Avaya Solution & Interoperability Test Lab

Application Notes for Synergem Evolution 911 Elite™ with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Synergem Evolution 911 Elite™ which were compliance tested with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services. Evolution 911 is a Public Safety 911 Call Center application that leverages the Call Center Elite functionality in Avaya Aura® Communication Manager.

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.

©2021 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring Synergem Evolution 911 Elite™ (Evolution 911 Elite) endpoints, which were compliance tested with Avaya Aura® Communication Manager (Communication Manager), Avaya Aura® Session Manager (Session Manager) and Avaya Aura® Application Enablement Services (AES). Evolution 911 Elite SIP endpoint registers to Session Manager via TCP. Evolution 911 Elite also uses the AES DMCC API for logging in agents for Automatic Call Distribution (ACD) functionality.

Evolution 911 Elite, Synergem's call-taking solution, was designed from the ground up to optimize the capabilities delivered by a Next Generation 9-1-1 ESInet built to the i3 standards (See NENA i3 standard).

Evolution 911 Elite provides all of the capabilities required to execute the call taking function in a Next Generation Public Safety Answering Point (PSAP). Evolution 911 is a Public Safety 911 Call Center desktop softphone application that leverages the Call Center Elite functionality in Communication Manager.

The Evolution 911 Elite user interface provides the capability to register SIP endpoints with Session Manager, answer incoming calls, place outgoing calls, release calls, manage calls (mute, hold, conference, transfer, speed dials, etc.), provide caller location information, log into Avaya ACD and provide access to agency contact lists. DMCC is used to control agent status functionality.

Supervisors are also configured to use H.323 DMCC stations to Service Observe Agent calls, this function relies on Service Observe Feature Access codes administered in Communication Manager.

The Windows based GUI is user friendly and customizable by agency and end user.

These Application Notes assume that Communication Manager and Session Manager are already installed, and basic configuration steps have been performed. Only steps relevant to this compliance test will be described in this document. For further details on configuration steps not covered in this document, consult references [1], [2], and [3].

2. General Test Approach and Test Results

The general test approach was to place calls to and from Evolution 911 Elite and exercise basic telephone and ACD operations. The main objectives were to verify the following:

- Registration
- Codecs (G.711MU, G.729)
- DTMF (SIP INFO)
- Inbound calls
- Outbound calls
- Hold/Resume
- Call termination (origination/destination)
- Conferences and transfers
- Agent log-in, log-out and states

©2021 Avaya Inc. All Rights Reserved.

- Supervisor Service Observation
- Serviceability

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 Evolution 911 Elite did not utilize secure capabilities at the request of Synergem.

2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the interoperability compliance testing was primarily on verifying call establishment on Evolution 911 Elite. Evolution 911 Elite operations such as inbound calls, outbound calls, hold/resume, transfer, conference, and Evolution 911 Elite interactions with Session Manager, AES, and Avaya SIP, and H.323 telephones were verified. The serviceability testing introduced failure scenarios to see if Evolution 911 Elite can recover from failures.

2.2. Test Results

The test objectives were verified. For serviceability testing, Evolution 911 Elite operated properly after recovering from failures such as cable disconnects, and resets of Evolution 911 Elite, and Session Manager and AES. The features tested worked as expected.

2.3. Support

Technical support on Synergem Evolution 911 Elite™ can be obtained through the following:
Phone: 1-866-859-0911
Email: support@synergemtech.com
Web: www.synergemtech.com/support

©2021 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Communication Manager, an Avaya G430 Media Gateway, a Session Manager, System Manager and Evolution 911 Elite. The solution described herein is also extensible to other Avaya Media Servers and Media Gateways.

