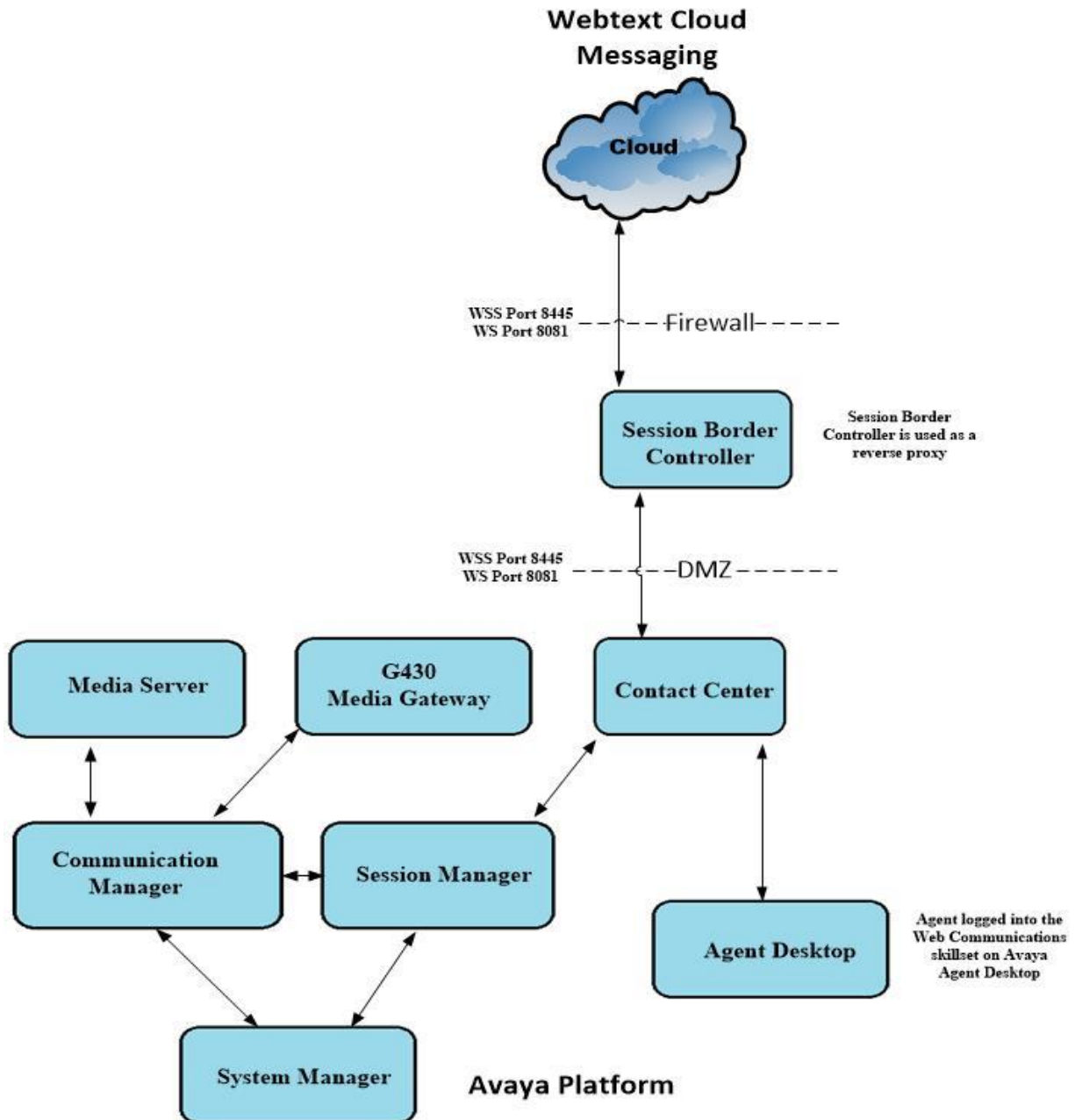


Figure 1: Connection of WEBTEXT Cloud Messaging with Avaya Aura® Contact Center R7.1

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

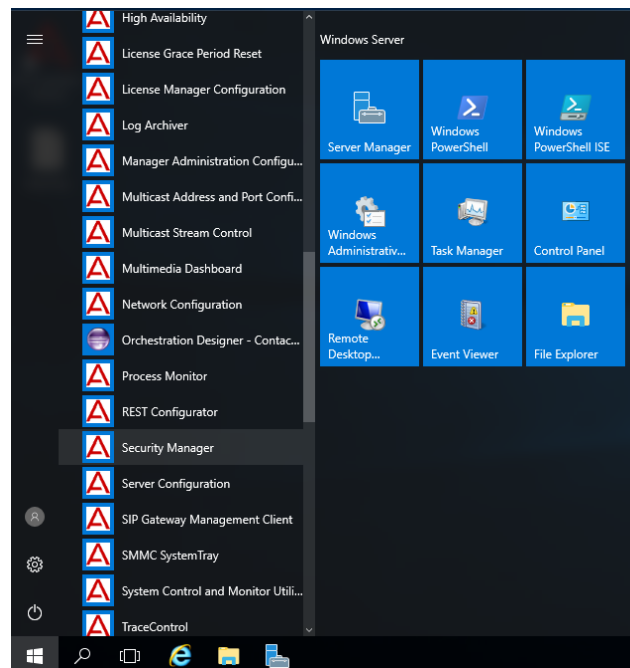
It is assumed that a fully working contact center is already in place with call routing and skillsets configured. The configuration of Contact Center for this solution focuses on the following:

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

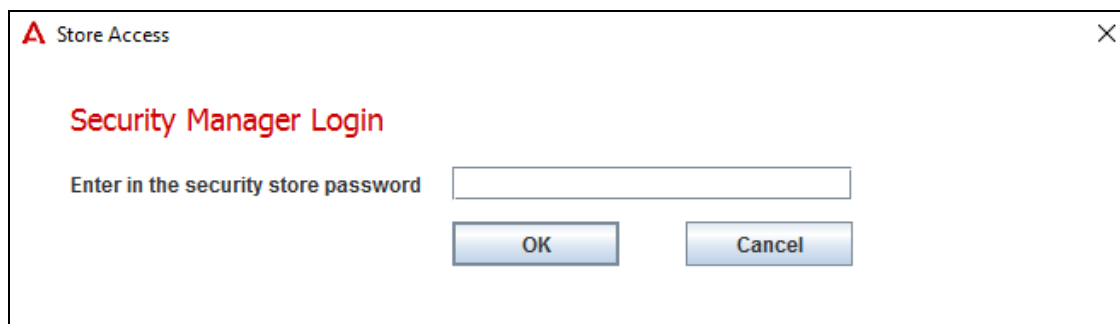
5.1. Configure Secure and Unsecure Web Services

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.

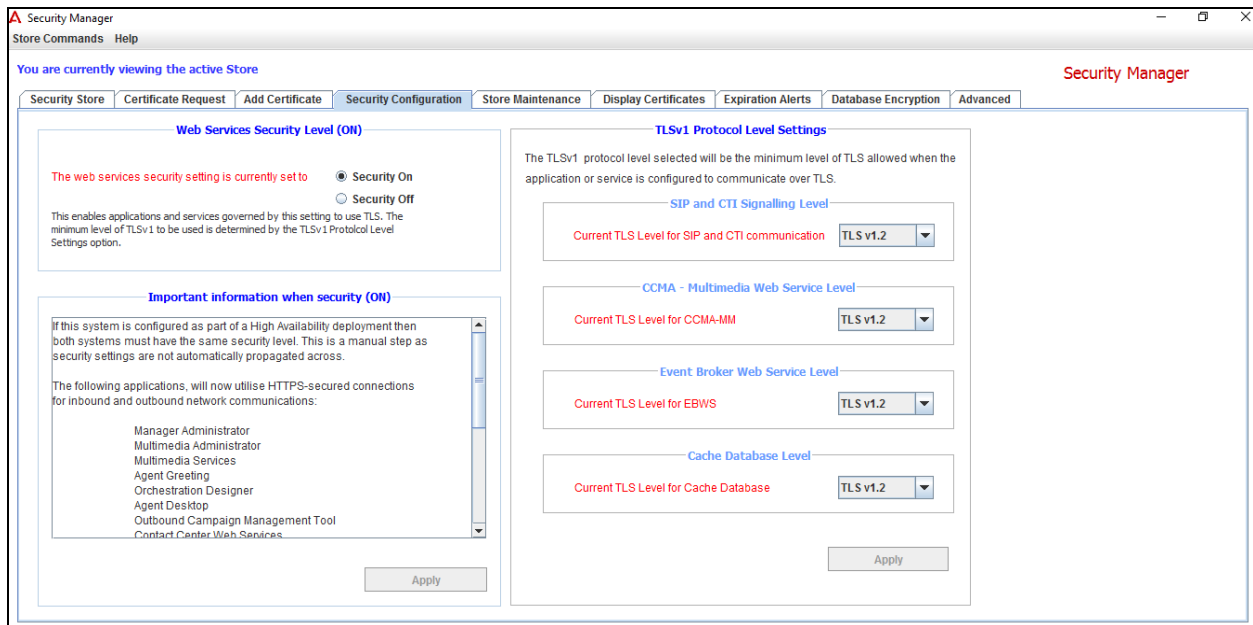
Log into AACC **Security Manager** from the AACC server as shown below.



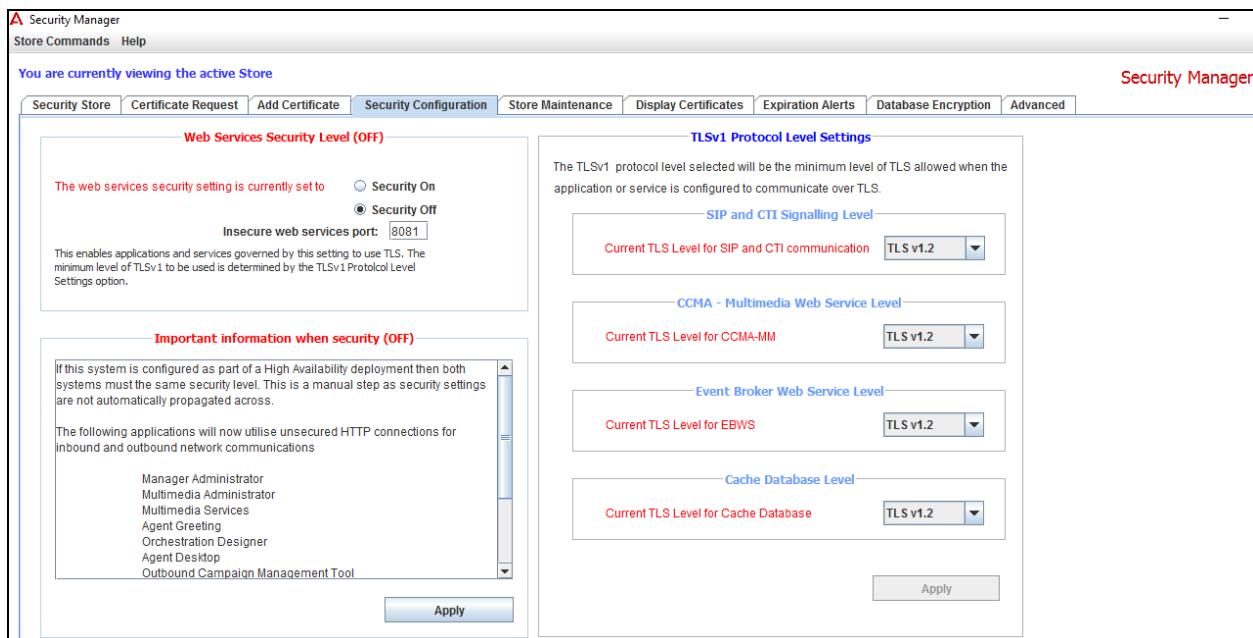
Enter the **security store password** and click **OK**.



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.

