Avaya Solution & Interoperability Test Lab

Configuring Avaya Aura® Conferencing 7.0 Co-Resident Simplex Server with TLS and the Document Conversion Server with SSL Certificates with Avaya Aura® Solution for Midsize Enterprise 6.2 Server Issue – 1.0

Abstract

These Application Notes describe the configuration steps required to administer Transport Layer Security on the Avaya Aura® Conferencing 7.0 Co-Resident Simplex Server. The Application Notes also identifies how to configure Secure Socket Layer SSL Certificates on the Document Conversion Server. The Application Note also describes how to administer Avaya Aura® Solution for Midsize Enterprise with Avaya Aura® Conferencing 7.0 Co-Resident Simplex Server.
Table of Contents

1. Introduction .................................................................................................................. 4
2. Interoperability Tests ................................................................................................. 4
   2.1. Test Description and Coverage .............................................................................. 4
      2.1.1. Web Collaboration Agent ............................................................................ 4
      2.1.2. Managing Conference Features .................................................................. 4
      2.1.3. Managing Dialpad Features ....................................................................... 5
      2.1.4. Sharing Information ..................................................................................... 5
      2.1.5. Test Results ................................................................................................. 5
3. Reference Configuration .............................................................................................. 6
4. Equipment and Software Validated .............................................................................. 8
5. Administer Avaya Aura® Communication Manager Server ........................................ 9
   5.1. Verify OPS Capacity ............................................................................................ 9
   5.2. Administer Dial Plan .......................................................................................... 10
   5.3. Administer IP Node-Name ................................................................................ 10
   5.4. Administer Signaling Group .............................................................................. 11
   5.5. Administer Trunk Group ................................................................................... 12
   5.6. Administer Calling Party Number Information .................................................. 12
   5.7. Administer Route Selection .............................................................................. 12
   5.8. Administer IP Network Region ......................................................................... 13
   5.9. Administer IP Codec Set .................................................................................. 14
   5.10. Verify Off PBX Telephone Station Mapping ...................................................... 14
   5.11. Administer Station Screen ............................................................................... 15
   5.12. Save Translations ............................................................................................. 15
6. Administer Avaya Aura® System Manager ................................................................. 16
   6.1. Access Avaya Aura® System Manager ............................................................... 16
   6.2. Administer SIP Domain ..................................................................................... 17
   6.3. Add Location ..................................................................................................... 18
   6.4. Administer Avaya Aura® Session Manager SIP Entity ........................................ 19
   6.5. Administer Avaya Aura® Communication Manager Server SIP Entity ................ 21
   6.6. Administer Avaya Aura® Conferencing SIP Entity ............................................ 22
   6.7. Administer SIP Entity Link ................................................................................ 23
   6.8. Administer Routing Policy ................................................................................ 24
   6.9. Administer Dial Pattern ..................................................................................... 25
   6.10. Administer Avaya Aura® Session Manager ....................................................... 26
   6.11. Administer Avaya Aura® Communication Manager as a Managed Element .... 28
   6.13. Administer Avaya Aura® Communication Manager Server Application Sequence 31
   6.14. Synchronize Avaya Aura® Communication Manager Data ................................ 33
   6.15. Add SIP User .................................................................................................... 34
   6.16. Access Conferencing Element Manager Console ............................................. 39
7. Configure TLS Certificates on AAC70 Network Elements ......................................... 41
   7.1. Generate Certificates for the Element Manager ............................................... 41
7.2. Generate Certificates for the Provisioning Manager ........................................... 41
7.3. Generate Certificates for the Personal Agent within the Provisioning Manager .... 42
7.4. Generate Certificates for the Application Server ............................................... 43
7.5. Generate Certificates for the Media Server .................................................... 43
7.6. Generate Certificates for the Web Conferencing Server .................................. 43
7.7. Generate Certificates for the Web Conferencing Manager Server .................... 44
7.8. Assign Certificates to the Element Manager ..................................................... 45
7.9. Assign Certificates to the Provisioning Manager ............................................... 46
7.10. Assign Certificates to the Application Server ................................................ 47
7.11. Assign Certificates to the Media Server ....................................................... 48
7.12. Assign Certificates to the Web Conferencing Server ..................................... 49
7.13. Assign Certificates to the Web Conferencing Management Server ................. 50
8. Generate SSL/TLS Certificates for the Documentation Conversion Server .......... 51
  8.1. Access OpenSSL on Avaya Aura Conferencing .............................................. 51
  8.2. Generate a Private Key ...................................................................................... 51
  8.3. Generate a Certificate Signing Request .......................................................... 52
  8.4. Generate a Certificate Chain File .................................................................... 52
  8.5. Generate a PKCS#12 File .............................................................................. 57
  8.6. Remove the Passphrase Key file ...................................................................... 57
  8.7. Importing Certificate from a Third Party CA ............................................... 57
  8.8. Importing CA Certificate from a Third Party CA .......................................... 59
  8.9. Add the System Manager CA Certificate to User IE Browser ......................... 60
9. Configuring SSL/TLS Certificates on the Documentation Conversion Server .... 63
  9.1. Access the Documentation Conversion Server ............................................... 63
  9.2. Documentation Conversion Server Certificates ............................................. 63
  9.3. Configure the HTTPD.Conf File ................................................................. 64
  9.4. Configure the Config.php File ...................................................................... 65
  9.5. Configure Documentation Conversion Server on Element Manager Console .. 66
10. Configuring Avaya Flare Experience on windows client .................................... 67
11. Verification Steps ............................................................................................... 68
12. Conclusion ......................................................................................................... 73
13. Additional References ....................................................................................... 73
1. **Introduction**

These Application Notes describe the configuration steps required to administer Transport Layer Security on the Avaya Aura® Conferencing 7.0 Co-Resident Simplex Server. The Application Notes also identifies how to configure Secure Socket Layer Certificates on the Document Conversion Server. The Application Note also describes how to administer Avaya Aura® Solution for Midsize Enterprise with Avaya Aura® Conferencing 7.0 Co-Resident Simplex Server. This Application Note assumes that the installation of the Linux Operating System patches and Avaya Aura Conferencing 7.0 Application software has been completed.

The Application Note will also describe the administration of an Avaya Flare Experience on windows client as a SIP user on Avaya Aura® System Manager. It will detail configuring a conference profile to allow a SIP user access to Web Collaboration Agent while joined to a Meet Me Conference from the Avaya Flare Experience on windows client. The Avaya Flare Experience on windows client endpoint is used to open Web Collaboration Agent as a provisioned user and start the Web Collaboration Agent from the client. With Web Collaboration Agent opened through the Avaya Flare Experience client the user can access a Library folder and upload the relevant documents and share these documents with the participants in the Meet Me conference.

2. **Interoperability Tests**

The following sections describe the test scenario that were used in to verify the functionality Avaya Conferencing and the Documentation Conversion Server through Web Collaboration Agent with Avaya Flare Experience on windows SIP client.

2.1. **Test Description and Coverage**

This section provides an overview of the test cases performed after the installation and configuration Avaya Conferencing and the Documentation Conversion Server through Web Collaboration Agent with Avaya Flare Experience on windows SIP client.