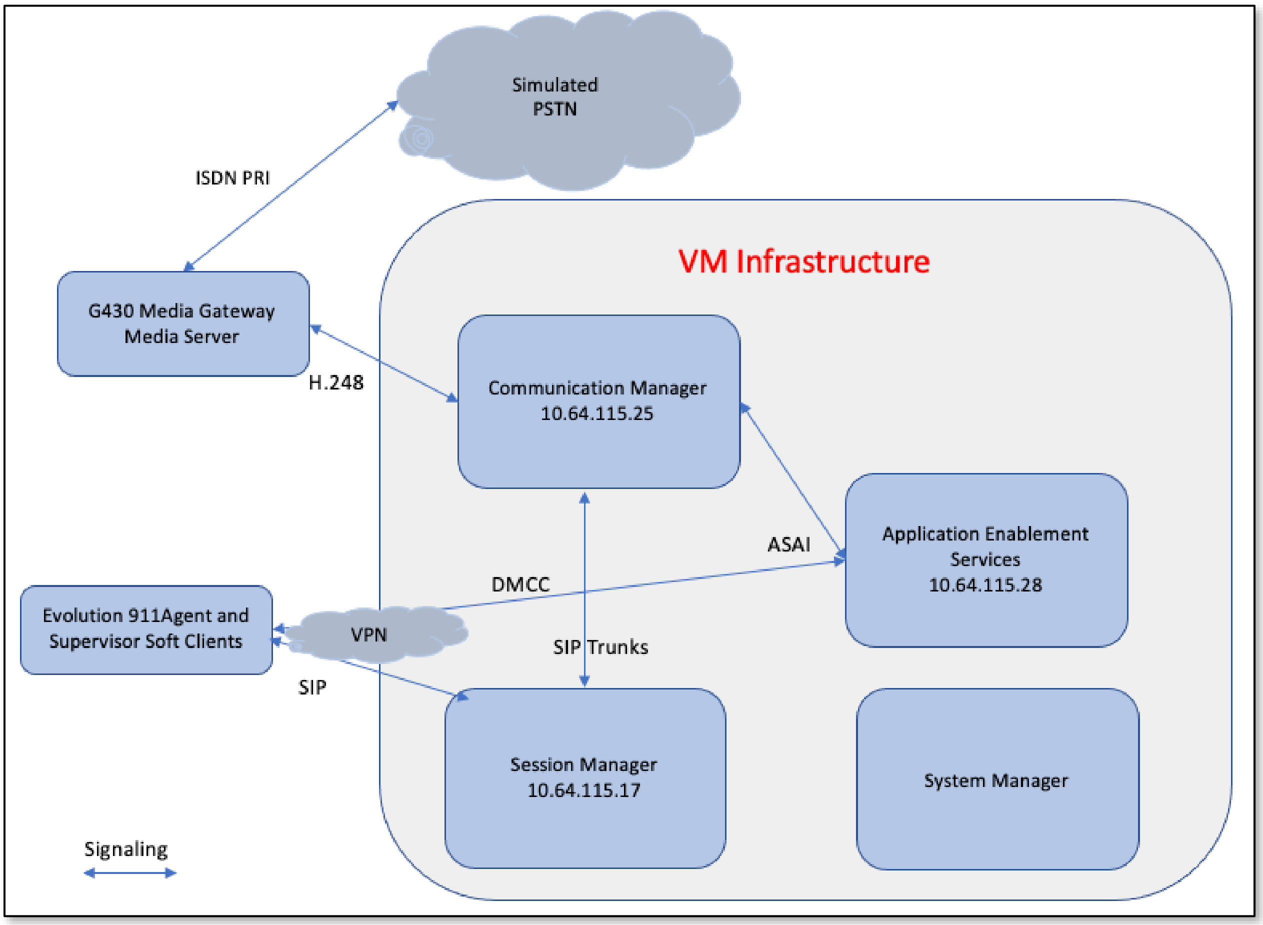


Figure 1: Test Configuration of Evolution 911 Elite ™ by Synergem

©2021 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

The following equipment and software were used for the test configuration.

Equipment		Software/Firmware
Avaya Aura® Communication Manager in Virtual Environment		8.1.3.1.0-FP3SP1
Avaya Aura® System Manager in Virtual Environment		8.1.2.0.0611588
Avaya Aura® Session Manager in Virtual Environment		8.1.2.1.812101
Avaya Aura® Media Server in Virtual Environment		8.0.2.127
Avaya G430 Media Gateway		41.24.0/1
Avaya Aura® Application Enablement Services in Virtual Environment		8.1.2.1.1.6-0
Avaya IP Deskphones		
	9641G (SIP) J169\179 (SIP)	7.1.1.0.9 3.0.0.1.6
Evolution 911 Elite™ by Synergem		4.3.0.004

©2021 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, and a SIP station. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface. Evolution 911 Elite and other SIP telephones are configured as off-PBX telephones in Communication Manager.

5.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient **Maximum Off-PBX Telephones – OPS** licenses. If not, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options                      Page   1 of  12
                                OPTIONAL FEATURES

     G3 Version: V18                                Software Package: Enterprise
       Location: 2                                   System ID (SID): 1
       Platform: 28                                  Module ID (MID): 1

                                                              USED
                             Platform Maximum Ports:   6400     66
                                   Maximum Stations:   2400     23
                           Maximum XMOBILE Stations:   2400      0
                Maximum Off-PBX Telephones - EC500:   9600      1
                Maximum Off-PBX Telephones -   OPS:   9600      4
                Maximum Off-PBX Telephones - PBFMC:   9600      0
                Maximum Off-PBX Telephones - PVFMC:   9600      0
                Maximum Off-PBX Telephones - SCCAN:      0      0
                     Maximum Survivable Processors:  313        0
```


©2021 Avaya Inc. All Rights Reserved.

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options                      Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                  USED
                 Maximum Administered H.323 Trunks:  4000      0
       Maximum Concurrently Registered IP Stations:  1000      2
         Maximum Administered Remote Office Trunks:  4000      0
Max Concurrently Registered Remote Office Stations:  1000      0
          Maximum Concurrently Registered IP eCons:   68       0
     Max Concur Reg Unauthenticated H.323 Stations:   100      0
                    Maximum Video Capable Stations:   2400     0
               Maximum Video Capable IP Softphones:   1000     2
                   Maximum Administered SIP Trunks:  4000     20
  Max Administered Ad-hoc Video Conferencing Ports:  4000      0
   Max Number of DS1 Boards with Echo Cancellation: 80     0
```

5.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.3** for configuring IP network region to specify which codec sets may be used within and between network regions. For the compliance testing, G.729 and G.711MU were tested for verification.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729            n          2        20
 2: G.711MU          n          2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
```


©2021 Avaya Inc. All Rights Reserved.

5.3. Configure IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and Session Manager. Enter the **change ip-network-region <n>** command, where **n** is a number between **1** and **250** inclusive, and configure the following:

- **Authoritative Domain** – Enter the appropriate name for the Authoritative Domain. Set to the appropriate domain. During the compliance test, the authoritative domain is set to **sildenver.org**. This should match the SIP Domain value on Session Manager, in **Section 6.1**.
- **Intra-region IP-IP Direct Audio** – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in the same IP network region. The default value for this field is **yes**.
- **Codec Set** – Set the codec set number as provisioned in **Section 5.2**.
- **Inter-region IP-IP Direct Audio** – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in different IP network regions. The default value for this field is **yes**.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: sildenver.org
    Name: SM                    Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```


©2021 Avaya Inc. All Rights Reserved.

5.4. Configure IP Node Name

This section describes the steps for setting IP node name for Session Manager in Communication Manager. Enter the **change node-names ip** command and add a node name for Session Manager and Application Enablement Services along with its IP address.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
procr               10.64.115.25
procr6              ::
sildvaes8           10.64.115.28
sildvams            10.64.115.3
sildvcmm1           10.64.115.12
sildvmg1            10.64.115.2
sildvsm2            10.64.115.17
sildvsm3            10.64.115.20
```


©2021 Avaya Inc. All Rights Reserved.

5.5. Configure SIP Signaling

This section describes the steps for administering a signaling group in Communication Manager for communication between Communication Manager and Session Manager. Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- **Group Type** – Set to **sip**.
- **Transport Method –** Set to **tls**.
- **Near-end Node Name** – Set to **procr**.
- **Far-end Node Name** – Set to the Session Manager name configured in **Section 5.4**.
- **Far-end Network Region** – Set to the region configured in **Section 5.3**.
- **Far-end Domain** – Set to **sildenver.org**. This should match the SIP Domain value in **Section 6.1**.
- **Direct IP-IP Audio Connections** – Set to **y**, since Media Shuffling is enabled during the compliance test.

```
add signaling-group 10                                          Page   1 of   3
                                SIGNALING GROUP

 Group Number: 10              Group Type: sip
  IMS Enabled? n         Transport Method: tls
        Q-SIP? n
     IP Video? n                                    Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                         Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: sildvsm2
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: sildenver.org
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  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? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```


©2021 Avaya Inc. All Rights Reserved.

5.6. Configure SIP Trunk

This section describes the steps for administering a trunk group in Communication Manager for communication between Communication Manager and Session Manager. Enter the **add trunk-group <t>** command, where **t** is an unallocated trunk group and configure the following:

- **Group Type** – Set the Group Type field to **sip**.
- **Group Name** – Enter a descriptive name.
- **TAC** (Trunk Access Code) – Set to any available trunk access code.
- **Outgoing Display –** Set to **y**.
- **Signaling Group** – Set to the Group Number field value configured in **Section 5.5**.
- **Number of Members –** Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
add trunk-group 10                                            Page   1 of   5
                                TRUNK GROUP

Group Number: 10                   Group Type: sip           CDR Reports: y
  Group Name: ToSM2                           COR: 1        TN: 1        TAC: 110
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                      Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 10
                                                     Number of Members: 10
```


©2021 Avaya Inc. All Rights Reserved.