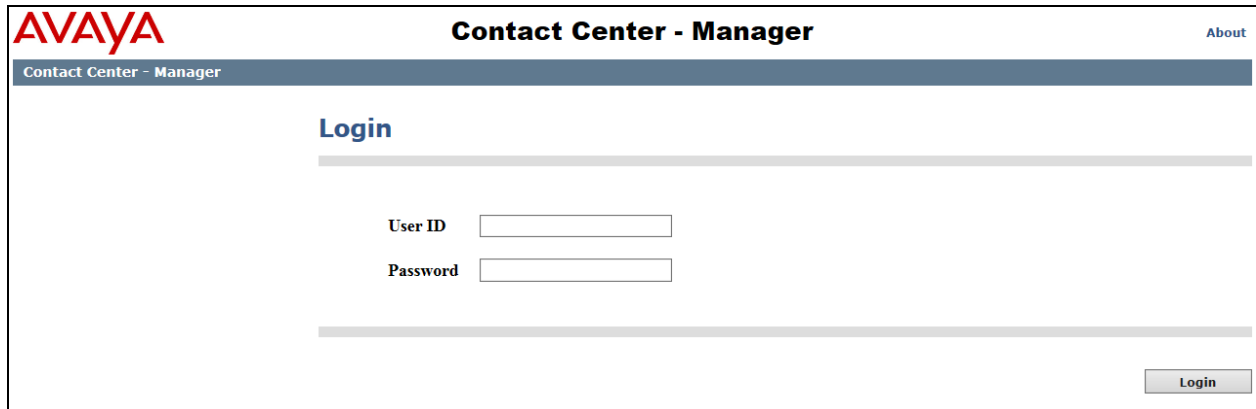


The below screenshot shows the setting for **Security Off**, and the **Insecure web services port** can be seen here as **8081**. Note that the secure port for Enterprise Web Chat is 8445.




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



The screenshot shows the Avaya Contact Center Manager login interface. At the top left is the Avaya logo, and at the top center is the title "Contact Center - Manager". A blue header bar contains the text "Contact Center - Manager". Below this, the word "Login" is displayed in blue. There are two input fields: "User ID" and "Password". A "Login" button is located at the bottom right of the form area.

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.



The screenshot shows the Avaya Contact Center Manager Launchpad page. At the top left is the title "Contact Center - Manager". At the top right are links: "About", "Audit Trail", "Change Password", and "Logout". Below the header bar, the word "Launchpad" is displayed in blue. A list of menu items is shown, each with a circular icon containing a gear. The "Configuration" item is highlighted with a red rectangular box. The other items are "Contact Center Management", "Access and Partition Management", "Real-Time Reporting", "Historical Reporting", "Call Recording and Quality Monitoring", "Prompt Management", "Scripting", "Emergency Help", "Outbound", "Multimedia", and "Data Management". At the bottom, a status bar shows "Last successful login: 25/01/2022 13:40:41".

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

Configuration Logged in user: Administrator Web | [Change Password](#) | [Log Out](#)

Server Download Status Launchpad Help

Skillsets Server: AACCT71-CCMS

Contact Type	Prefix	Skillset Name	Default Activity Code	Threshold Class	Call Age Preference	Out Of Service Mode	Target Sen
Social_Networking	SN_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Voice_Mail	VM_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
SMS	SM_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Fax	FX_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Scanned_Document	SD_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
OpenQ	OQ_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
IM	IM_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Video	VI_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Outbound	OB_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Web_Communications	WC_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
EMail	EM_	Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Voice		Default_Skillset	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Voice		Sales	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Voice		Support	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
Web_Communications	WC_	Webtext	00, Skillset_Default_Activity_Code	Skillset_Template	First In Queue	N/A	0
*							

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.

Skillsets				
	Contact Type	Prefix	Skillset Name	Default Activity Code
	Social_Networking	SN_	Default_Skillset	00, Skillset_Default_Activity_Code
	Voice_Mail	VM_	Default_Skillset	00, Skillset_Default_Activity_Code
	SMS	SM_	Default_Skillset	00, Skillset_Default_Activity_Code
	Fax	FX_	Default_Skillset	00, Skillset_Default_Activity_Code
	Scanned_Document	SD_	Default_Skillset	00, Skillset_Default_Activity_Code
	OpenQ	OQ_	Default_Skillset	00, Skillset_Default_Activity_Code
	IM	IM_	Default_Skillset	00, Skillset_Default_Activity_Code
	Video	VI_	Default_Skillset	00, Skillset_Default_Activity_Code
	Outbound	OB_	Default_Skillset	00, Skillset_Default_Activity_Code
	Web_Communications	WC_	Default_Skillset	00, Skillset_Default_Activity_Code
	EMail	EM_	Default_Skillset	00, Skillset_Default_Activity_Code
	Voice		Default_Skillset	00, Skillset_Default_Activity_Code
	Voice		Sales	00, Skillset_Default_Activity_Code
	Voice		Support	00, Skillset_Default_Activity_Code
	Web_Communications	WC_	Webtext	00, Skillset_Default_Activity_Code
*				

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



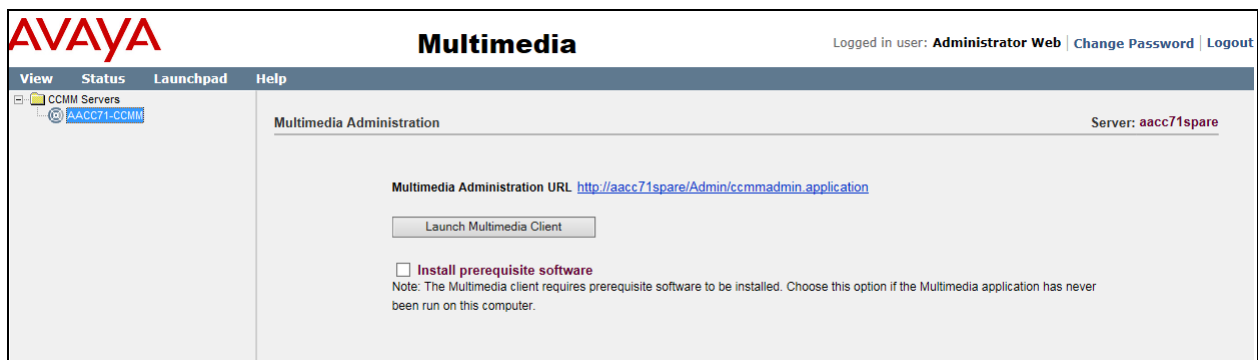
Contact Center - Manager [About](#) | [Audit Trail](#) | [Change Password](#) | [Logout](#)

Launchpad

- Contact Center Management
- Access and Partition Management
- Real-Time Reporting
- Historical Reporting
- Call Recording and Quality Monitoring
- Prompt Management
- Configuration
- Scripting
- Emergency Help
- Outbound
- Multimedia**
- Data Management

Last successful login: 25/01/2022 13:40:41

Click on **Launch Multimedia Client**.



AVAYA **Multimedia** Logged in user: **Administrator Web** | [Change Password](#) | [Logout](#)

View | **Status** | **Launchpad** | **Help**

CCMM Servers

- AACC71-CCMM

Multimedia Administration Server: **aacc71spare**

Multimedia Administration URL <http://aacc71spare/Admin/ccmmadmin.application>

[Launch Multimedia Client](#)

☐ **Install prerequisite software**

Note: The Multimedia client requires prerequisite software to be installed. Choose this option if the Multimedia application has never been run on this computer.

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.

CCMM Administration

AVAYA

Web Comms Settings

Web Comms Agent Timers

Keep Alive Time: 0 Minute(s) 30 Second(s)

Message Refresh: 3 Second(s)

Desirable Response: 30 Second(s) (Customer Awaiting Agent)

60 Second(s) (Agent Awaiting Customer)

Consult Request Timeout: 30 Second(s)

Force Idle Customer Check: ☐

Force Idle Customer Check Timeout: 180 Second(s)

Save Timestamp on Chat Messages: ☒

Save Chat History: ☒

Enable Transfer To Skillset: ☒

Concurrent Chats Limit per Customer: 3

Requested Call-backs Limit per Customer: 3

Chat Conversation

☐ E-mail chat log to Customer

Enterprise Web Chat

Enable Enterprise Web Chat: ☒

Chat session to survive a webpage refresh: ☒

External Web Server Domain: *

Transcript Filtering Web Service:

EWC Web Applications port:

Save Cancel Help

User: webadmin | Server Time: 15:35 | Status:

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.

Skillset	Welcome Message
WC_Default_Skillset	
WC_Webtext	

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.

Skillset Name	Route Point	Auto-Sign	Office Hou	Chat Histo	Comfort N	On Hold N	Max Conci
PO_Default_Skillset							
SN_Default_Skillset							
VM_Default_Skillset							
SM_Default_Skillset							
FX_Default_Skillset							
SD_Default_Skillset							
OB_Default_Skillset							
WC_Default_Skillset	OpenQRoutePointAddress						50

Skillset:
WC_Default_Skillset

Route Point:
OpenQRoutePointAddre

Office Hours:
Unlink Hours

Chat History Header:
Unlink Chat

Comfort Group:
Unlink Group

On Hold Group:
Unlink Group

Web On Hold Group:
Unlink Group

Max Concurrent Chats:
50

Auto-Signature:

Reload Grid

Save
Cancel
Help

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

The screenshot displays the Avaya CCMM Administration web application. The left sidebar contains the Avaya logo and a navigation menu with the following items: General Administration (selected), Server Settings, Skillset Settings, Administrator Settings, Agent Settings, General Settings, and Office Hours. Below the menu is a list of system components: E-mail, Web Comms, Social Networking, IM, Voice Mail, Fax, Scanned Documents, Text Messaging (SMS), Workspaces Configuration, Agent Desktop Configuration, and General Administration (highlighted in orange).

The main content area features a table with the following columns: Skillset Name, Route Point, Auto-Sign, Office Hou, Chat Histo, Comfort Iv, On Hold Iv, and Max Conci. The table contains two rows: EM_Default_Skillset and WC_Webtext. The WC_Webtext row is highlighted in orange and shows 'OpenQRoutePointAddress' in the Route Point column and '50' in the Max Conci column.

Below the table is a pagination bar showing 'Page 2 of 2'. Below the pagination bar is the 'Edit Skillset' form for 'WC_Webtext'. The form includes the following fields and controls:

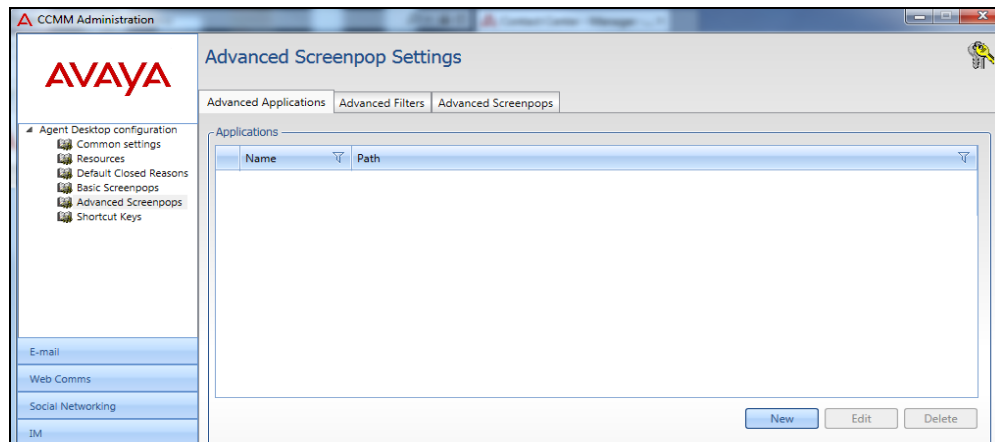
- Skillset:** WC_Webtext
- Route Point:** OpenQRoutePointAddress (dropdown menu)
- Office Hours:** (dropdown menu) with an 'Unlink Hours' button
- Chat History Header:** (dropdown menu) with an 'Unlink Chat' button
- Comfort Group:** (dropdown menu) with an 'Unlink Group' button
- On Hold Group:** (dropdown menu) with an 'Unlink Group' button
- Web On Hold Group:** (dropdown menu) with an 'Unlink Group' button
- Max Concurrent Chats:** 50
- Auto-Signature:** A large text area for the signature, with a 'Reload Grid' button to its right.
- Buttons:** Save, Cancel, and Help buttons are located at the bottom right of the form.