2.1.1. **Web Collaboration Agent**

The following Basic Web Collaboration Agent Features were tested:

- Log into a Conference as a Moderator
- Log into a Conference as a Participant
- Log into a Conference as a Guest

2.1.2. **Managing Conference Features**

The following Managing Conference Features were tested:

- Adding a Participant to a Conference
- Silence and Unsilence participants
- Promote a Participant to Moderator
- Clearing Raised Hands
• Assigning and Un-assigning Presenter Capabilities to Participants
• Searching for Users

2.1.3. Managing Dialpad Features
The following Dialpad Features were verified:
• Set Moderator
• Raise Hand/Lower Hand
• Count Participants
• Enable/Disable Lecture Mode
• Lock/Unlock Conference
• End Conference

2.1.4. Sharing Information
The following sharing features were verified using Web Collaboration Agent with Avaya Flare Experience on windows SIP client.
• Upload documents through Web Collaboration Agent.
• Navigate Documents through Web Collaboration Agent.
• View Documents within the Library.
• Share Documents to participants with Web Collaboration Agent.

2.1.5. Test Results
All test cases passed. The following are the observations for the Avaya Flare Experience on windows SIP client:
• Microsoft Office 2010 or later is required to convert Microsoft Office Documents.
• DNS Routing is required for the Documentation Conversion Server.
• The macros needed to be disabled on Microsoft Word and PowerPoint.
3. Reference Configuration
The configuration used in these Application Notes is shown in Figure 1.

The Avaya Aura® Conferencing software is installed and configured on mcp core Linux 15.1.1 Operating System installed on a S8800 Server. The Avaya Aura® Conferencing Co-resident Simplex Server contains the Application Server, the Media Server and the Web Conferencing Server all on the one Server. The Avaya Aura® Conferencing Server provides audio, web and video conferencing and control from the co-resident Server.

The Documentation Conversion Server is installed on Microsoft Windows Server 2008 R2 Operating System. The Document Conversion Server allows Word and PowerPoint documents to be uploaded within a meet me conference and shared and view by the participants within the conference.

Avaya Aura® Solution for Midsize Enterprise is installed on Avaya System Platform on a S8800 Server. Avaya Aura® Solution for Midsize Enterprise contains Avaya Aura® System Manager, Avaya Aura® Session Manger and Avaya Aura® Communication Manger as virtual machines running with the Avaya Aura® Solution for Midsize Enterprise. Avaya Aura® Communication Manager running as an Evolution Server is used for Off-PBX Station Mapping (OPS).

The diagram indicates logical signaling connections. All components in the Corporate LAN are physically connected to a single Avaya Ethernet Routing Switch (ERS) 2550T-PWR, and are administered in subnet range 192.168.1.x. The Avaya Flare Experience on windows SIP client are endpoints that register to the Avaya Aura® Session Manger. These endpoints are used to launch the Web Collaboration Agent Application. The Web Collaboration Agent is an application that provides tools for managing and participating in conferences for the purpose on sharing documents.
Figure 1 Avaya Conferencing Server with DCS Server
4. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Avaya Aura®</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8800 Server</td>
<td>Avaya Aura® Conferencing R7.0 Release 15.0.18.1 Update: Service Pack 2 Patch 1</td>
</tr>
<tr>
<td>Avaya S8800 Server</td>
<td>Avaya Aura® Solution for Midsize Enterprise R6.2 Release 6.2.0.0.3105 Update: Service Pack 3</td>
</tr>
<tr>
<td>Avaya S8800 Server</td>
<td>Avaya Aura® System Manager R6.2 Release 6.2.15.1.1959 Update: Service Pack 3</td>
</tr>
<tr>
<td>Avaya S8800 Server</td>
<td>Avaya Aura® Session Manager R6.2 R6.2.3.0.623006 Update: Service Pack 3</td>
</tr>
<tr>
<td>Avaya S8800 Server</td>
<td>Avaya Aura® Communication Manager R16x.02.0.823.0.20199 Update: Service Pack 4</td>
</tr>
<tr>
<td>Avaya S8800 Server</td>
<td>Document Conversion Server Release 15.0.18.1 Update: Service Pack 2 Patch 1</td>
</tr>
<tr>
<td>Avaya Flare Experience on IPAD</td>
<td>Avaya Flare Experience on IPAD Release 1.1</td>
</tr>
<tr>
<td>Avaya Flare Experience on Windows</td>
<td>Avaya Flare Experience on Windows Release 1.1.0.5</td>
</tr>
</tbody>
</table>
5. Administer Avaya Aura® Communication Manager Server

This section highlights the important commands for administering a SIP Trunk and Signaling Group to carry calls made to the Conferencing Meet Me number. It will also cover the commands required for defining the Flare Experience on windows SIP client as an Off-PBX Station (OPS) These steps will also document the licensing settings required to configure the Conferencing Server with Communication Manager.

5.1. Verify OPS Capacity

Use the `display system-parameters customer-options` command to verify that the required software licenses have been enabled. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to obtain additional capacity. On Page 4 the Multimedia Call Handling (Basic) value was set to Yes. The Multimedia Call Handling (Enhanced) value was also set to Yes. The Multimedia IP SIP Trunking value was also set to Yes.

<table>
<thead>
<tr>
<th>Display Command</th>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Emergency Access to Attendant? y</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Enable 'admin' Login? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enhanced Conferencing? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enhanced EC500? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Survivable Server? n</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise Wide Licensing? n</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ESS Administration? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Extended Cvg/Fwd Admin? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Five Port Networks Max Per MCC? n</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forced Entry of Account Codes? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Global Call Classification? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hospitality (Basic)? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hospitality (G3V3 Enhancements)? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Trunks? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Stations? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISDN Feature Plus? n</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISDN/BRI Trunks? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISDN-PRI? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local Survivable Processor? n</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malicious Call Trace? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Media Encryption Over IP? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mode Code for Centralized Voice Mail? n</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multifrequency Signaling? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multimedia Call Handling (Basic)? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multimedia Call Handling (Enhanced)? y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Multimedia IP SIP Trunking? y</td>
<td></td>
</tr>
</tbody>
</table>

On Page 19 of the system-parameters features page the Direct IP-IP Audio Connections value was set to Yes. The IP Audio Hairpinning value was set to No. The SIP Endpoint Managed Transfer value was set to Yes.
On Page 2 of the system-parameters ip-options page the Override ip-codec-set for SIP direct-media connections was set to Yes.

<table>
<thead>
<tr>
<th>Display System-parameters Ip-options</th>
<th>Page 2 of 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-Options System Parameters</td>
<td></td>
</tr>
<tr>
<td>Force Phones and Gateways to Active Survivable Servers? n</td>
<td>Override ip-codec-set for SIP direct-media connections? y</td>
</tr>
</tbody>
</table>

5.2. Administer Dial Plan

This section describes the Dial Plan Analysis screen. This is Communication Manager’s way of translating digits dialed by the user. The user can determine the beginning digits and total length for each type of call that Communication Manager needs to interpret. The Dialed String beginning with the number 7 and with a Total Length of 5 digits was used to administer the extension range used for the Flare Experience SIP client. The Call Type was set to ext for extension. The Dialed String beginning with the number 8 with a Total length of 5 was used for the Meet Me number with call type aar to route using the aar table (See Section 5.7) to join a Conference.