5.7. Configure CTI-link

This section describes the steps for administering a CTI Link for AES. Enter the **add cti-link <c>** command, where **c** is an unallocated cti link.

- **Extension** – Type in an available extension number
- **Type** – Set to **ADJ-IP**
- **Name** – Type in a descriptive name

```
add cti-link 1                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 30099
     Type: ADJ-IP
                                                                        COR: 1
     Name: AES8
Unicode Name? n
```

5.8. Configure ip-services

This section describes configuration required to configure ip services for AES. Enter the **change ip-services** command and configure Page 1 and Page 3 as following:

- On Page 1, enter **AESVCS** and set Enabled to **y**.
- On Page 3, configure the host name of AES in **AES Services Server** and set a password in **Password.**

```
change ip-services                                               Page   1 of   3

                                   IP SERVICES
 Service      Enabled     Local        Local       Remote      Remote    TLS
  Type                    Node         Port        Node        Port   Encryption
AESVCS          y     procr           8765


change ip-services                                               Page   3 of   3
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      sildvaes8        *                     y
```


©2021 Avaya Inc. All Rights Reserved.

5.9. Note Service Observation Feature Access Codes

Note the system Feature Access Codes for Service Observing, these will be used when configuring Evolution 911 Elite™ as described in **Section 8.**

```
display feature-access-codes                                    Page   5 of  12
                               FEATURE ACCESS CODE (FAC)
                                 Call Center Features
  AGENT WORK MODES
                           After Call Work Access Code: *50
                                    Assist Access Code: *51
                                   Auto-In Access Code: *52
                                  Aux Work Access Code: *53
                                     Login Access Code: *54
                                    Logout Access Code: *55
                                 Manual-in Access Code: *56
  SERVICE OBSERVING
             Service Observing Listen Only Access Code: *57
             Service Observing Listen/Talk Access Code: *58
                 Service Observing No Talk Access Code: *59
   Service Observing Next Call Listen Only Access Code: *60
 Service Observing by Location Listen Only Access Code: *61
 Service Observing by Location Listen/Talk Access Code: *62

  AACC CONFERENCE MODES
                     Restrict First Consult Activation:      Deactivation:
    Restrict Second Consult Activation:      Deactivation:
```

5.10. Note DMCC Stations

If not already configured, add stations for the Evolution 911 Elite ™ Supervisors to use for Service Observing Agent calls. Following is a display of one such station used in testing which was previously administered, this is used when configuring Evolution 911 Elite™ as described in **Section 8.**

```
display station 30055                                           Page   1 of   5
                                     STATION

Extension: 30055                         Lock Messages? n             BCC: 0
     Type: 9608                          Security Code: *              TN: 1
     Port: S000032                     Coverage Path 1:               COR: 1
     Name: DMCC6                       Coverage Path 2:                COS: 1
Unicode Name? n                     Hunt-to Station:                 Tests? y
STATION OPTIONS
                                         Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                           Message Lamp Ext: 30055
            Speakerphone: 2-way             Mute Button Enabled? y
        Display Language: english                Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal            Media Complex Ext:
   Survivable Trunk Dest? y                        IP SoftPhone? y

                                             IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                            Customizable Labels? y
```


©2021 Avaya Inc. All Rights Reserved.

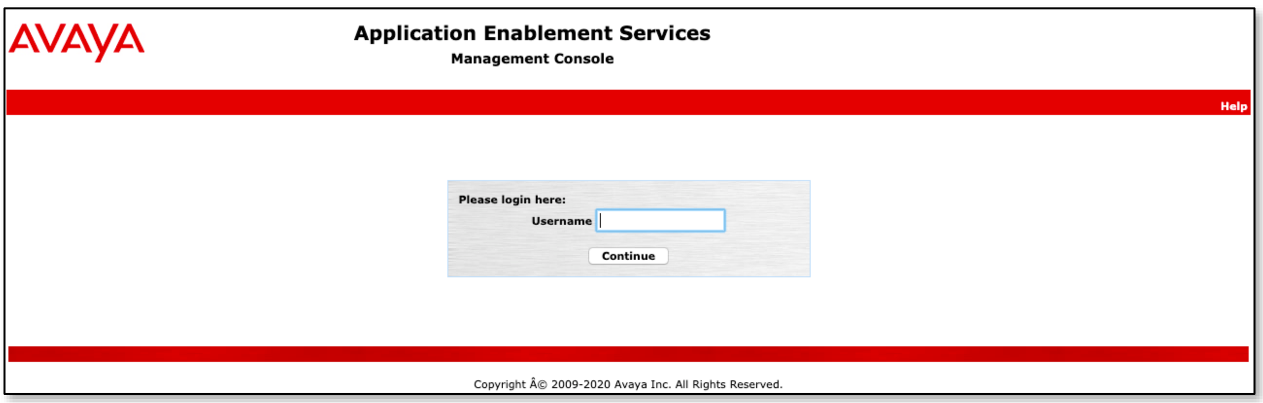
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer CTI user
- Administer security database
- Administer ports
- Obtain Tlink name
- Restart services