The bottom status bar shows 'User: webadmin | Server Time: 15:37 | Status:'.

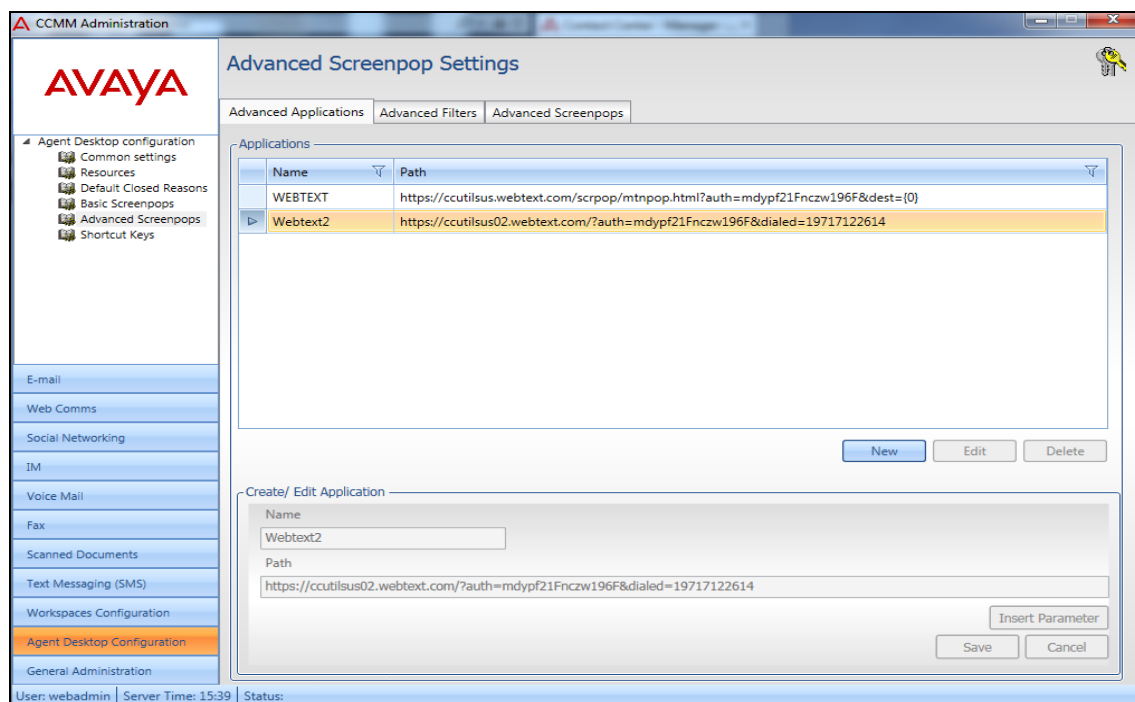
5.3. Configure Avaya Agent Desktop

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 by 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.

CCMM Administration

Advanced Screenpop Settings

Advanced Applications | **Advanced Filters** | Advanced Screenpops

Filters

Name	Intrinsic Name	Match Values
Webtext	Skillset	Sales

New Edit Delete

Create/ Edit Filter

Name: Webtext

Intrinsic Type: Skillset

Contact Types:

- ☒ Voice
- ☐ E-mail
- ☐ Web Communications
- ☐ IM
- ☐ Scanned Documents
- ☐ Fax
- ☐ Open Queue

Skillsets:

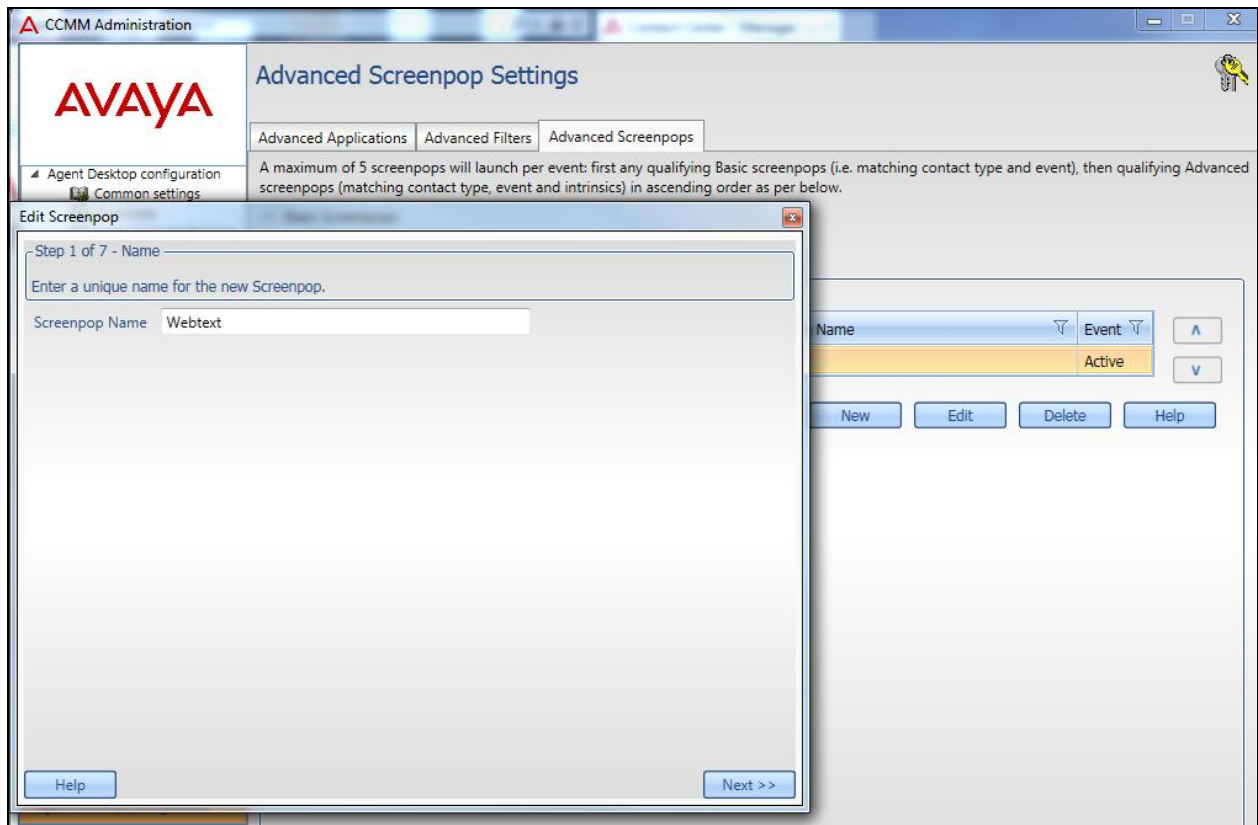
Select	Name
<input type="checkbox"/>	Agent_Queue_To
<input type="checkbox"/>	Default ACD
<input type="checkbox"/>	Default NACD
<input type="checkbox"/>	Default_Skillset
<input checked="" type="checkbox"/>	Sales
<input type="checkbox"/>	Support

Page 1 of 1

Save Cancel

User: webadmin | Server Time: 15:39 | Status:

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.

Edit Screenpop

Step 2 of 7 - Contact Types

Select the contact types for this screenpop

Contact Types

- ☒ Voice
- ☐ E-mail
- ☐ Web Communications
- ☐ IM
- ☐ Scanned Documents
- ☐ Fax
- ☐ Open Queue
- ☐ Outbound
- ☐ SMS
- ☐ Social Networking
- ☐ Voice Mail
- ☐ POM Outbound
- ☐ Video

Screenpop Summary

'Webtext' will launch the application
<https://ccutilsus02.webtext.com/?auth=mdypf21Fnczw196F&dialcd=19717122614>
for Active contacts of type Voice
if it satisfies the filter 'Webtext'.

Help << Prev Next >>

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.

Edit Screenpop

Step 3 of 7 - Launch Event

Now select the event on which this screenpop will launch.

Triggers

Launch Event: **Active**

Screenpop Summary

'Webtext' will launch the application
<https://ccutilsus02.webtext.com/?auth=mdypf21Fnczw196F&dialed=19717122614>
for Active contacts of type Voice
if it satisfies the filter 'Webtext'.

Help << Prev Next >>

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

Step 4 of 7 - Application

Select the application that will launch when this Screenpop is displayed

Application Name: Webtext2 [+] [Edit]

Path: <https://ccutilsus02.webtext.com/?auth=mdypf21Fnczw196F&dialcd=19717122614>

Screenpop Summary

'Webtext' will launch the application
<https://ccutilsus02.webtext.com/?auth=mdypf21Fnczw196F&dialcd=19717122614>
for Active contacts of type Voice
if it satisfies the filter 'Webtext'.

Help [<< Prev] [Next >>]

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

The screenshot shows a window titled "Edit Screenpop" with a close button in the top right corner. The window contains the following elements:

- Step 5 of 7 - Customise Application**: A section header with a blue line underneath.
- Instructions**: A text box containing the text: "Match each parameter with an intrinsic value by selecting values from the drop down boxes and clicking set. Use the application path as a guide. The summary will update as parameters are set."
- Application Path**: A text field containing the URL: "https://ccutilsus02.webtext.com/?auth=mdypf21Fnczw196F&dialcd=19717122614".
- Set Parameters**: A section with two dropdown menus labeled "Parameter" and "Intrinsic", and a "Set" button to the right.
- Parameters**: A large empty rectangular box for listing parameters.
- Screenpop Summary**: A text box containing the text: "'Webtext' will launch the application https://ccutilsus02.webtext.com/?auth=mdypf21Fnczw196F&dialcd=19717122614 for Active contacts of type Voice if it satisfies the filter 'Webtext'."
- Buttons**: A "Help" button on the bottom left, and "<< Prev" and "Next >>" buttons on the bottom right.

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

The screenshot shows a window titled "Edit Screenpop" with a close button in the top right corner. The window is divided into several sections:

- Step 6 of 7 - Filter**: This section contains instructions: "Optionally select a filter (NOTE: If a filter is selected, screenpops will only display if the conditions of the filter are satisfied)" and "Only filters containing all of your selected contact types (Voice) are available."
- Select Filter**: This section contains a "Filter" label, a dropdown menu showing "Webtext", a blue "+" button, and an "Edit" button.
- Selected Filter Conditions**: This section is divided into two columns. The left column is labeled "Intrinsic Name:" and contains the text "Skillset". The right column is labeled "Match Values:" and contains a text box with the text "Sales".
- Screenpop Summary**: This section contains a summary of the screenpop configuration: "'Webtext' will launch the application https://ccutilsus02.webtext.com/?auth=mdypf21Fnczw196F&dialcd=19717122614 for Active contacts of type Voice if it satisfies the filter 'Webtext'."

At the bottom of the window, there are three buttons: "Help", "<< Prev", and "Next >>".