<table>
<thead>
<tr>
<th>Display Dialplan Analysis</th>
<th>Page 1 of 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIAL PLAN ANALYSIS TABLE</td>
<td></td>
</tr>
<tr>
<td>Location: all Percent Full: 1</td>
<td></td>
</tr>
<tr>
<td>Dialed String Total Call Dialed String Total Call Dialed String Total Call</td>
<td>Dialed String Total Call Dialed String Total Call Dialed String Total Call</td>
</tr>
<tr>
<td>1 3 dac</td>
<td></td>
</tr>
<tr>
<td>2 5 aar</td>
<td></td>
</tr>
<tr>
<td>3 5 ext</td>
<td></td>
</tr>
<tr>
<td>35 5 aar</td>
<td></td>
</tr>
<tr>
<td>5 5 aar</td>
<td></td>
</tr>
<tr>
<td>60 4 aar</td>
<td></td>
</tr>
<tr>
<td>7 5 ext</td>
<td></td>
</tr>
<tr>
<td>8 5 aar</td>
<td></td>
</tr>
<tr>
<td>* 2 fac</td>
<td></td>
</tr>
</tbody>
</table>

5.3. Administer IP Node-Name

This section describes IP Node-Name. This is where Communication Manager assigns the IP Address and node-name to Session Manager. In the example below the node-name is SessionM1 and the IP Address is 192.168.1.87. The Communication Manager Server automatically populates a processor node name to the IP Address of Communication Manager Server. This node name is procr with IP Address 192.168.1.82.

<table>
<thead>
<tr>
<th>List Node-Names All</th>
<th>NODE NAMES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Name</td>
</tr>
<tr>
<td>IP</td>
<td>EnterpriseCM</td>
</tr>
<tr>
<td>IP</td>
<td>SessionM1</td>
</tr>
<tr>
<td>IP</td>
<td>SessionM2</td>
</tr>
<tr>
<td>IP</td>
<td>BSM</td>
</tr>
<tr>
<td>IP</td>
<td>Default</td>
</tr>
<tr>
<td>IP</td>
<td>procr</td>
</tr>
</tbody>
</table>
5.4. Administer Signaling Group

This section describes the Signaling Group screen. The Group Type was set to sip and the Transport Method was set to tls. Since the Flare Experience on windows SIP client is using a Communication Manager Server for Off Pbx Station Mapping the IMS Enabled setting must be set to n. Since the SIP trunk is between Communication Manager Server and Session Manager the Near-end Node Name is the node name of the “procr” of the Communication Manager Server. The Far-end Node Name is the node name of the Session Manager Server. This is SessionM1. The Near-end Listen Port and Far-end Listen Port are both set to port number 5061. The Far-end Network-Region was set to 1. The Direct IP-IP Audio Connections was set to Yes. The IP Audio Hairpinning value was set to No. The Initial IP-IP Direct Media value was set to Yes.

```
display signaling-group 120

SIGNALING GROUP

Group Number: 120
Group Type: sip
IMS Enabled? n
Transport Method: tls
Q-SIP? n
IP Video? y
Priority Video? n
Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y
Peer Server: SM

Near-end Node Name: procr
Far-end Node Name: SessionM1
Near-end Listen Port: 5061
Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Domain:

Bypass If IP Threshold Exceeded? n
RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload
Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3
IP Audio Hairpinning? n
Enable Layer 3 Test? n
Initial IP-IP Direct Media? Y
H.323 Station Outgoing Direct Media? n
Alternate Route Timer(sec): 6
```
5.5. Administer Trunk Group

This section describes the **Trunk Group** used to carry a call made to the meet me conference on the Flare Experience on windows SIP client. Trunk Group 120 was configured as a SIP Trunk with the **Group Type** set to sip. The trunk **Group Name** was set as To ASM. The **Direction** of the calls was set to two-way as there will be calls to and from the Flare Experience on windows SIP client. The **Service Type** was set to tie as the trunk is an internal trunk between Communication Manager Server and Session Manager. The **Signaling Group** number assigned to this trunk is 120. The **Number of Members** assigned to this trunk group is 100. All other fields on this page are left as default.

### display trunk-group 120

<table>
<thead>
<tr>
<th>Group Number: 3</th>
<th>Group Type: sip</th>
<th>CDR Reports: y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name: To ASM</td>
<td>COR: 1</td>
<td>TN: 1</td>
</tr>
<tr>
<td>Direction: two-way</td>
<td>Outgoing Display? n</td>
<td>Night Service:</td>
</tr>
<tr>
<td>Dial Access? n</td>
<td>Auth Code? N</td>
<td></td>
</tr>
<tr>
<td>Queue Length: 0</td>
<td>Member Assignment Method: auto</td>
<td></td>
</tr>
<tr>
<td>Service Type: tie</td>
<td>Signaling Group: 120</td>
<td></td>
</tr>
<tr>
<td>Number of Members: 100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.6. Administer Calling Party Number Information

Use the **change private-numbering 0** to add an **Extension Code** of 5 with **Extension Length** of 7 and 8. The **Total Length** of the CPN number was 5.

### change private-numbering 0

<table>
<thead>
<tr>
<th>Ext Ext Len Code</th>
<th>Trk Grp(s)</th>
<th>Private Prefix</th>
<th>Total Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 5</td>
<td></td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>8 5</td>
<td></td>
<td>5</td>
<td>Total Administered: 2</td>
</tr>
</tbody>
</table>

5.7. Administer Route Selection

Use the **change aar analysis 8** to administer the automatic alternate route selection to route calls between the Communication Manager to Session Manager. Calls to the Meet Me conference number beginning with 8 that are a **minimum** of 5 digits and a **maximum** of 5 digits in length are sent to routing pattern 120. The **Call Type** was set to unk u.
Use the change route-pattern 120 to add trunk group 120 to route pattern 120. Ensure the Secure SIP value was set to No.

<table>
<thead>
<tr>
<th>Grp</th>
<th>FRL</th>
<th>NPA</th>
<th>Pfx</th>
<th>Hop</th>
<th>Toll No.</th>
<th>Inserted</th>
<th>DCS/IXC</th>
<th>QSIG</th>
<th>Digits</th>
<th>Intw</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>120</td>
<td>0</td>
<td>n</td>
<td>user</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:</td>
<td></td>
<td></td>
<td>n</td>
<td>user</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 5.8. Administer IP Network Region

This section describes **IP Network Region** screen. It was decided to place all the Flare Experience on windows SIP client in network region 1. The **Authoritative Domain** must mirror the domain name of Session Manager. This was *silstack.com*. The codec used on the SIP endpoints were placed in **Codec Set 1**. IP Shuffling was turned on so both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** were set to **yes**.

```plaintext
display ip-network-region 1
```