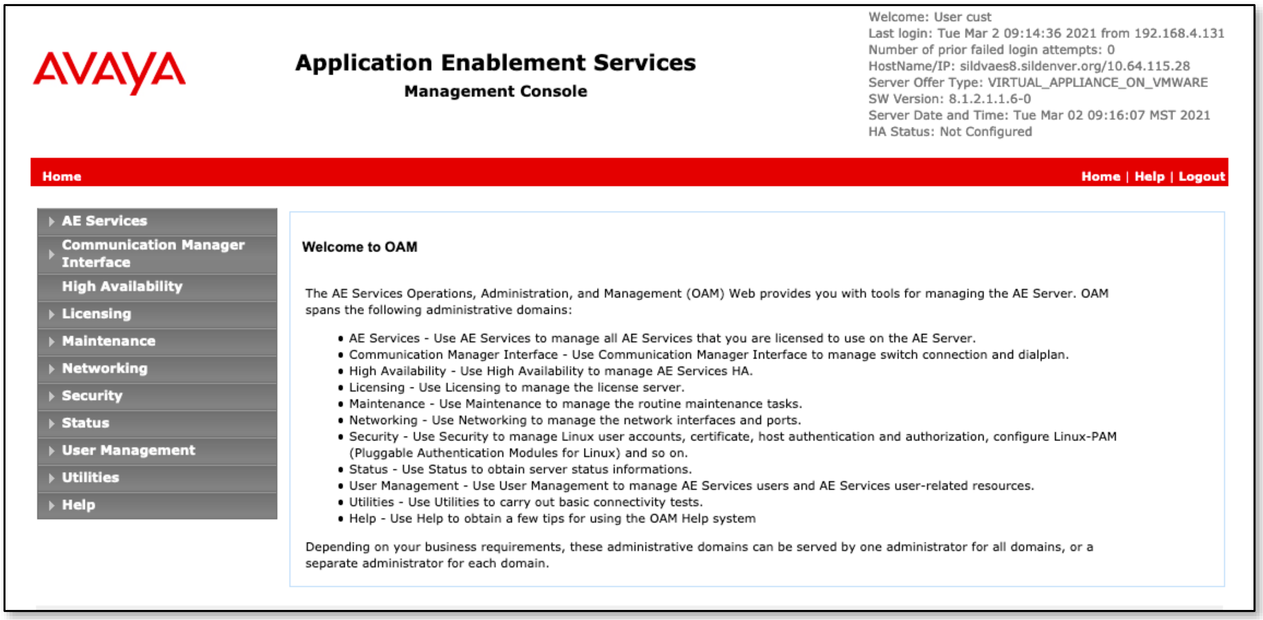
6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of the Application Enablement Services server. The **Please login here** screen is displayed. Log in using the appropriate credentials.



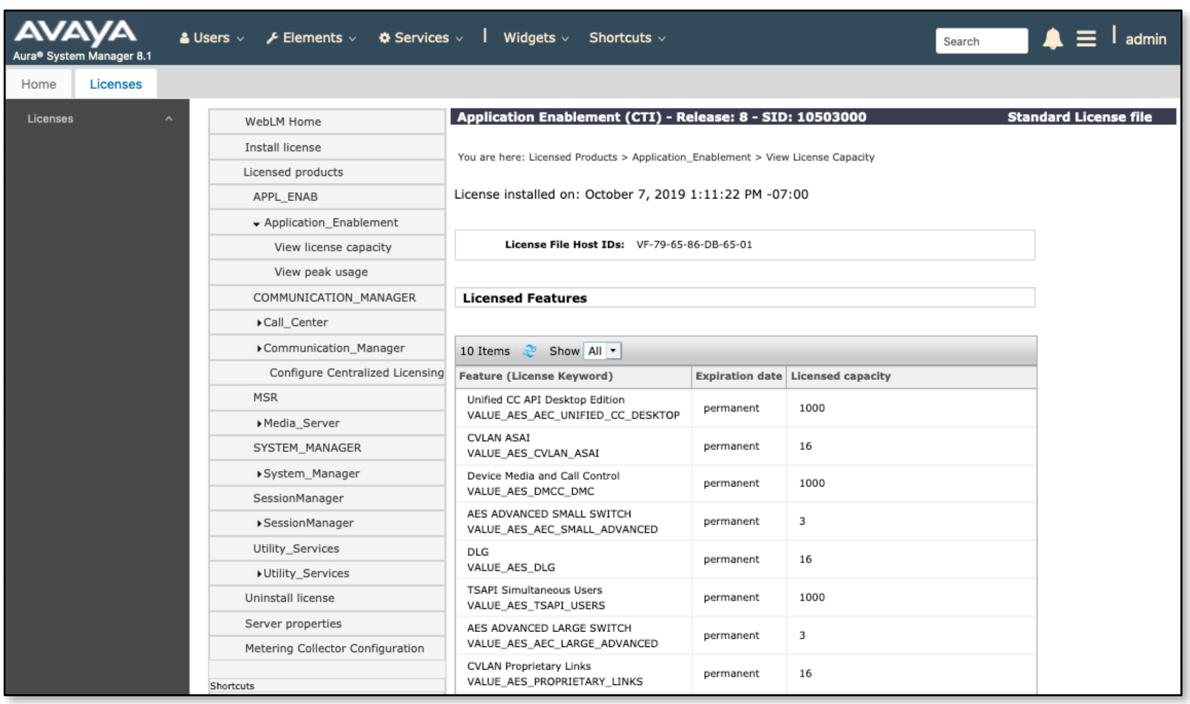
©2021 Avaya Inc. All Rights Reserved.

The **Welcome to OAM** screen is displayed next.



6.2. Verify License

System Manager was used as a central license server for the test environment. On System Manager, navigate to **Services → Licenses → Application Enablement**. Log in using the appropriate credentials and navigate to display installed licenses.

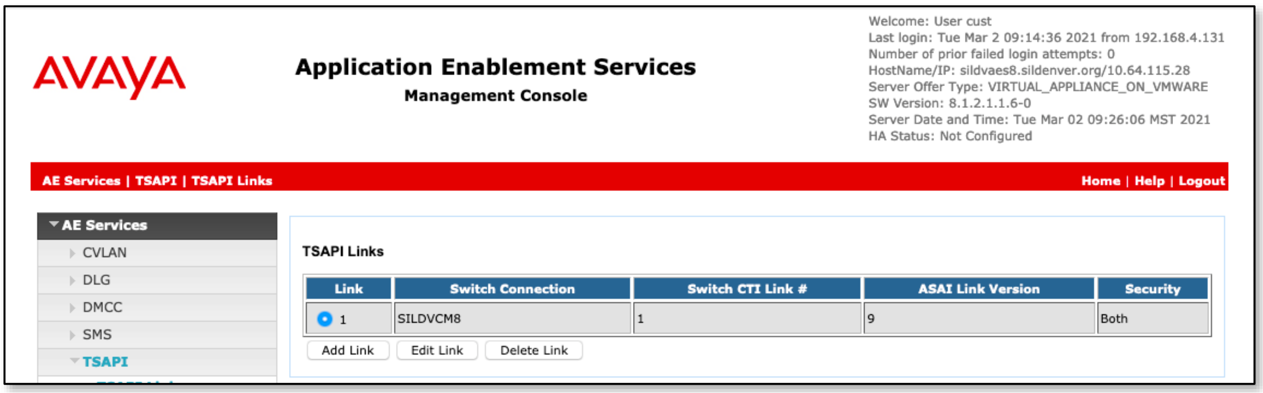


©2021 Avaya Inc. All Rights Reserved.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** as shown above. Note that the TSAPI license is used for monitoring and call control via DMCC.