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

The screenshot shows a window titled "Edit Screenpop" with a close button in the top right corner. The window is divided into three main sections:

- Step 7 of 7 - Presentation Options**: This section contains a text box with the instruction: "Optionally select if a url launches internally on Agent Desktop and if the internal screenpops close when the contact is closed."
- Presentation Options**: This section contains two checked checkboxes:
 - ☒ Launch Screenpop in a tab inside AAAD
 - ☒ Auto Close Screenpop tab(s) on Work Item Release
- Screenpop Summary**: This section contains a text box with the following text:

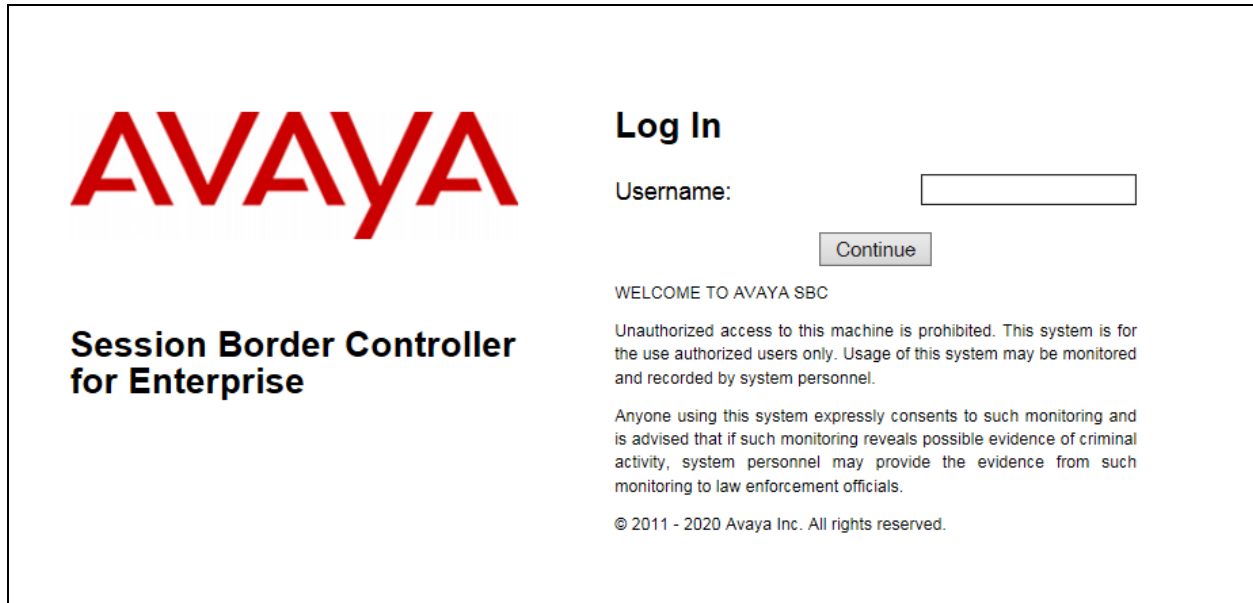
'Webtext' will launch the application
<https://ccutilsus02.webtext.com/?auth=mdypf21Fnczw196F&dialcd=19717122614>
for Active contacts of type Voice
if it satisfies the filter 'Webtext'.

At the bottom of the window, there are three buttons: "Help", "<< Prev", and "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.



The image shows the login page for the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold black. On the right, under the heading 'Log In', there is a 'Username:' label followed by a text input field. Below the input field is a 'Continue' button. Further down, there is a 'WELCOME TO AVAYA SBC' message, a disclaimer about unauthorized access, a consent statement, and a copyright notice for 2011-2020 Avaya Inc.

AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Continue

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

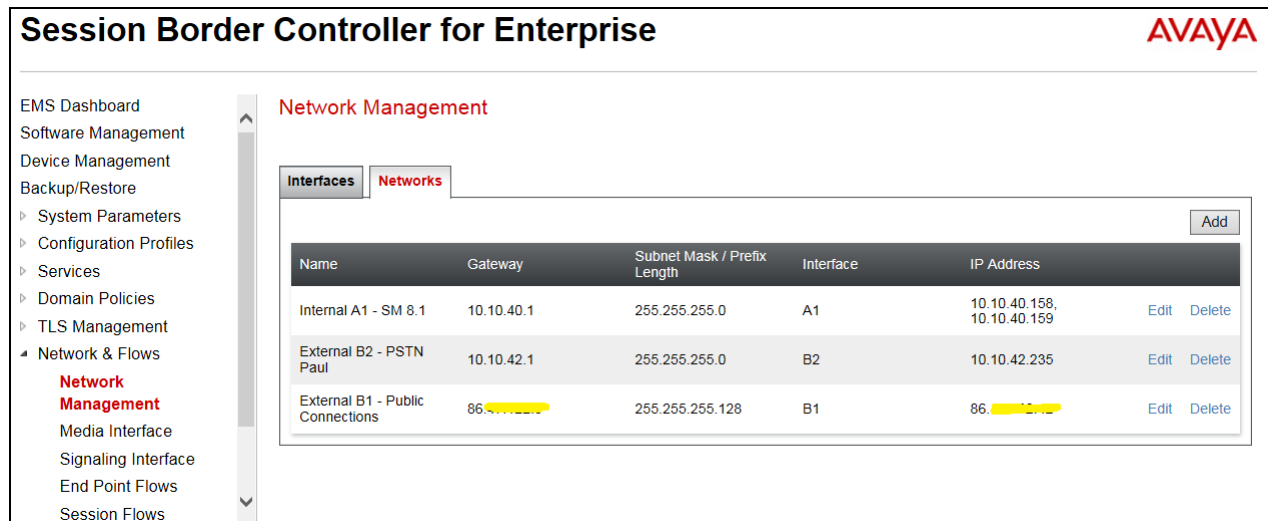
From the top left of the screen, select the SBCE from the **Device** drop-down menu.

The screenshot shows the Avaya EMS Dashboard for Enterprise. The top navigation bar includes 'Device: EMS', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The sidebar on the left lists 'EMS' and 'ASBCE8vmpp'. The main content area is titled 'Dashboard' and contains several sections:

- Information**: A table with system details.

Information	
System Time	02:04:39 PM GMT Refresh
Version	8.1.3.0-31-21052
GUI Version	8.1.3.0-21196
Build Date	Wed Sep 15 17:30:15 UTC 2021
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	01/25/2022 11:55:49 GMT
Failed Login Attempts	0
- Installed Devices**: A list showing 'EMS' and 'ASBCE8vmpp'.
- Active Alarms (past 24 hours)**: None found.
- Incidents (past 24 hours)**: None found.

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.



Session Border Controller for Enterprise AVAYA

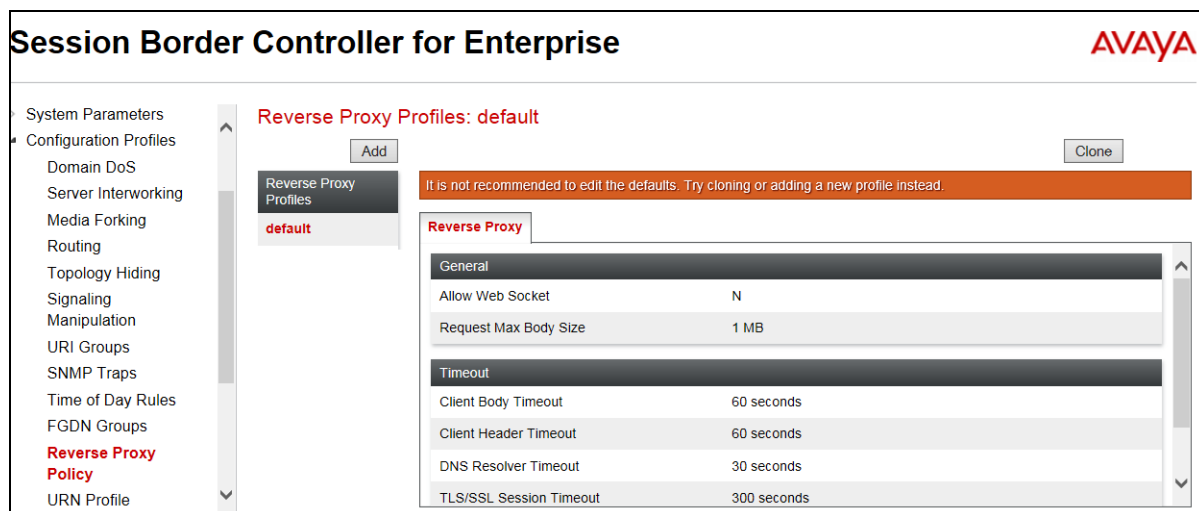
EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
Network Management
Media Interface
Signaling Interface
End Point Flows
Session Flows

Network Management

Interfaces Networks Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Internal A1 - SM 8.1	10.10.40.1	255.255.255.0	A1	10.10.40.158, 10.10.40.159	Edit	Delete
External B2 - PSTN Paul	10.10.42.1	255.255.255.0	B2	10.10.42.235	Edit	Delete
External B1 - Public Connections	86.100.123.1	255.255.255.128	B1	86.100.123.1	Edit	Delete

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**.



Session Border Controller for Enterprise AVAYA

System Parameters
Configuration Profiles
Domain DoS
Server Interworking
Media Forking
Routing
Topology Hiding
Signaling Manipulation
URI Groups
SNMP Traps
Time of Day Rules
FGDN Groups
Reverse Proxy Policy
URN Profile

Reverse Proxy Profiles: default

Add Clone

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Reverse Proxy

General

Allow Web Socket N

Request Max Body Size 1 MB

Timeout

Client Body Timeout 60 seconds

Client Header Timeout 60 seconds

DNS Resolver Timeout 30 seconds

TLS/SSL Session Timeout 300 seconds

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

Editing Rule: WEBSOCKET

General

Allow Web Socket

☒

Request Max Body Size

5

MB

Timeout

Client Body Timeout

60

seconds

Client Header Timeout

60

seconds

DNS Resolver Timeout

30

seconds

TLS/SSL Session Timeout

300

seconds

Server Read Timeout

60

seconds

Rate/Connection Limiting

Enable Rate Limiting

☐

Total Number of Clients

Max Simultaneous Connections

per client

Average Request Rate

per client/

per second

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.

Session Border Controller for Enterprise

AVAYA

I-GDN Groups
Reverse Proxy
Policy
URN Profile
Recording Profile
H248 Profile
Services
Domain Policies
TLS Management
Network & Flows
DMZ Services
Relay
Firewall
TURN/STUN
PPM Mapping
Monitoring & Logging

Relay Services: ASBCE8vmpg

Application Relay
Reverse Proxy
XMPP
H248 Relay

Service Name

Status

Listen IP:Port & Protocol

Listen Domain Network

Connect IP Network

Server Protocol

Server Addresses & Ports

PPM Mapping Profile

View

Clone

Edit

Delete

WebServiceSecure

Enabled

86.47.122.42:8445

HTTPS

External B1 - Public Connections (B1, VLAN 0)

10.10.40.158

Internal A1 - SM 8.1 (A1, VLAN 0)

HTTPS

10.10.40.96:8445

View

Clone

Edit

Delete

WebService

Enabled

86.47.122.42:8081

HTTP

External B1 - Public Connections (B1, VLAN 0)

10.10.40.158

Internal A1 - SM 8.1 (A1, VLAN 0)

HTTP

10.10.40.96:8081

View

Clone

Edit

Delete

Add

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**.

Service Name

WebService

×

Enabled

☒

Listen IP

External B1 - Public Connec

86.

Listen Port

8081

Listen Protocol

HTTP

Listen TLS Profile
(TLS Server Profile)

None

Listen Domain
(Optional)

Connect IP

Internal A1 - SM 8.1 (A1, VL

10.10.40.158

Server Protocol

HTTP

Server TLS Profile
(TLS Client Profile)

None

Rewrite URL

☐

Load Balancing
Algorithm

None

PPM Mapping Profile

None

Reverse Proxy Policy Profile

WEBSOCKET

Whitelisted IPs
Max of 5 comma-separated IPs.

Add

Server Addresses	Received Server Host	Whitelisted URL	URL Replace
10.10.40.96:8081	Any	/	
			Delete

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.

Service Name

WebServiceSecure

×

Enabled

☒

Listen IP

External B1 - Public Connec

86.