<table>
<thead>
<tr>
<th>Region: 1</th>
<th>Location: 1</th>
<th>Authoritative Domain: silstack.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEDIA PARAMETERS</td>
<td>Intra-region IP-IP Direct Audio: yes</td>
<td></td>
</tr>
<tr>
<td>Codec Set: 1</td>
<td>Inter-region IP-IP Direct Audio: yes</td>
<td></td>
</tr>
<tr>
<td>UDP Port Min: 2048</td>
<td>IP Audio Hairpinning? n</td>
<td></td>
</tr>
<tr>
<td>UDP Port Max: 3329</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIFFSERV/TOS PARAMETERS</td>
<td>RTCP Reporting Enabled? y</td>
<td></td>
</tr>
<tr>
<td>Call Control PHB Value: 46</td>
<td>RTCP MONITOR SERVER PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Audio PHB Value: 46</td>
<td>Use Default Server Parameters? y</td>
<td></td>
</tr>
<tr>
<td>Video PHB Value: 26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.1P/Q PARAMETERS</td>
<td>AUDIO RESOURCE RESERVATION PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Call Control 802.1p Priority: 6</td>
<td>RSVP Enabled? n</td>
<td></td>
</tr>
<tr>
<td>Audio 802.1p Priority: 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video 802.1p Priority: 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.323 IP ENDPOINTS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.323 Link Bounce Recovery? y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idle Traffic Interval (sec): 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keep-Alive Interval (sec): 5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.9. Administer IP Codec Set

This section describes the IP Codec Set screen. IP Codec G.711MU, G.711A and G.729 were used for testing purposes with the Remote User SIP endpoints.

<table>
<thead>
<tr>
<th>Codec Set: 1</th>
<th>IP Codec Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Silence Frames Packet</td>
<td></td>
</tr>
<tr>
<td>Codec Suppression Per Pkt Size(ms)</td>
<td></td>
</tr>
<tr>
<td>1: G.711MU n 2 20</td>
<td></td>
</tr>
<tr>
<td>2: G.711A n 2 20</td>
<td></td>
</tr>
<tr>
<td>3: G.729 n 2 20</td>
<td></td>
</tr>
</tbody>
</table>

5.10. Verify Off PBX Telephone Station Mapping

This section show the off-pbx-telephone station-mapping. When A SIP User was added in Section 6.14 on System Manager it creates the off-pbx-telephone station mapping settings in Communication Manager. The Flare Experience on windows SIP client 70031 uses off pbx Application OPS which is used for SIP enabled telephones. The SIP Trunk Selection is set to aar. The Config Set which is the desired call treatment was set to 1.

<table>
<thead>
<tr>
<th>Station Extension</th>
<th>Appl</th>
<th>CC</th>
<th>Phone Number</th>
<th>Config Trunk Set</th>
<th>Mapping Select</th>
<th>Calls Allowed Mode</th>
<th>Calls Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>70031</td>
<td>OPS</td>
<td>70031</td>
<td>1 / aar</td>
<td>both</td>
<td>all</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On page 2 the Call Limit is set to 6 as shown below. This is the maximum amount of simultaneous calls for extension 70031. The Mapping Mode field was set to both in this configuration setup. This is used to control the degree of integration between the Remote User SIP telephones. The Calls Allowed field was set to all. This identifies the call filter type for a SIP Phone. The Bridged Calls field was set to none as it was not needed for testing purposes.

<table>
<thead>
<tr>
<th>Station Extension</th>
<th>Appl</th>
<th>Call Limit</th>
<th>Mapping Mode</th>
<th>Calls Allowed</th>
<th>Bridged Calls</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>70031</td>
<td>OPS</td>
<td>6</td>
<td>both</td>
<td>all</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>
5.11. Administer Station Screen

This screen describes the station form setup for the Flare Experience on windows SIP client on Communication Manager. The Extension used was 70031 with phone Type 9640SIP. The Name of the phone was set to 70031, 70031 and all other values on Page 1 of the station form were left as default.

```
display station 70031

STATION

Extension: 70031
Type: 9640SIP
Port: S00010
Name: 70031, 70031

STATION OPTIONS

Lock Messages? n
BCC: 0
Security Code: TN: 1
Coverage Path 1: COR: 1
Coverage Path 2: COS: 1
Hunt-to Station:

Time of Day Lock Table:
Loss Group: 19
Personalized Ringing Pattern: 1
Message Lamp Ext: 40030
Speakerphone: 2-way
Mute Button Enabled? y
Display Language: english
Expansion Module? n
Survivable GK Node Name:
Survivable COR: internal
Survivable Trunk Dest? y

Media Complex Ext:
IP SoftPhone? n
IP Video? n
```

The SIP Trunk value was set to aar on Page 6 of the station form.

```
add station 70031

STATION

SIP FEATURE OPTIONS

Type of 3PCC Enabled: None

SIP Trunk: aar
```

5.12. Save Translations

Use the save translation command to save these changes.

```
save translation

SAVE TRANSLATION

Command Completion Status          Error Code
Success                          0
```
6. Administer Avaya Aura® System Manager

This following section describes administering SIP Entities between Session Manager and the Communication Manager Server in order to establish a SIP Entity link between Session Manager and the Communication Manager Server. It also discusses administering the SIP Entities between Session Manager and the Conferencing Server. This section discusses administering a SIP user with a conferencing profile to allow the Avaya Flare Experience on windows client SIP client start Web Collaboration Agent for the purpose of uploading and sharing documents. This Application Note assumes that single sign on for the Conferencing Element Manager on System Manager has been completed as documented in Reference 1 in Section 13. This Application Note also assumes the meet me number has been administered in the Conferencing Provisioning Client. The concluding steps of this section describe accessing the Conferencing Element Manager Console through with System Manager with single sign on.

6.1. Access Avaya Aura® System Manager

Access the System Manager web interface, by entering http://<ip-addr>/SMGR as the URL in an Internet browser, where <ip-addr> is the IP address of the server running System Manager graphical user interface. Log in with the appropriate User ID and Password and press the Log On button to access System Manager.

![Avaya Aura® System Manager 6.2](image)

Recommended access to System Manager is via FCMN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on
The main menu of the System Manager Graphical User Interface is displayed in the following screenshot. Under Elements select Routing.

6.2. Administer SIP Domain

The following screenshot shows the configuration used to add a SIP Domain. Under the heading Routing on the left hand side of the system management interface of System Manager, access the sub heading Domains. The name of the SIP Domain used in Session Manager silstack.com was added. The Type was set to sip. Press the Commit button to add the SIP Domain.
### 6.3. Add Location

To add a new Location, click on **Routing** and access the **Locations** sub heading. A location **Name** Galway Stack was added to the Session Manager. The **Default Audio Bandwidth** was set to 80Kbit/sec. The **Commit** button was pressed to confirm changes. Locations are used to identify logical and physical locations where SIP entities reside for the purposes of bandwidth management or location based routing.

![Location Details](image)

Edit this new location record and scroll down the screen to the **Location Pattern** area. In the **Location Pattern** an IP Address Pattern for **192.168.1.x** was added. The 192.168.1.x is the subnet range used to connect the devices. The **Commit** button was pressed to add the IP Address Pattern to the Location.