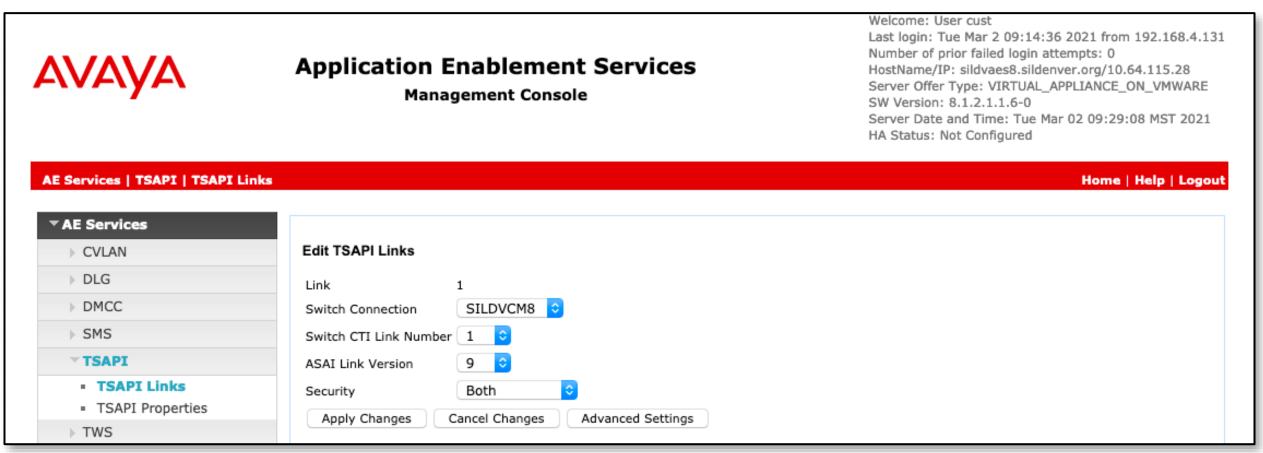
6.3. Administer TSAPI Link

Select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**, note that an existing TSAPI Link was used for testing, details are displayed using the **Edit Link** button.



The **Add (or Edit) TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "**SILDVCM8**" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.7**. ASAI Link Version 9 was used in the testing. Retain the default values in the remaining fields.

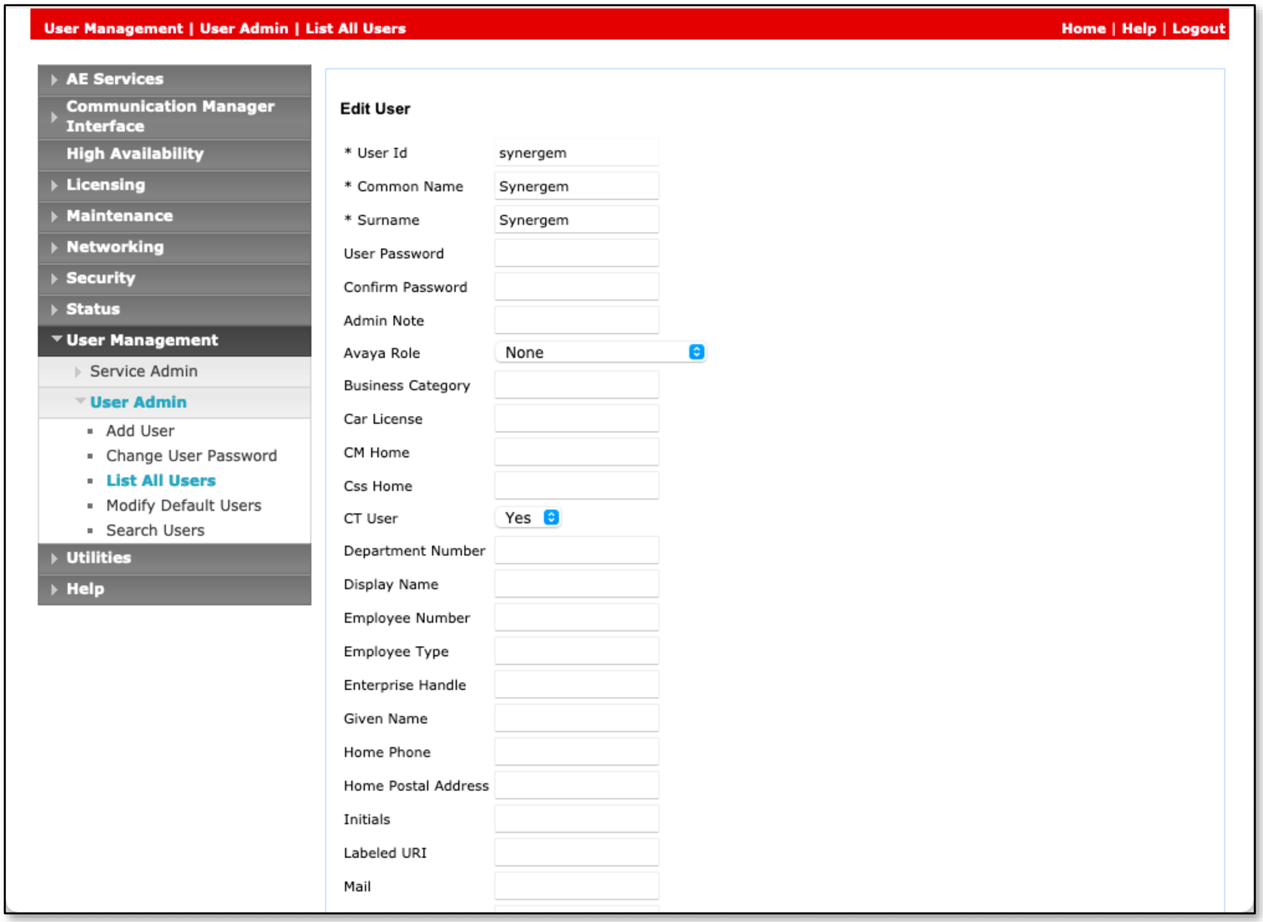


©2021 Avaya Inc. All Rights Reserved.

6.4. Administer CTI User

Select **User Management → User Admin → Add User** from the left pane, to display the **Add User** screen in the right pane.