Listen Port

8445

Listen Protocol

HTTPS

Listen TLS Profile
(TLS Server Profile)

SM81_Interface

Listen Domain
(Optional)

Connect IP

Internal A1 - SM 8.1 (A1, VL

10.10.40.158

Server Protocol

HTTPS

Server TLS Profile
(TLS Client Profile)

SM81_Interface

Rewrite URL

☐

Load Balancing
Algorithm

None

PPM Mapping Profile

None

Reverse Proxy Policy Profile

WEBSOCKET

Whitelisted IPs
Max of 5 comma-separated IPs.

Add

Server Addresses	Received Server Host	Whitelisted URL	URL Replace	
10.10.40.96:8445	Any	/		Delete

Finish

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.

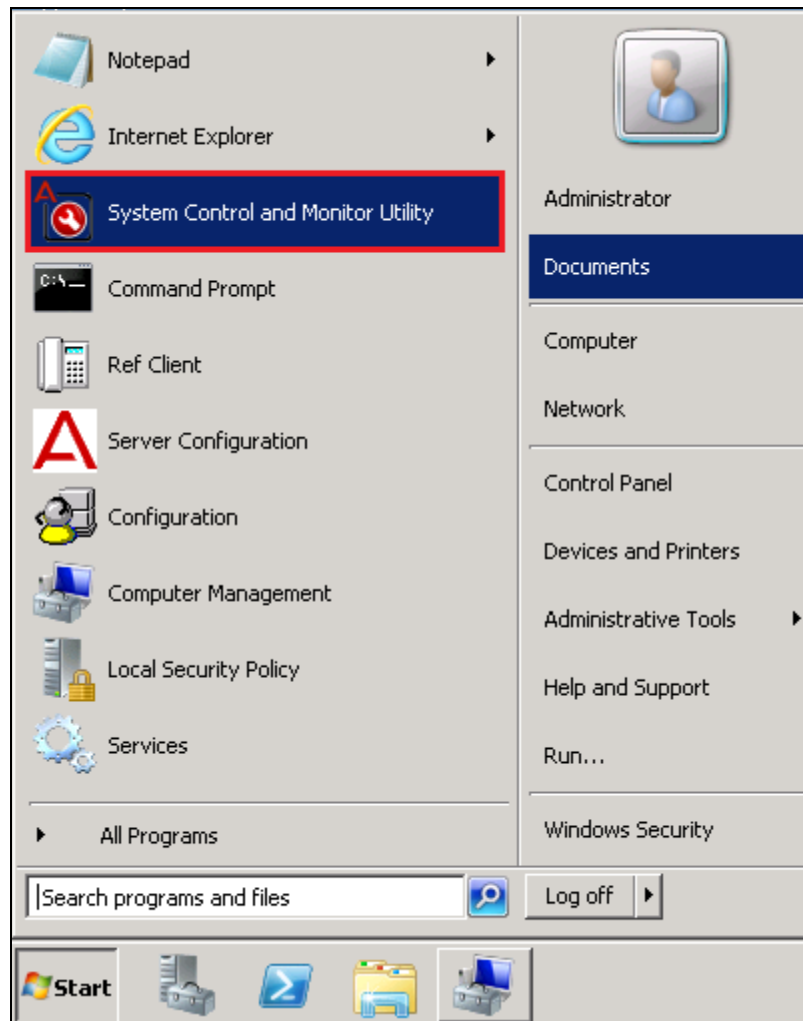
Please note that information such as, the public routable FQDN and port for the EWC service, skillset names and associated numbers, and any certificates required for TLS communication, will need to be shared with WEBTEXT.

8. Verification Steps

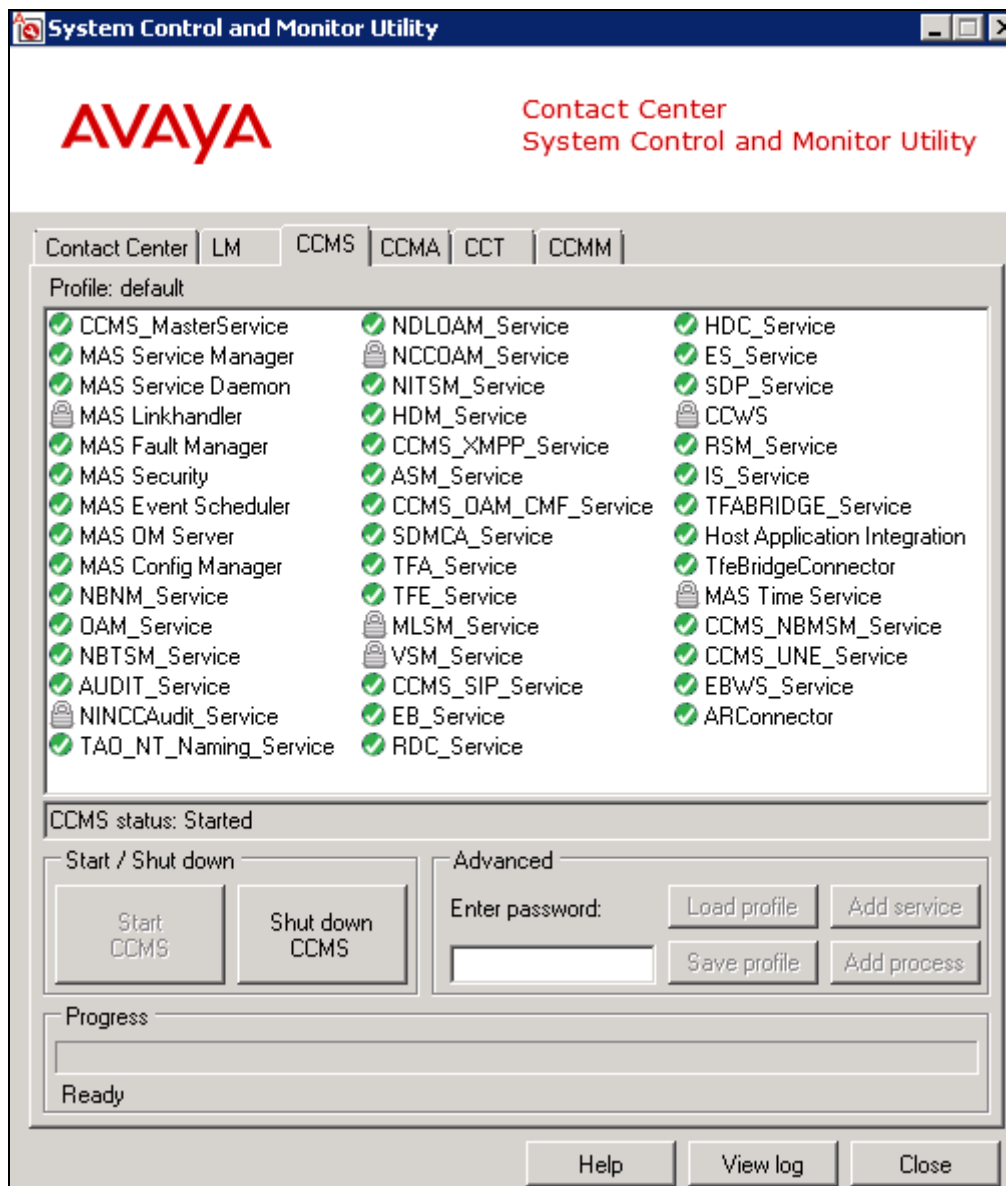
This section provides the tests that can be performed to verify correct configuration of WEBTEXT Contact Center Messaging with Avaya Aura® Contact Center.

8.1. Verify Avaya Aura® Contact Center Services

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



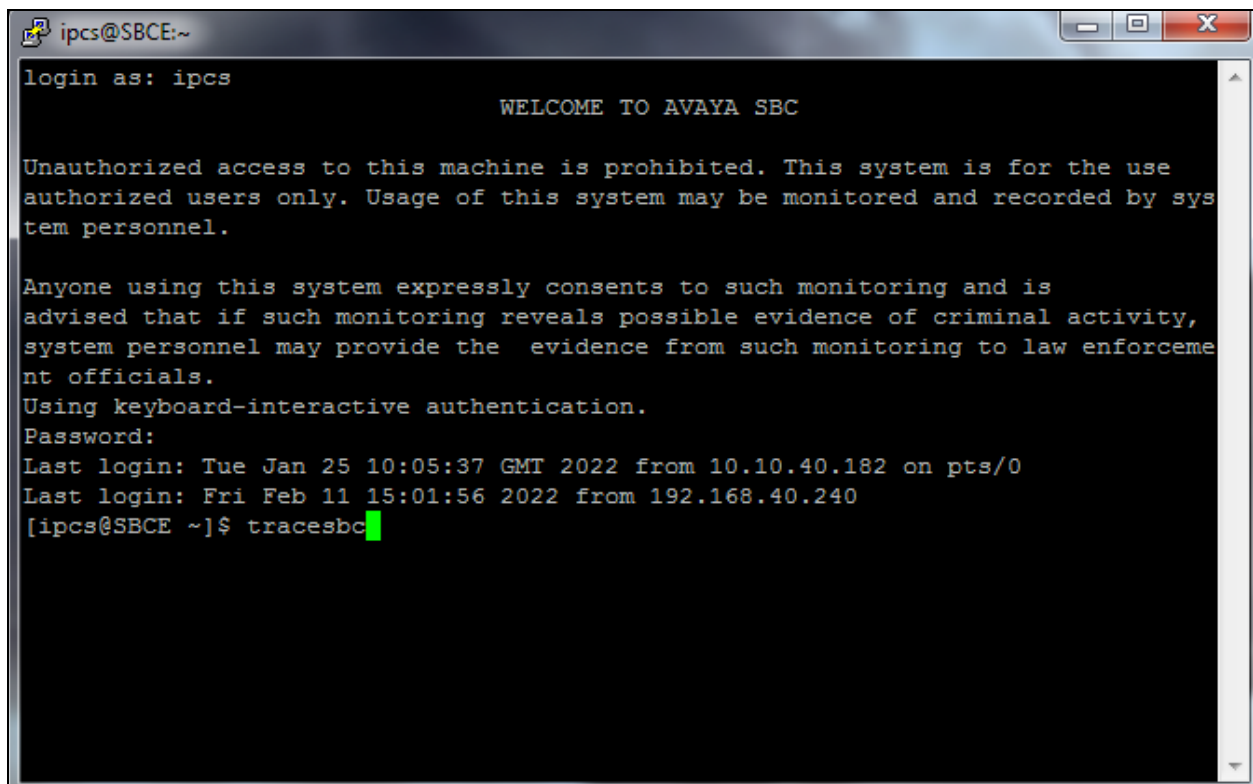
Navigate across each of the tabs, paying special attention to any service that may not be running. The **CCMS** services are all showing green below which indicates that the Contact Center Manager Server is fully operational. Check this the case for all services on all tabs.