![Location Pattern](image)
6.4. Administer Avaya Aura® Session Manager SIP Entity

Under **Routing** access the sub heading **SIP Entities**. The Session Manager SIP Entity is the first part of the link between Session Manager and the Communication Manager Server. The **Name** of the SIP Entity was **MESSM**. The **FQDN or IP Address** was set to **192.168.1.40**. This is the IP Address of the SIP Signaling Interface in the Session Manager Server. The **Type** was set to **Session Manager**. The **Location** was set to **Galway Stack**, the **Time Zone** set to **Europe/Dublin** and the **SIP Link Monitoring** was set to Use Session Manager Configuration. Press the **Commit** button.
The following screenshot shows what **Port** settings need to be configured for the SIP Entity. With the signaling protocol being set to **TLS** port **5061** was used in the SIP Entity SIP trunk. Press the **Commit** button.
6.5. Administer Avaya Aura® Communication Manager Server SIP Entity

The Evolution Server SIP Entity is the second part of the link between the Session Manager and the Communication Manager Server. The Name of the SIP Entity was MESCM. The FQDN or IP Address was set to 192.168.1.82 which was the IP Address of the Communication Manager Server. The Type was set to CM for Communication Manager. The Location was set to Galway Stack and the SIP Link Monitoring was set to Use Session Manager Configuration. Press the Commit button.
6.6. Administer Avaya Aura® Conferencing SIP Entity

The following describes the Conferencing SIP Entity to the Session Manager. The Name of the SIP Entity was AAC70. The FQDN or IP Address was set to 192.168.1.115 which was the IP Address of the Application Server component. The Type was set to Conferencing for Conferencing. The Location was set to Galway Stack and the Time Zone was set to Europe/Dublin.

Under SIP Link Monitoring heading. The SIP Link Monitoring setting was set to Use Session Manager Configuration. The Supports Call Admission Control was enabled. The Shared Bandwidth Manager settings were also enabled. The Primary Session Manager Bandwidth Association setting was set to MESSM. The Commit button was pressed to confirm the changes.
6.7. Administer SIP Entity Link

To administer the SIP Entity link access the sub heading **Routing → Entity Links** on the left hand side of the Session Manager GUI. Select the **New** button.

The SIP Entity Link shown below is the link between Session Manager and the Communication Manager Server. The Name of the Entity Link was **SMONE-MESCM**. The SIP Entity 1 was set to **Session Manager One**. The Protocol was **TLS** and the Port was **5061**. The SIP Entity 2 was set to **MESCM**.

The SIP Entity Link shown below is the link between Session Manager and the Messaging Server. The Name of the Entity Link was **SMONE-AAC70**. The SIP Entity 1 was set to **Session Manager One**. The Protocol was **TLS** and the Port was **5061**. The SIP Entity 2 was set to **AAC70**.
6.8. Administer Routing Policy

To administer the Routing Policy in System Manager Select Elements → Routing → Routing Policy → New.

Under the Routing Policy details section. The Routing Policy Name was set to AAC70. The Routing Policy with IP Address as 192.168.1.115 for AAC70 was selected as the Routing Policy. The Commit button was selected to commit the changes.
6.9. Administer Dial Pattern

Under **Dial Patterns** add the **Pattern** for **80956** (the meet me extension) with a **minimum** length of 5 digits a **maximum** length of 5 digits with a **SIP Domain** as **silstack.com** and **Originating Location** as **Galway Stack**.

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Min</th>
<th>Max</th>
<th>Emergency Call</th>
<th>SIP Domain</th>
<th>Originating Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>80956</td>
<td>5</td>
<td>5</td>
<td></td>
<td>silstack.com</td>
<td>Galway Stack</td>
</tr>
</tbody>
</table>
6.10. Administer Avaya Aura® Session Manager

In order to provide the link between Session Manager and System Manager, Session Manager must be added to the configuration. Under the Session Manager heading on the left hand side of the System Manager GUI click on the Session Manager Administration sub heading. Under the Session Manager Instances select the New button.
The **SIP Entity Name** was set to **Session Manager One**. The **Management Access Point** was set to **192.168.1.35**. This is the management IP Address for the server running Session Manager. The **SIP Entity IP Address** was set to **192.168.1.87**. This was the IP Address of the SIP Signaling Interface in Session Manager. The **Network Mask** was set to **255.255.255.224** and the **Default Gateway** was set to **192.168.1.33**.

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIP Entity Name</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Management Access Point Host Name/IP</strong></td>
</tr>
<tr>
<td><strong>Direct Routing to Endpoints</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Module</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIP Entity IP Address</strong></td>
</tr>
<tr>
<td><strong>Network Mask</strong></td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
</tr>
<tr>
<td><strong>Call Control PHB</strong></td>
</tr>
<tr>
<td><strong>QOS Priority</strong></td>
</tr>
<tr>
<td><strong>Speed &amp; Duplex</strong></td>
</tr>
</tbody>
</table>
6.11. Administer Avaya Aura® Communication Manager as a Managed Element

In order for Communication Manager to supply configuration and feature support to the Flare Experience on windows SIP client as a Remote User when it registers to Session Manager, Communication Manager must be added as an application. Under the Inventory heading on the left hand side of the System Manager GUI access the Manage Elements sub heading. Under Elements select the New button.

The Manage Element Name was MESCM. The Type was set to Communication Manager. The Node IP Address was set to 192.168.1.82.
Access the **Attributes** section and set the **Login**. This was the login used to access the Communication Manager Evolution Server. The **Password** was set to the password used to access the Communication Manager Evolution Server. The **Port** was set to **5022**.

```
<table>
<thead>
<tr>
<th>Attributes</th>
<th><img src="image" alt="Attributes" /></th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Login</em></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>••••••</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>••••••</td>
</tr>
<tr>
<td>Is SSH Connection</td>
<td>✔</td>
</tr>
<tr>
<td><em>Port</em></td>
<td>5022</td>
</tr>
<tr>
<td>Alternate IP Address</td>
<td></td>
</tr>
<tr>
<td>RSA SSH Fingerprint (Primary IP)</td>
<td></td>
</tr>
<tr>
<td>RSA SSH Fingerprint (Alternate IP)</td>
<td></td>
</tr>
<tr>
<td>Is ASG Enabled</td>
<td></td>
</tr>
</tbody>
</table>
```
6.12. Administer Avaya Aura® Communication Manager Server Application

To configure the Communication Manager Evolution Server Application access **Session Manager** → **Application Configuration** → **Applications**. Under **Application Entries**, select the New button.

The Name of the Application was MESCM. The SIP Entity used was MESCM. The CM System for SIP Entity used was MESCM. The Description of the Application was MESCM.
6.13. Administer Avaya Aura® Communication Manager Server Application Sequence

To configure the Communication Manager Evolution Server Application Sequence access the Session Manager heading on the left hand side System Manager GUI. Access the sub heading Application Configuration → Application Sequences.
The Evolution Server Application Sequence Name was added as MESCM. The Description field was set to MESCM. Under the Available Applications field select the plus button to the left of the MESCM Name. This will then populate MESCM in the Application in this Sequence field. Select the Commit button to save the changes.
6.14. Synchronize Avaya Aura® Communication Manager Data

To synchronize the Communication Manager Data access **Inventory → Synchronization → Communication System** heading on the left hand side of the System Manager GUI. Access the sub heading **Communication System**. The following screenshot shows the MESCM, the Communication Manager Evolution Server synchronized to the Session Manager by highlighting the **Initialize data for the selected devices** option and selecting the **Now** key.