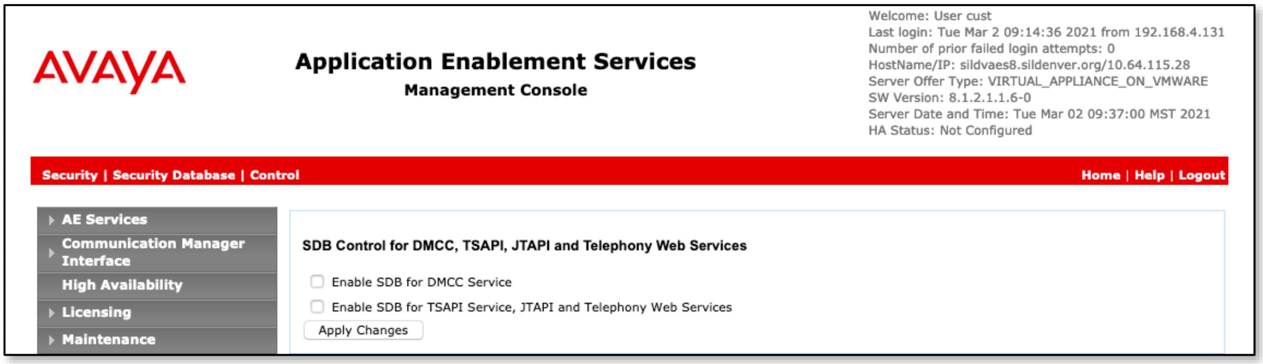
Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select "Yes" from the drop-down list. Retain the default value in the remaining fields.



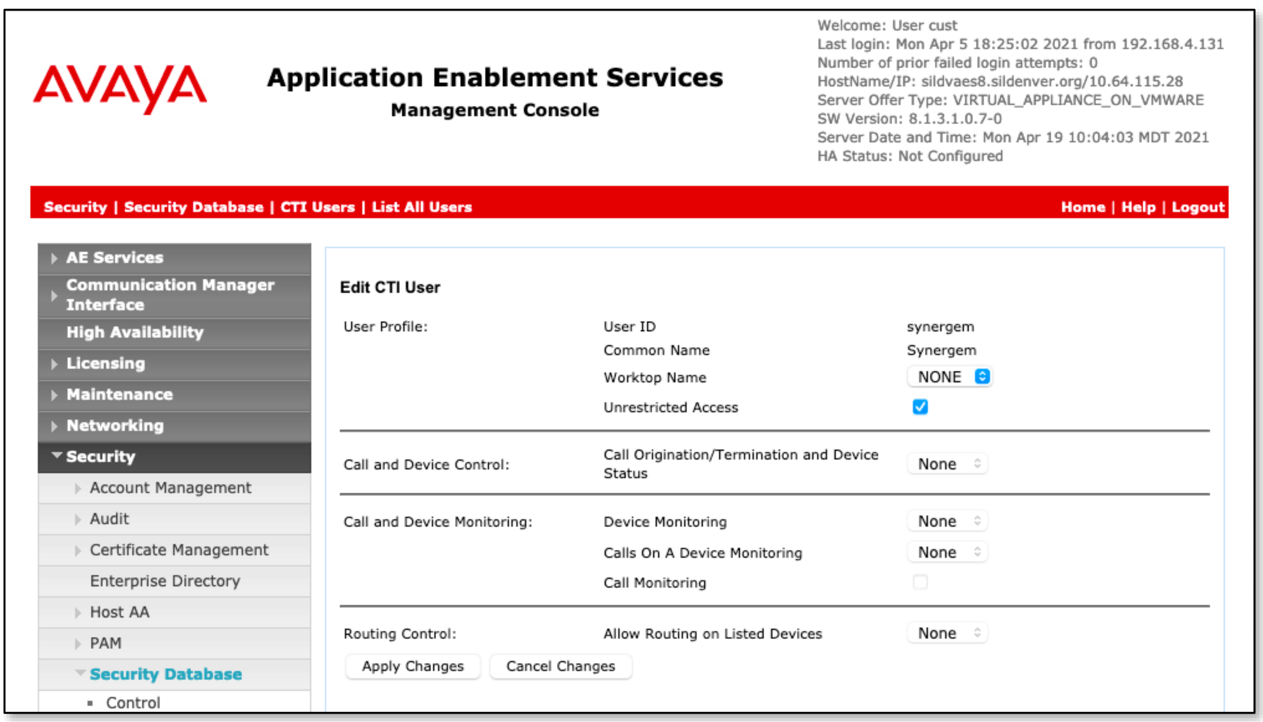
©2021 Avaya Inc. All Rights Reserved.

6.5. Administer Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain both parameters are unchecked, as shown below.



In the event that the security database is used by the customer with parameters already enabled, then configure access privileges for the CTI user from **Section 6.4**. On the Edit CTI User screen, check **Unrestricted Access** to grant access to any devices administered in the application.