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

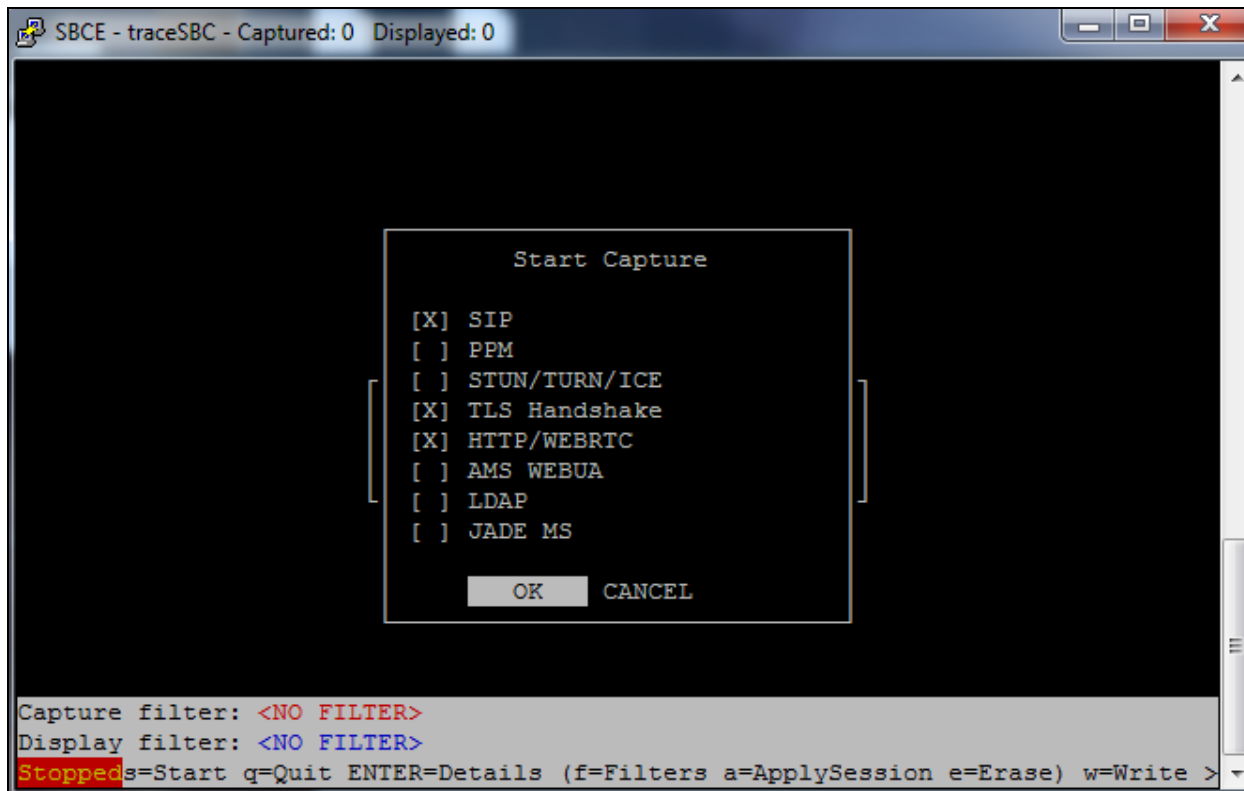
The “tracesbc” facility on the Session Border Controller for Enterprise shows all connections that pass through the SBCE including the Reverse Proxy connections. Before an SMS is sent to the number associated with the SMS service to the Agent Desktop, open the tracesbc and once the SMS is sent the messaging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

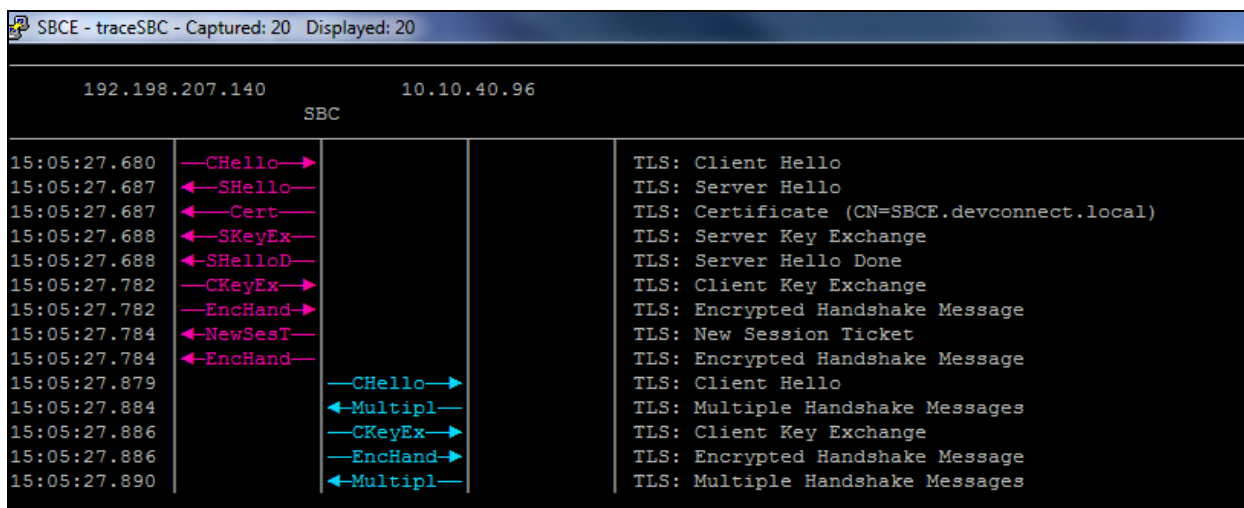


```
ipcs@SBCE:~  
login as: ipcs  
WELCOME TO AVAYA SBC  
Unauthorized access to this machine is prohibited. This system is for the use  
authorized users only. Usage of this system may be monitored and recorded by sys  
tem personnel.  
Anyone using this system expressly consents to such monitoring and is  
advised that if such monitoring reveals possible evidence of criminal activity,  
system personnel may provide the evidence from such monitoring to law enforceme  
nt officials.  
Using keyboard-interactive authentication.  
Password:  
Last login: Tue Jan 25 10:05:37 GMT 2022 from 10.10.40.182 on pts/0  
Last login: Fri Feb 11 15:01:56 2022 from 192.168.40.240  
[ipcs@SBCE ~]$ tracesbc
```

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.

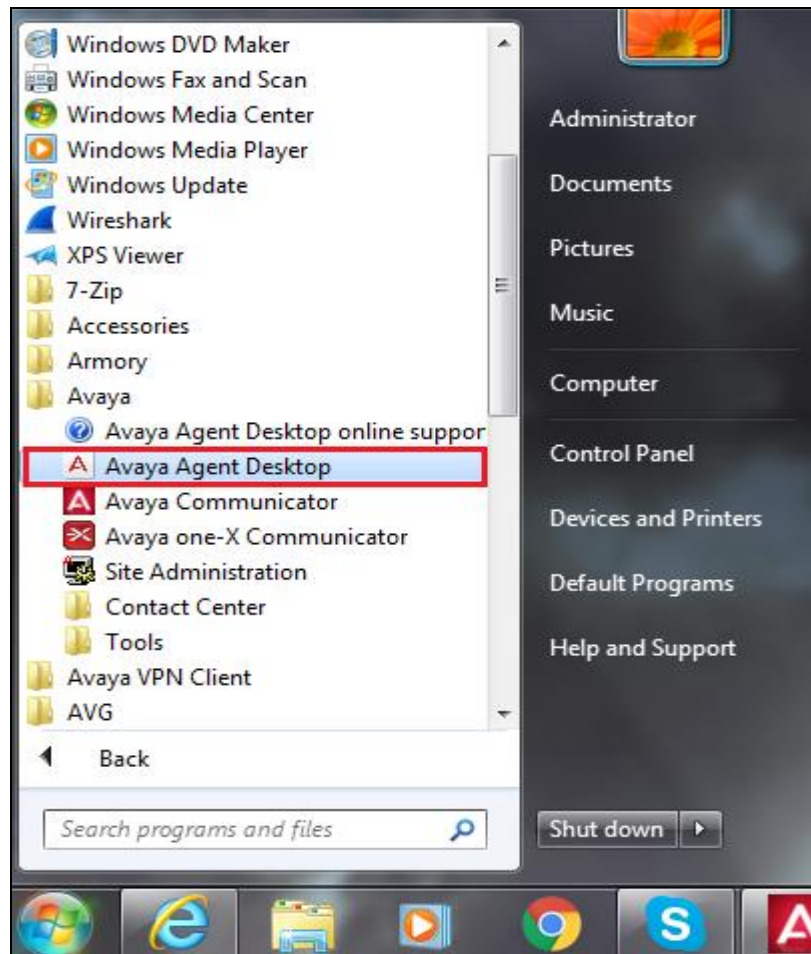


The exchange below shows the certificate exchange between WEBTEXT and AACC was successful.

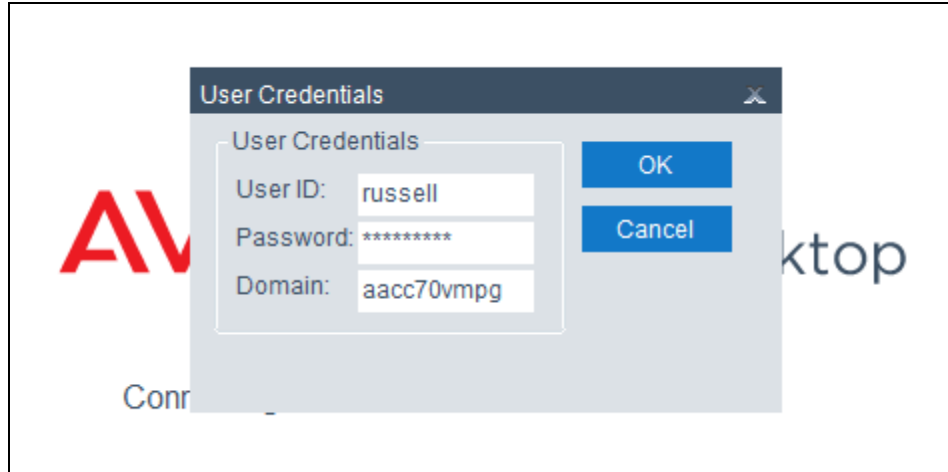


8.3. Verify SMS Sent/Received on Avaya Agent Desktop

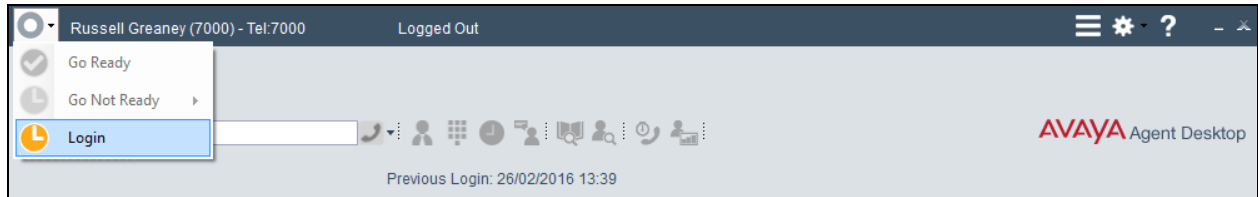
From a client PC where AAAD is installed, open **Avaya Agent Desktop**.



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**.

A screenshot of the 'Enter Login details' dialog box. It has two tabs: 'Telephony' and 'Multimedia' (which is selected and highlighted with a red border). Under the 'Multimedia' tab, there is a section titled 'Account Info' containing two input fields: 'ID:' with the value '7000' and 'Password:' with the value '*****'. At the bottom right of the dialog, there are two buttons: 'Login' (highlighted with a red border) and 'Cancel'.

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

The screenshot displays the AVAYA Agent Desktop interface. At the top, a status bar shows a green checkmark, the agent's name "Russell Greaney (7000) - Tel:7000", and the status "Ready". To the right are icons for a menu, settings, help, and window management. Below the status bar is a toolbar with various icons for customer search, call management, and other functions. The main interface is divided into two sections. On the left is a "Customer Details" form with fields for Title, Last Name, and First Name, each with a "Create" button. Below these are tabs for Details, History, CI Details, and Reviews. Further down are sections for Phone (with Edit and Add buttons), Email, Addresses, and URI. At the bottom of the left section is a "Custom Fields" table with columns for Customer, Contact, and Intrinsic. The right section is a large, empty workspace. At the bottom of the interface, a status bar shows "Previous Login: 15/03/2016 14:41".