![Synchronization screenshot](image)
6.15. Add SIP User

To add a SIP User to Session Manager, access the User Management → Manage Users heading on the left hand side of the System Manager GUI. Select the New button to add a new SIP User to Session Manager.

Select the Identity sub heading. The Last Name was set to 70031 and First Name was set to 70031. The Login Name was set to 70031@silstack.com. The Authentication Type was set to Basic.
Next, click on the **Communication Profile** Tab. Select the **Communication Profile** subheading. The **Communication Profile Password** was set. This will match the Flare Experience on windows user password on Login to the client. Select the **Done** button to save the changes.

![Communication Profile](image)

Select the **Communication Address** heading. The **Type** was set to **Avaya E.164**. The **Fully Qualified Address** was set to `+35391770031@silstack.com`. The **Add** button was pressed to save the changes.

![Communication Address](image)
Select **Session Manager Profile** heading was selected. The **Primary Session Manager** was set to **MESSM**. This equates to the Session Manager SIP entity. The **Origination Application Sequence** was set to **MESCM**. The **Termination Application Sequence** was set to **MESCM**. The **Home Location** was set to **Galway Stack**.

In order for the Station Profile template information to be pushed from the Session Manager down to the Communication Manager Evolution Server, **enable the CM Endpoint Profile** box. The **System** was set to **MESCM**. This is the Communication Manager Server Element Name. The **Extension** was set to **70031** and the **Template** and **Set Type** was set to **9640SIP**.
Click on **Endpoint Editor** and under **Feature Options** the settings were left as default.

Within **Button Assignments** a value of 6 **call-appr** buttons were set. The **Done** button was pressed.
The Conferencing Profile parameter was selected. The Auto Generate Participant and Moderator Security Codes setting was enabled. The Location field was set to Galway Stack. The Get Template button was selected.

The executive template was selected from the drop down template menu.

Press Commit to save the changes.
6.16. Access Conferencing Element Manager Console

To access the Conferencing Element Manager Console under the Elements heading on the System Manager GUI select the Conferencing section.

The following page is displayed

![Conferencing Dashboard](image)

Select the Single sign on Name called AAC-EM.

![Conferencing Dashboard](image)

This will direct to the Single sign on page for Element Manager Console. Type in the **Login** and **Password** and select the **Log On** button.
The user gets directed to the Element Manager Console access page. Select the **Connect** button to connect to the Element Manager Console.

The following page is displayed.
7. Configure TLS Certificates on AAC70 Network Elements

The Conferencing Server uses the Transport Layer Security protocol to prevent eavesdropping and tampering of communications sent across a network. This section describes the Transport layer security certificates needed to be generated and assigned to each network element in the Conferencing Server.

7.1. Generate Certificates for the Element Manager

To generate transport layer security certificates to the Element Manager access the Security ➔ Certificate Management ➔ Enrollment Request heading on the Element Manager Console.

The Logical Name for Provisioning Manager was EMConsoleCertTLS. The Bit length was set to 1024. The Common name was set to emoam.silstack.com. The Enrollment password must match the enrollment password configured on the System Manager during the System Manager install. The Submit button was selected to confirm the changes.

7.2. Generate Certificates for the Provisioning Manager

To generate transport layer security certificates to the Provisioning Manager access the Security ➔ Certificate Management ➔ Enrollment Request heading on the Element Manager Console. The Logical Name for Provisioning Manager was ProvIntOAMCertTLS. The Common name was set to aac70.silstack.com. The Bit length was set to 1024. The Enrollment password must match the enrollment password configured on the System Manager during the System Manager install. The Submit button was selected to confirm the changes.
7.3. Generate Certificates for the Personal Agent within the Provisioning Manager

To generate transport layer security certificates for the Personal Agent within the Provisioning Manager access the Security ➔ Certificate Management ➔ Enrollment Request heading on the Element Manager Console. The Logical Name for Provisioning Manager was ProvPACertTLS. The Common name was set to 135.64.186.112. The Bit length was set to 1024. The Enrollment password must match the enrollment password configured on the System Manager during the System Manager install. The Submit button was selected to confirm the changes.
7.4. Generate Certificates for the Application Server

To generate transport layer security certificates for the Application Server access the Security → Certificate Management → Enrollment Request heading on the Element Manager Console. The Logical Name for the Application Server was ASIntOAMCertTLS. The Common name was set to 192.168.1.115. The Bit length was set to 1024. The Enrollment password must match the enrollment password configured on the System Manager during the System Manager install. The Submit button was selected to confirm the changes.

7.5. Generate Certificates for the Media Server

To generate transport layer security certificates for the Media Server access the Security → Certificate Management → Enrollment Request heading on the Element Manager Console. The Logical Name for the Media Server was MediaSIPCertTLS. The Common name was set to 192.168.1.116. The Bit length was set to 1024. The Enrollment password must match the enrollment password configured on the System Manager during the System Manager install. The Submit button was selected to confirm the changes.

7.6. Generate Certificates for the Web Conferencing Server

To generate transport layer security certificates for the Web Conferencing Server access the Security → Certificate Management → Enrollment Request heading on the Element Manager Console. The Logical Name for the Web Conferencing Server was WebCollServCertTLS. The
Bit length was set to 1024. The Common name was set to wcs.silstack.com. The Enrollment password must match the enrollment password configured on the System Manager during the System Manager install. The Submit button was selected to confirm the changes.

7.7. Generate Certificates for the Web Conferencing Manager Server
To generate transport layer security certificates for the Web conferencing Manager Server access the Security -> Certificate Management -> Enrollment Request heading on the Element Manager Console. The Logical Name for the Web Conferencing Server was WebCollManCertTLS. The Bit length was set to 1024. The Common name was set to 192.168.1.117. The Enrollment password must match the enrollment password configured on the System Manager during the System Manager install. The Submit button was selected to confirm the changes.
### 7.8. Assign Certificates to the Element Manager

To assign transport layer security certificates to the Element Manager access **Feature Server Elements** → **Element Manager** heading on the Element Manager Console. Highlight the **Element Manager** section and select the **Edit** button.

![Element Manager Console](image)

The **Enable HTTP Port** setting was left unchecked. Under the **Internal OAM** section the HTTPS Certificate was set to **EMConsoleCertTLS**. The **Apply** button was selected to apply the changes.

![Edit EM](image)
7.9. Assign Certificates to the Provisioning Manager

To assign transport layer security certificates to the Provisioning Manager access Feature Server Elements ➔ Provisioning Managers heading on the Element Manager Console. Highlight the Provisioning Managers section and select the Edit button.

Under the Prov section the Enable HTTP Port setting was unchecked. The Internal OAM HTTPS Certificate was set to ProvIntOAMCertTLS. Under the PA section. The Enable HTTP Port was unchecked. The HTTPS Certificate was set to ProvIntOAMCertTLS. The Enable SIP TLS Port was checked. The SIP Certificate was set to ProvPA CertTLS. The Apply button was selected to apply the changes.
7.10. Assign Certificates to the Application Server

To assign transport layer security certificates to the Application Server access Feature Server Elements→ Application Servers heading on the Element Manager Console. Highlight the Application Servers section and select the Edit button.