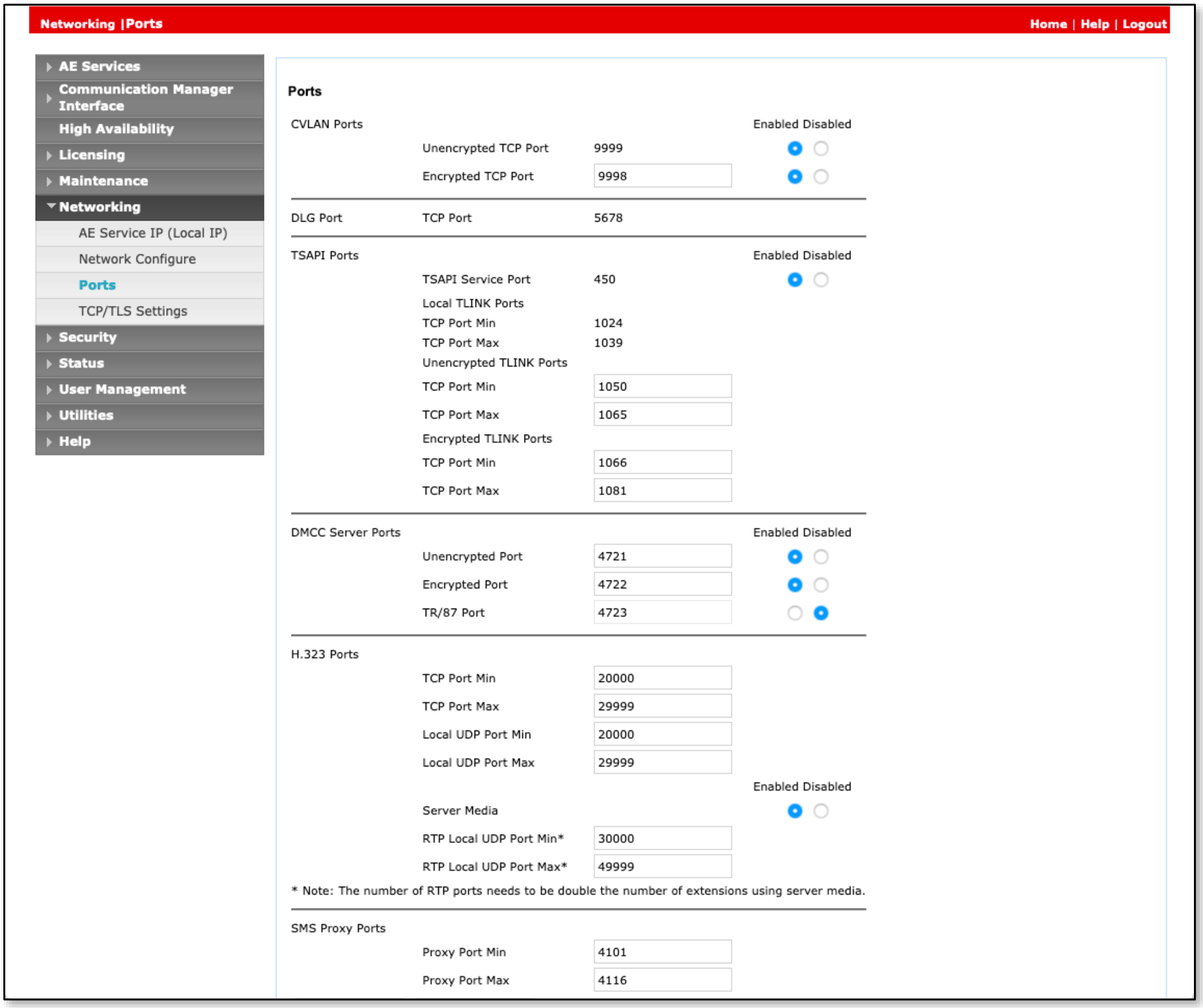


©2021 Avaya Inc. All Rights Reserved.

6.6. Administer Ports

Select **Networking → Ports** from the left pane, to display the **Ports** screen in the right pane.

Enable the **TSAPI Ports → TSAPI Service Port 450**, and the **DMCC Server Ports → Unencrypted Port 4721** as shown below. For this testing, only the Unencrypted port was used.

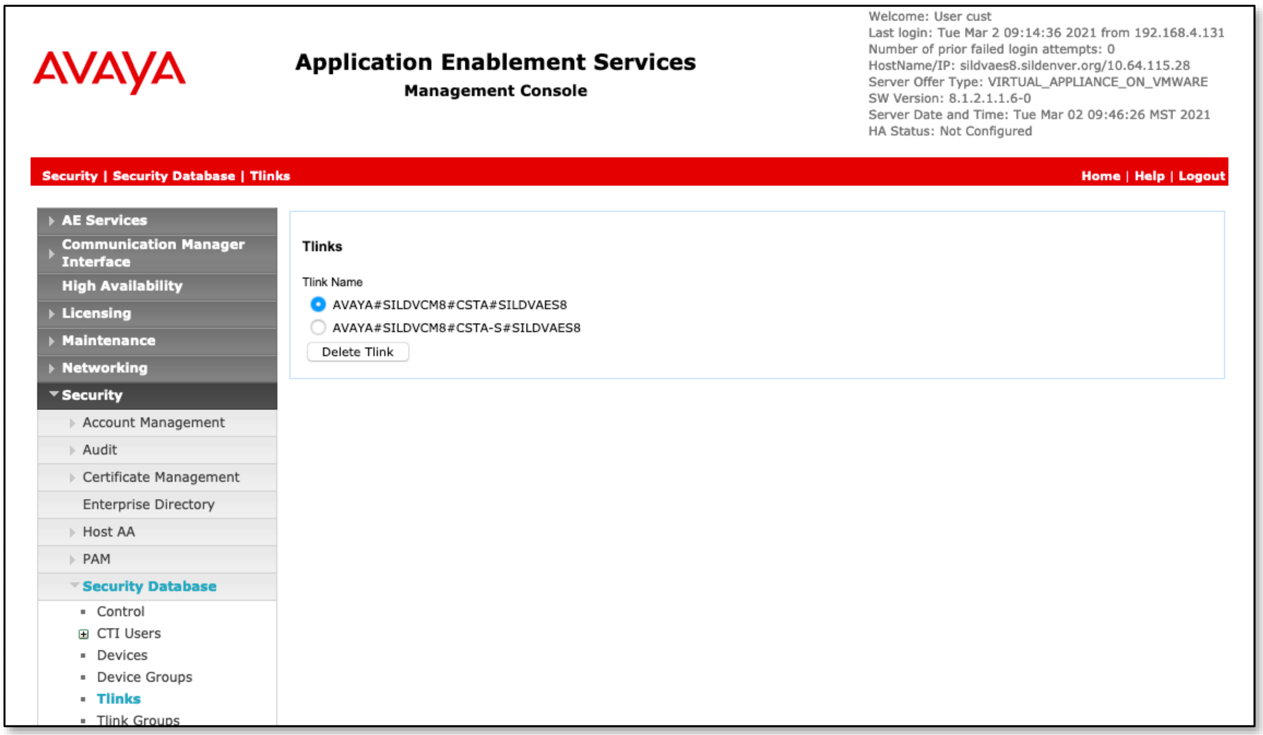


©2021 Avaya Inc. All Rights Reserved.

6.7. Obtain Tlink Name

Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Evolution 911 Elite™ by Synergem.

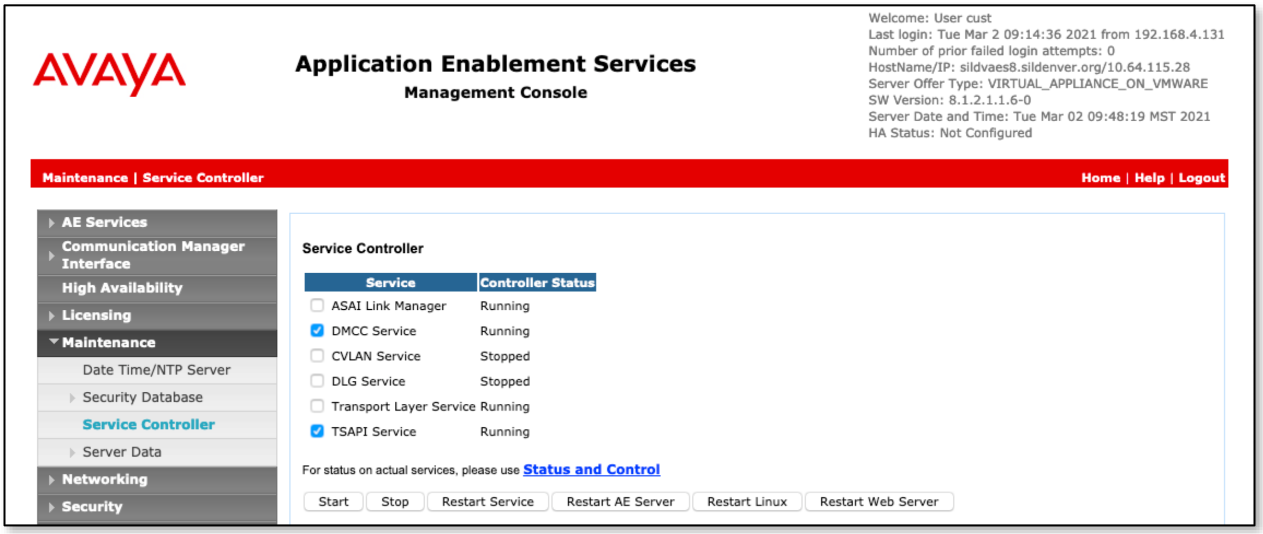
In this case, the associated Tlink name is "AVAYA#**SILDVCM8**#CSTA#**SILDVAES8**".