AVAYA Agent Desktop

Customer Details

Title Create

Last Name

First Name

Details History CI Details Reviews

Phone Edit Add

Email

Addresses

URI

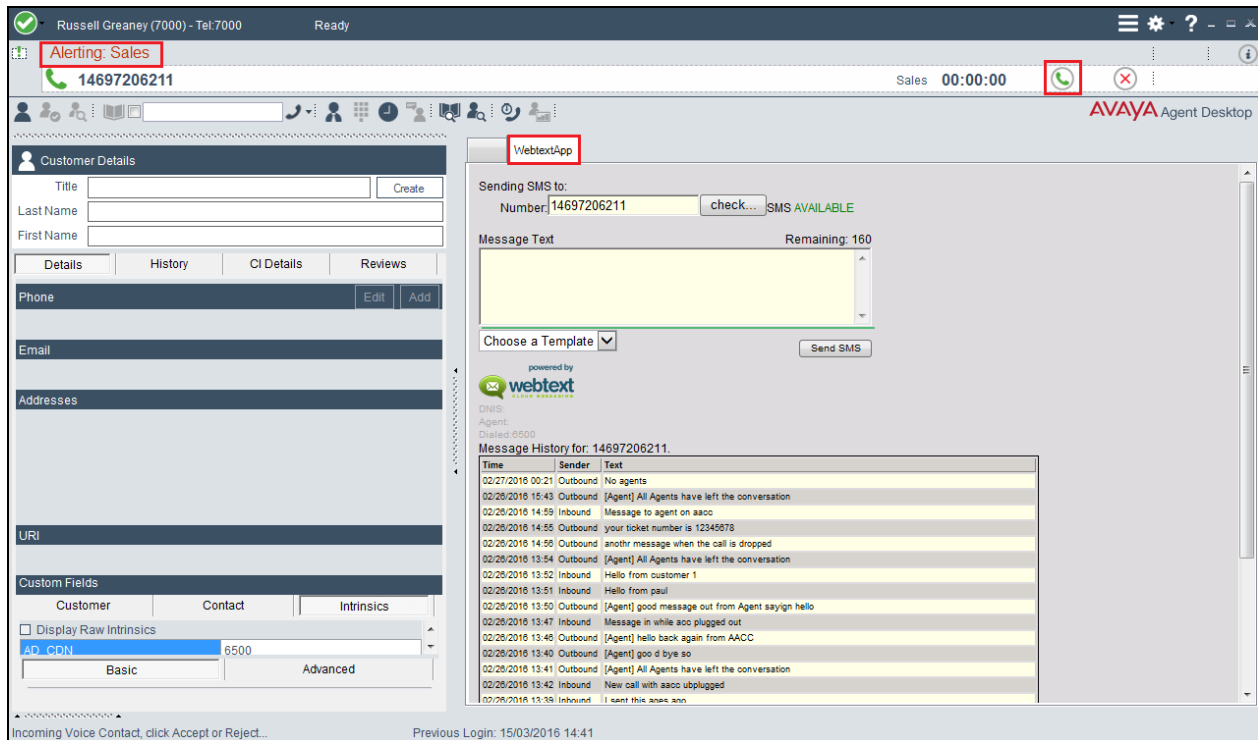
Custom Fields

Customer	Contact	Intrinsic
<input type="text"/>		

Previous Login: 15/03/2016 14:41

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.

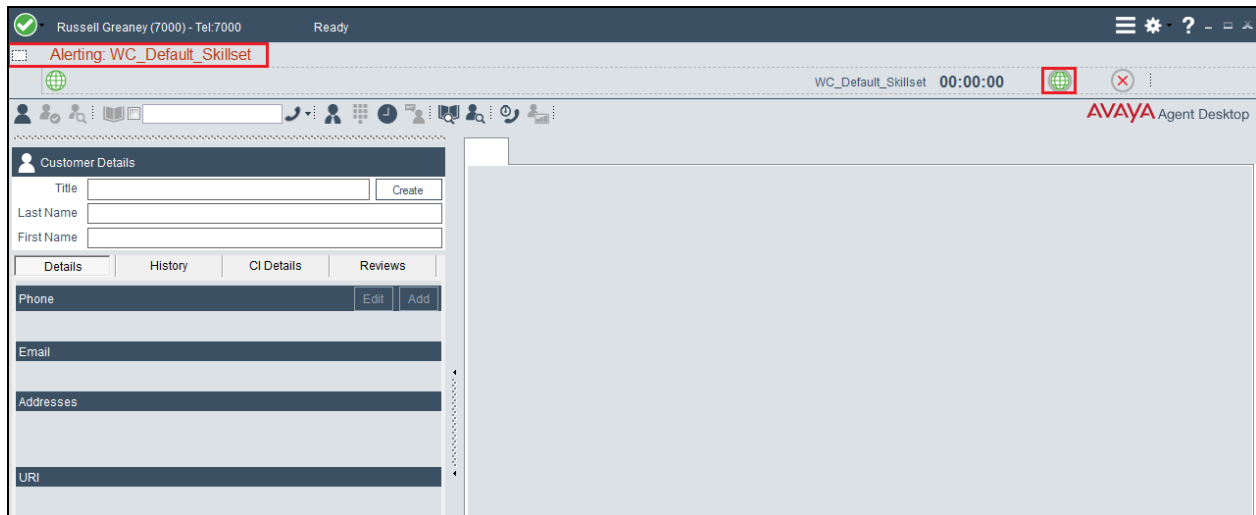


The **Number** is automatically populated with the CLID of the caller and the agent can simply enter the SMS message that needs to be sent and the **Send SMS** button is pressed. This will send a text message to the phone number highlighted below.

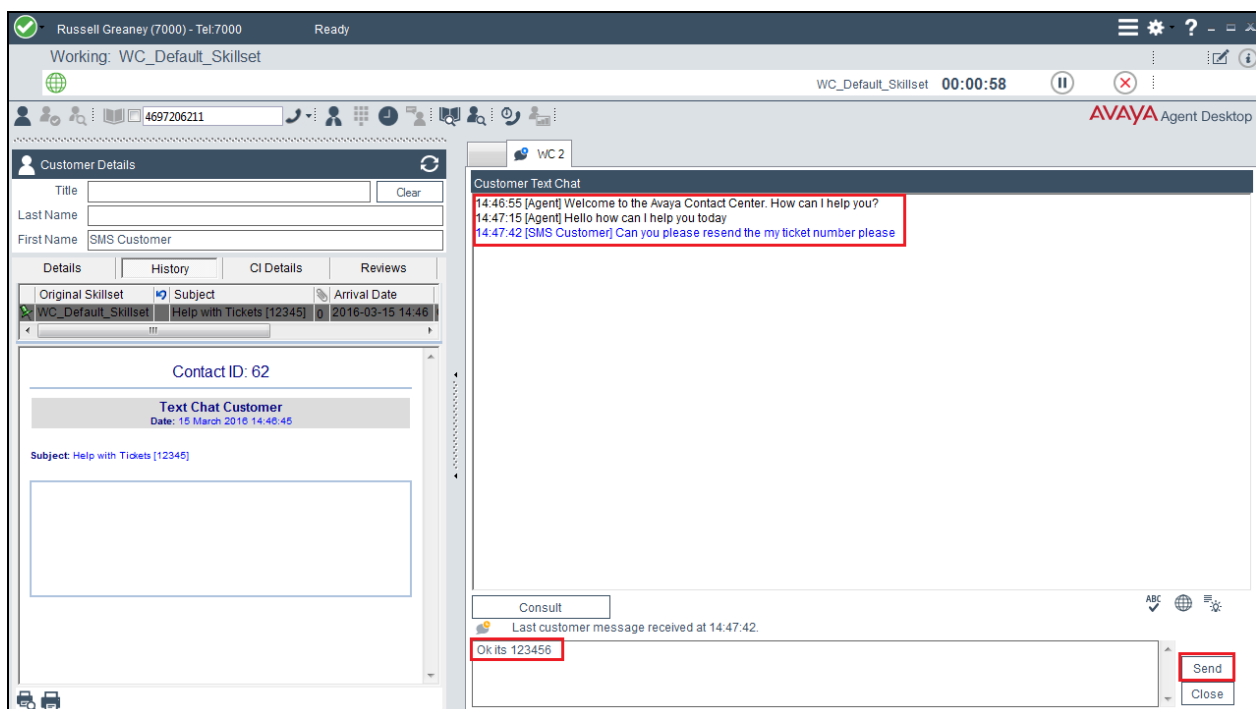
The screenshot displays the Avaya WebtextApp interface. At the top, a status bar shows 'Working: Sales' and the phone number '14697206211'. Below this, a 'Customer Details' section includes fields for Title, Last Name, and First Name, along with tabs for Details, History, CI Details, and Reviews. The main area is titled 'WebtextApp' and contains the 'Sending SMS to:' section. The 'Number' field is populated with '14697206211' and has a 'check...' button next to it, which shows 'SMS AVAILABLE'. The 'Message Text' field contains the text 'Your reference number is 1234'. To the right of the message text, it says 'Remaining: 131'. Below the message text is a 'Choose a Template' dropdown menu. At the bottom right of the main area is a 'Send SMS' button. The interface also shows a 'powered by webtext' logo and some system information like 'DNIS: Agent: Dialed: 6500' and 'Message History for: 14697206211'.

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.

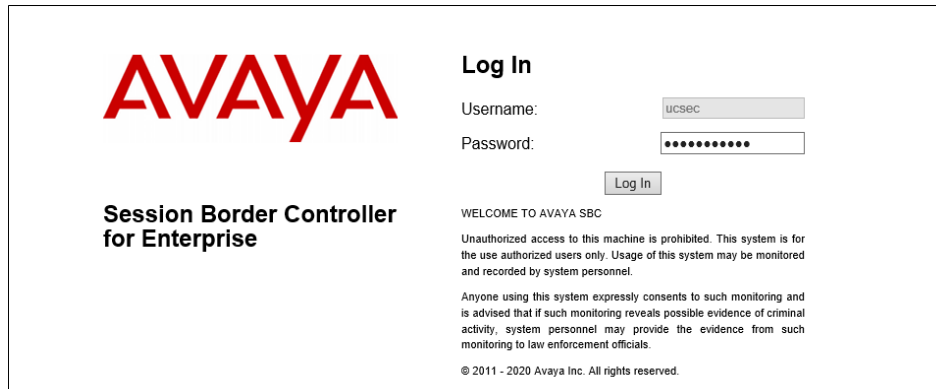
The following tasks are performed:

- 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.



The image shows the login page for the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise'. On the right, under the heading 'Log In', there are input fields for 'Username' (containing 'ucsec') and 'Password' (masked with dots). Below these fields is a 'Log In' button. At the bottom of the page, there is a disclaimer: 'WELCOME TO AVAYA SBC. Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials. © 2011 - 2020 Avaya Inc. All rights reserved.'

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

Information	
System Time	02:49:49 PM IST Refresh
Version	8.1.1.0-26-19214
GUI Version	8.1.1.0-19189
Build Date	Wed Jul 22 23:36:51 UTC 2020
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	07/21/2021 14:46:02 IST
Failed Login Attempts	0

Installed Devices
EMS
SBCE-rw

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.