Under the Transport section the Enable SIP TLS setting was checked. The SIP TLS Port was set to 5061. The SIP Certificate was set to ASIntOAMCertTLS. The Apply button was selected to apply the changes.
### 7.11. Assign Certificates to the Media Server

To assign transport layer security certificates to the Media Server access **Feature Server Elements ➔ Media Servers and Clusters ➔ Media Servers** heading on the Element Manager Console. Highlight the **Media Servers** section and select the **Edit** button.

Under the **Transport** section the **Enable SIP TLS** setting was checked. The **SIP TLS Port** was set to **5061**. The **SIP Certificate** was set to **MediaSIPCertTLS**. The **Enable SOAP/TLS** setting was checked. The **SOAP Certificate** was set to **MediaSIPCertTLS**. The **Apply** button was selected to apply the changes.
7.12. Assign Certificates to the Web Conferencing Server

To assign transport layer security certificates to the Web Conferencing Server access Feature Server Elements→Web Conferencing→Web Conferencing Servers heading on the Element Manager Console. Highlight the Web Conferencing Servers section and select the Edit button.

Under Web Server Transport section the Enable HTTP Port setting was unchecked. The HTTP Certificate was set to WebCollServCertTLS. The Apply button was selected to apply the changes.
7.13. Assign Certificates to the Web Conferencing Management Server

To assign transport layer security certificates to the Web Conferencing Server access Feature Server Elements→Web Conferencing→Web Conferencing Management Servers heading on the Element Manager Console. Highlight the Web Conferencing Management Servers section and select the Edit button.

Under Web Server Transport section the Enable HTTP Port setting was unchecked. The HTTP certificate was set to ProvPACertTLS. The Apply button was selected to apply the changes.
8. Generate SSL/TLS Certificates for the Documentation Conversion Server

This section describes the administration steps required to configure SSL/TLS certificates on the Documentation Conversion Server. The steps will describe administering a TLS certificate from a trusted Certificate Authority. This section also describes configuring an SSL certificate, a private key file and a certificate chain file needed to be placed in the relevant folder on the Documentation Conversion Server. The OpenSSL package that is included as part of the Conferencing Platform provides the tool to generate RSA private keys, certificate signing requests and the ability to import to private key and signed certificate into a PKCS#12 file.

8.1. Access OpenSSL on Avaya Aura Conferencing

To access OpenSSL on the Conferencing Server, Open an SSH session using Port 22 to the network address of the Conferencing Server called AAC70.

Input the Login as ntsysadm and the ntsysadm password for the Conferencing Server.

```
login as: ntsysadm
Password:

[ntsysadm@aac70 ~]$ open
```

8.2. Generate a Private Key

The following command was typed to generate a new RSA private key. The certificate called againstlss.key was used for the private key.

```
[ntsysadm@aac70 ~]$ openssl genrsa -des3 -out againstlss.key 1024
```
8.3. Generate a Certificate Signing Request

The following command was typed to generate a certificate signing request. The name `againtls.csr` was the name used for the certificate signing request. The `CN=WIN-2QFEMD3T9C$` value was the FQDN for the Document conversion Server. This generated a certificate signing request file called `againtls.csr`. Use WinSCP or similar tool to transfer the `againtls.csr` to a windows based PC in preparation for Section 8.4.

```
[ntsysadm@aac70 ~]$ openssl req -new -key againtls.key -out againtls.csr -subj 
"/C=US/O=Avaya/CN=WIN-2QFEMD3T9C4.silstack.com"
```

8.4. Generate a Certificate Chain File

Since the user generated the certificate signing request `againtls.csr` file in the previous step, this file is used to generate a certificate chain file. This application note accessed the Avaya Certificate Services internal page to generate the certificate chain file. Users of this Application Note may need contact an authorized Avaya sales representative to obtain access for third party certificate bodies.

Select the **Request a certificate** heading on the Avaya Certificates Services page.
Select the **Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file** heading.

The following page was displayed.

<table>
<thead>
<tr>
<th>Advanced Certificate Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>The policy of the CA determines the types of certificates you can request. Click the following link to:</td>
</tr>
<tr>
<td>Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Submit a Certificate Request or Renewal Request</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Saved Request:</strong></td>
</tr>
<tr>
<td>Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):</td>
</tr>
<tr>
<td><img src="Gateway_Browse.png" alt="File Browse" /></td>
</tr>
<tr>
<td><strong>Certificate Template:</strong></td>
</tr>
<tr>
<td><img src="Gateway_SavedRequest.png" alt="Internal Server" /></td>
</tr>
<tr>
<td><strong>Additional Attributes:</strong></td>
</tr>
<tr>
<td>Attributes:</td>
</tr>
<tr>
<td><img src="Gateway_SavedRequest.png" alt="Attributes" /></td>
</tr>
<tr>
<td><img src="Gateway_SavedRequest.png" alt="Submit Button" /></td>
</tr>
</tbody>
</table>
Using the certificate signing request file `againtle.csr` file, the certificates from the `againtls.csr` file were copied and pasted into the **Base-64-encoded certificate request** section under **Save Request** of the Avaya Services page.

The **Submit** button was selected.

The **Base 64 encoded** setting was selected and the **Download certificate** sub heading was also selected.
The following File Download is displayed. The **Save** button was selected.

The certificate was saved in the folder **AAC70** and was given the **File name** called **againtls.crt**.
Also on the Certificates Issued page. Select the Base 64 encoded setting and then the Download certificate chain subheading.

The following File Download is displayed. The Save button was selected.

The certificate was saved in the folder AAC70 and was given the File name called againtls.p7b.
Using the certificate chain file `againtls.p7b` generated in the previous step, this file was converted to a chain file using OpenSSL. This is the Root CA of the Documentation Conversion Server. The Root CA chain file was named `chainagaintls.crt`.

```plaintext
[ntsysadm@aac70 ~]$ openssl pkcs7 -print_certs -in againtls.p7b -out chainagaintls.crt
```

### 8.5. Generate a PKCS#12 File

The following command was typed in OpenSSL to generate a PKCS#12 file. The private key certificate `againtls.key` and the certificate `againtls.crt` generated in the previous steps were used to generate the PKCS#12 file. The PKCS#12 file `againtls.p12` was created containing the certificate and the private key.

```plaintext
[ntsysadm@aac70 ~]$ openssl pkcs12 -export -out againtls.p12 -inkey againtls.key -in againtls.crt
```

### 8.6. Remove the Passphrase Key file

The following command was use in OpenSSL to remove the passphrase from the protected key file `againtls.key`. The unprotected key file was renamed to the file called `tlsunprotected.key`.

```plaintext
[ntsysadm@aac70 ~]$ openssl rsa -in againtls.key -out tlsunprotected.key
```

### 8.7. Importing Certificate from a Third Party CA

To import the third party CA certificate access the **Security**→**Certificate Management**→**Keystore** heading on the Element Manager Console. The **Add** button was selected.
The **Logical Name** was set to **againtls.p12**. The **Browse** button was then selected.

![Add PKCS#12 File dialog box](image1)

From the **CertificatesAgaintls** folder the third party certificate **againtls.p12** was selected.

![Select PKCS#12 File dialog box](image2)

With the **PKCS#12** file **againtls.p12** selected, the password was inputted and the **Apply** button was selected to apply the changes.

![Add PKCS#12 File dialog box](image3)
The third party certificate **againtls.p12** was seen to be imported to the Keystore on the Element Manager Console.

### 8.8. Importing CA Certificate from a Third Party CA

To import CA certificates from a third party access the **Security → Certificate Management → Truststore** heading on the Element Manager Console. The **Add** button was selected.

From the **CertificatesAgaintls** folder the third party CA certificate **againtls.crt** was selected.
The CA certificate **againtls.crt** was seen to be imported to the Truststore on the Element Manager Console.

### 8.9. Add the System Manager CA Certificate to User IE Browser

Select Services → Security → Certificates → Authority on System Manager.

Select the heading **Download to Internet Explorer**.

The **Save File** button was selected.
The **File name** called `default.cacert.crt` was saved to **Desktop**.

The **Certificate** was selected and the **Install Certificate** button was selected.

The **Certificate Import Wizard** appears. The **Next** button was selected.
The **Place all certificates in the following store** field was selected. The **Browse** option was then selected. The certificate store **Trusted Root Certification Authorities** was selected from the certification store. The **Next** button was selected.

The **Finish** button was selected to complete the Certificate Import Wizard.
9. Configuring SSL/TLS Certificates on the Documentation Conversion Server

This section describes the steps needed to configure SSL/TLS Certificates on the Documentation Conversion Server. This Application Notes assumes that the Documentation Conversion Server software has already been copied and installed and that configuration of the Java bin folder (Refer to Section 13 Reference 1) through windows was completed as well disabling macros on Microsoft Word and PowerPoint.

9.1. Access the Documentation Conversion Server

Access the Documentation Conversion Server, by opening a Remote Desktop session and entering the IP Address of the Documentation Conversion Server and select the Connect button as shown below.

![Remote Desktop Connection](image)

9.2. Documentation Conversion Server Certificates

In the root folder of the Documentation Conversion Server installation directory, C:/dcs, the folder called certs was created manually.

![Folder Structure](image)

Copy the SSL certificate file, againtls.crt, the private key file, tlsunprotected.key and the certificate chain file, chaintls.crt into the certs folder.
9.3. Configure the HTTPD.Conf File

The httpd.conf file is generated in the C:/dcs/Conf/ folder after selecting and opening the Setup DCS.bat file from the C:/dcs folder.

The following sections were added to the httpd.conf file. The **Listen** directive port at the beginning of the httpd.conf file was changed to **8443**.

**Listen 8443**

The # comment tag was removed from the following line **#LoadModule ssl_module modules/mod_ssl.so** to leave the below line in the httpd.conf file.

**LoadModule ssl_module modules/mod_ssl.so**
The section called `<IfModule ssl_module>` in the `httpd.conf` file was appended with the below information. It contains the location of the certificates in the root folder of the Documentation Conversion Server.

```xml
<IfModule ssl_module>
  SSLRandomSeed startup builtin
  SSLRandomSeed connect builtin
  SSLEngine on
  SSLCertificateFile C:/dcs/certs/againtls.crt
  SSLCertificateKeyFile C:/dcs/certs/tlsunprotected.key
  SSLCertificateChainFile C:/dcs/certs/chainagaintls.crt
</IfModule>
```

The `ServerName` setting was configured to match the FQDN of the Documentation Conversion Server with port **8443**.

```text
ServerName WIN-2QFEMD3TC4.SILStack.com:8443
```

**9.4. Configure the Config.php File**

In the `Config.php` file located in `C:/dcs/htdocs/app` folder on the Documentation Conversion Server set the access key setting to 123456.

```php
self::$setting['access_key'] = 123456;
```
9.5. Configure Documentation Conversion Server on Element Manager Console

To configure the Documentation Conversion Server access Feature Server Elements ➔ Web Conferencing ➔ Documentation Conversion Servers headings on the Element Manager Console. Select the Edit button.

![Diagram of Element Manager Console with selected options]

The Long Name was set to DocumentConversionServer. The FQDN was set to win-2qfemd3t9c4.silstack.com. The Protocol was set to HTTPS with Port number 8443. The Access Key was set to 123456 to match the access key set on the Config.php file in Section 9.4. The Apply button was selected to apply these changes.

![Diagram of Edit Document Conversion Server window with selected options]
10. Configuring Avaya Flare Experience on windows client

The Avaya Flare Experience on windows client endpoint is used to open Web Collaboration Agent as a provisioned user and start the Web collaboration Agent from the client. With Web Collaboration Agent opened through the Avaya Flare Experience client the user can access a Library folder and upload the relevant documents and share these documents with the participants in the Meet Me conference. The Flare Experience on windows client was installed on a standard pc. The Flare Experience client is a SIP user that registers to Session Manager. To administer the settings access the Settings section on the client and then the Server setting. The Server address was set to 192.168.1.87 with the Server port as 5061. The Transport type was set to TLS. The Domain was set to silstack.com.

Under the Log in section the Login Extension was set to 70031 and the extension password was set. The Login button was selected to login.
11. Verification Steps

The following four verification steps were tested using the sample configuration. The following steps can be used to verify installation in the field.

1. Verified Flare Experience on windows SIP client could join a Meet Me conference as a Moderator.
2. Verified Web Collaboration Agent could be started from Flare Experience on windows SIP client.
3. Verified SSL Certificates worked successfully on the Documentation Conversion Server.
4. Verified the Documentation Conversion Server could be started successfully.
5. Verified that a document could be uploaded within the Meet Me Conference.
6. Verified that a document could be viewed and shared within a Meet Me Conference.

Verified Flare Experience on windows SIP client could join a Meet Me conference as a Moderator.

The Moderator code 170031 was inputted.
The Documentation Conversion Server was started successfully.

The SSL Certificates worked successfully on the Documentation Conversion Server by browsing to the DNS name of the DCS and SSL port number.
The Web Collaboration Agent could be started from Flare Experience on windows SIP client by selecting the **Web Collaboration button** highlighted.

![Image of Web Collaboration Agent initialization]

The Web Collaboration Agent was seen to initialize.

![Image of Web Collaboration Agent initializing]

The Begin Sharing heading was seen in Web Collaboration.

![Image of Begin Sharing button]

The Document from library heading was selected.

![Image of Document from library selection]

A document was uploaded within the Meet Me Conference using the Upload button.
The Word document named test was selected.

The document named test was seen to be uploading.
The following uploaded Word document was able to be viewed and shared.
12. Conclusion
These Application Notes described the configuration steps required to administer Transport Layer Security on the Avaya Aura® Conferencing 7.0 Co-Resident Simplex Server. The Application Notes also identified how to configure Secure Socket Layer Certificates on the Document Conversion Server. The Application Note also detailed how to administer Avaya Aura® Solution for Midsize Enterprise with Avaya Aura® Conferencing 7.0 Co-Resident Simplex Server.

13. Additional References
This section references Avaya documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.