Installed Certificates	View	Delete
SBCE_RW_Inside.pem	View	Delete
SBCE_RW_Outside.pem	View	Delete
sbsectigo.crt	View	Delete
724sect.crt	View	Delete

Installed CA Certificates	View	Delete
AvayaDeviceEnrollmentCAchain.crt	View	Delete
SMGR_RW_RootCert.pem	View	Delete
sectigoCA.cer	View	Delete

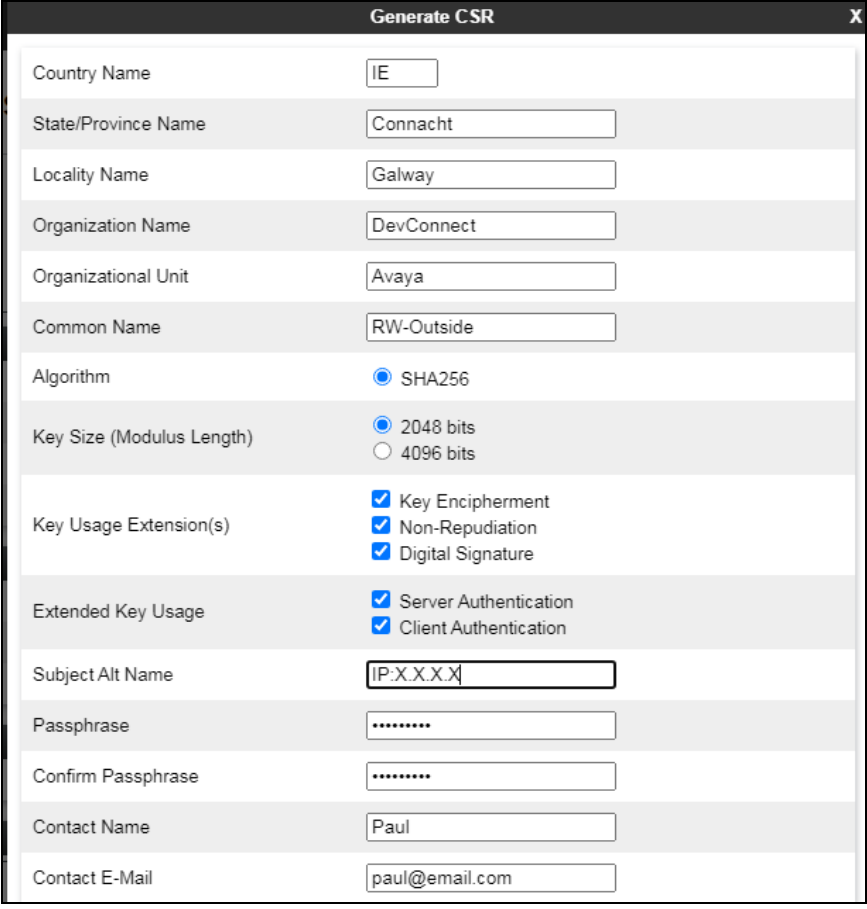
Installed Certificate Revocation Lists
No certificate revocation lists have been installed.

Installed Certificate Signing Requests

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**.



The screenshot shows a web form titled "Generate CSR" with a close button (X) in the top right corner. The form contains the following fields and options:

Field	Value
Country Name	IE
State/Province Name	Connacht
Locality Name	Galway
Organization Name	DevConnect
Organizational Unit	Avaya
Common Name	RW-Outside
Algorithm	<input checked="" type="radio"/> SHA256
Key Size (Modulus Length)	<input checked="" type="radio"/> 2048 bits <input type="radio"/> 4096 bits
Key Usage Extension(s)	<input checked="" type="checkbox"/> Key Encipherment <input checked="" type="checkbox"/> Non-Repudiation <input checked="" type="checkbox"/> Digital Signature
Extended Key Usage	<input checked="" type="checkbox"/> Server Authentication <input checked="" type="checkbox"/> Client Authentication
Subject Alt Name	IP:X.X.X.X
Passphrase	*****
Confirm Passphrase	*****
Contact Name	Paul
Contact E-Mail	paul@email.com

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.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top header shows "Session Border Controller for Enterprise" and the Avaya logo. On the left is a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled "Certificates" and includes an "Install" button (highlighted with a red box) and a "Generate CSR" button. Below these are four sections: "Installed Certificates" (listing SBCE_RW_Inside.pem, SBCE_RW_Outside.pem, sbcsectigo.crt, and 724sect.crt with View and Delete links), "Installed CA Certificates" (listing AvayaDeviceEnrollmentCAchain.crt, SMGR_RW_RootCert.pem, and sectigoCA.cer with View and Delete links), "Installed Certificate Revocation Lists" (showing a message that no lists have been installed), and "Installed Certificate Signing Requests" (which is currently empty).

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).

Install Certificate X

Type: ☒ Certificate, ☐ CA Certificate, ☐ Certificate Revocation List

Name: SBCE_Outside

Overwrite Existing: ☒

Allow Weak Certificate/Key: ☒

Certificate File: Choose File No file chosen

Trust Chain File: Choose File No file chosen

Key: ☒ Use Existing Key, ☐ Upload Key File

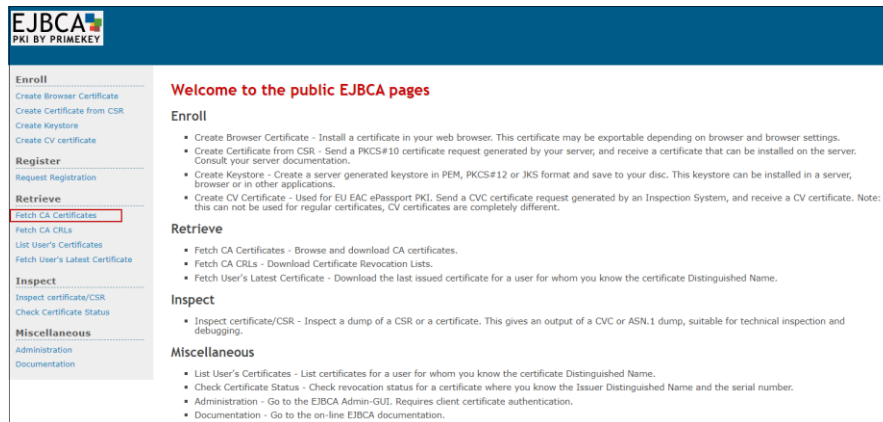
Key File: SBCE_RW_Outside.key

Upload

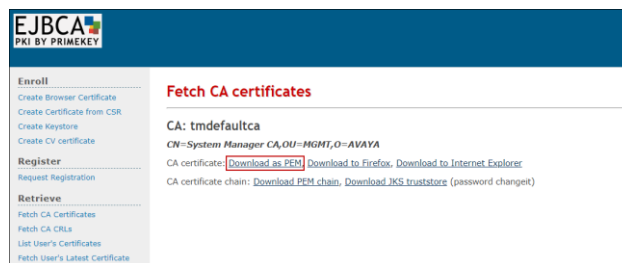
Note: The installation of the “Inside” identity certificate follows the same procedure, but uses the key generated for the inside cert instead.

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**.



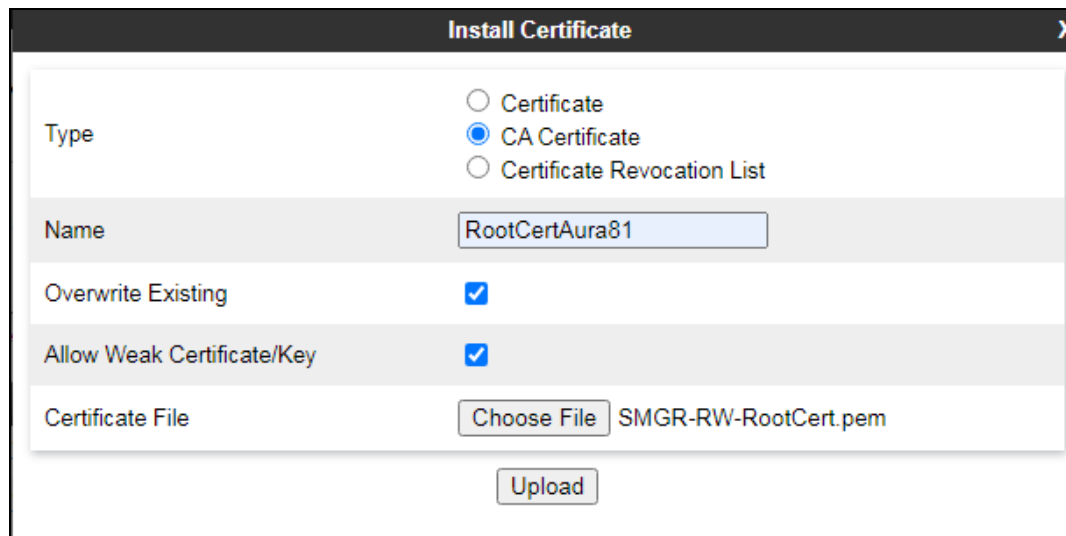
Click **Download as PEM**.



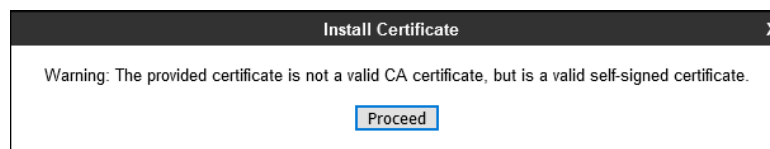
Save the .pem file to the local PC, e.g., **SystemManagerCA.pem** in the reference configuration.

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:

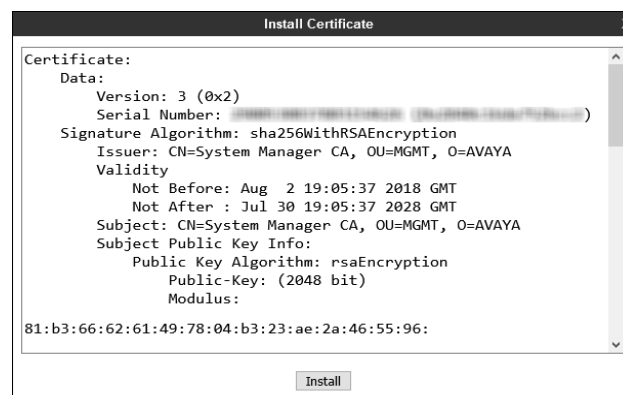
- **Type: CA Certificate.**
- **Name:** enter a descriptive name, e.g., **RootCertAura81.**
- Check the boxes for **Overwrite Existing** and **Allow Weak Certificate/Key.**
- Click **Browse** to select the System Manager CA certificate previously downloaded, in this case **SMGR-RW-RootCert.pem.**
- Click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

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
 Certificates
 Client Profiles
 Server Profiles
 SNI Group
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Certificates Install Generate CSR

Installed Certificates

SBCE_RW_Inside.pem	View Delete
SBCE_RW_Outside.pem	View Delete
sbcsectigo.crt	View Delete
724sect.crt	View Delete

Installed CA Certificates

AvayaDeviceEnrollmentCAchain.crt	View Delete
SMGR_RW_RootCert.pem	View Delete
sectigoCA.cer	View Delete

Installed Certificate Revocation Lists

No certificate revocation lists have been installed.

Installed Certificate Signing Requests

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).

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
 Certificates
 Client Profiles
 Server Profiles
 SNI Group
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Client Profiles: Client-Outside Add Delete

Client Profiles

- Client-INSIDE
- Client-Outside**

Client Profile

Click here to add a description.

TLS Profile

Profile Name	Client-Outside
Certificate	724sect.crt
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	sectigoCA.cer
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

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**.

The screenshot shows the 'Edit Profile' dialog box. At the top, there is a warning message: 'WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.' Below this, there is a section for 'TLS Profile' with fields for 'Profile Name' (set to 'Client-INSIDE'), 'Certificate' (set to 'SBCE_RW_Inside.pem'), and 'SNI' (unchecked). The 'Certificate Verification' section shows 'Peer Verification' set to 'Required', 'Peer Certificate Authorities' with a list containing 'AvayaDeviceEnrollmentCAchain.crt', 'SMGR_RW_RootCert.pem', and 'sectigoCA.cer', 'Peer Certificate Revocation Lists' (empty), 'Verification Depth' set to '1', 'Extended Hostname Verification' (unchecked), and 'Server Hostname' (empty).

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

The screenshot shows the 'Edit Profile' dialog box. The 'Renegotiation Parameters' section has 'Renegotiation Time' set to '0' seconds and 'Renegotiation Byte Count' set to '0'. The 'Handshake Options' section has 'Version' set to 'TLS 1.2' (checked), 'Ciphers' set to 'Default' (selected), and 'Value' set to 'HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH'. There are 'Back' and 'Finish' buttons at the bottom.

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.

Server Profiles: Server-Outside

Add

Delete

Server Profiles

Server-INSIDE

Server-Outside

Click here to add a description.

Server Profile

TLS Profile

Profile Name

Server-Outside

Certificate

724sect.crt

SNI Options

None

Certificate Verification

Peer Verification

None

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

Renegotiation Byte Count

0

Handshake Options

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**.

Edit Profile [X]

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile

Profile Name:

Certificate:

SNI Options:

SNI Group:

Certificate Verification

Peer Verification:

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

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

©2022 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 DevConnect Program at devconnect@avaya.com.