©2021 Avaya Inc. All Rights Reserved.

6.8. Restart Services

Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service** and click **Restart Service**.



©2021 Avaya Inc. All Rights Reserved.

7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

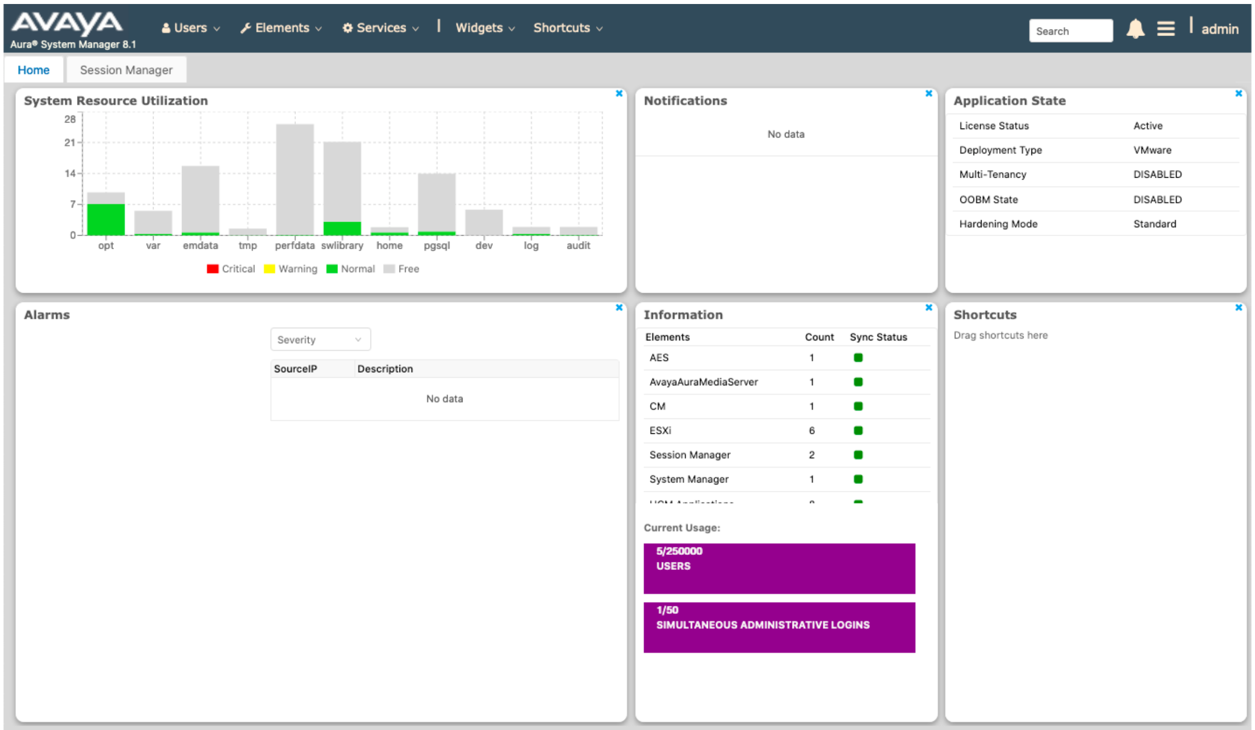
In this section, the following topics are discussed:

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- User Management

©2021 Avaya Inc. All Rights Reserved.

7.1. Configure SIP Domain

Launch a web browser, enter **http://<IP address of System Manager>** in the URL, and log in with the appropriate credentials.

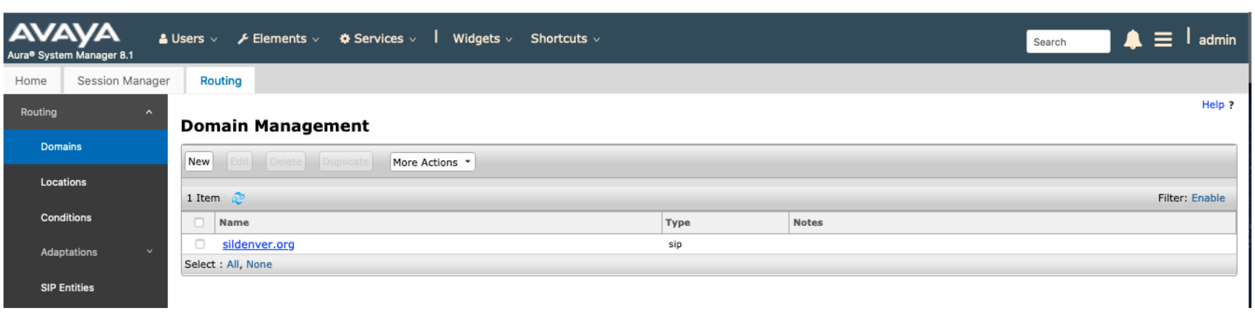


In the main menu, navigate to **Elements → Routing → Domains**, and click on the **New** button (not shown) to create a new SIP Domain. Enter the following values and use default values for remaining fields:

- **Name –** Enter the Authoritative Domain Name specified in **Section 5.3**, which is **sildenver.org**.
- **Type** – Select **SIP**.

Click **Commit** to save.

The following screen shows the Domains page used during the compliance test.



©2021 Avaya Inc. All Rights Reserved.

7.2. Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

From the main menu, navigate to **Elements → Routing → Locations**, and click on the **New** button (not shown) to create a new SIP endpoint location.

<u>General section (not shown)</u>
Enter the following values and use default values for remaining fields.

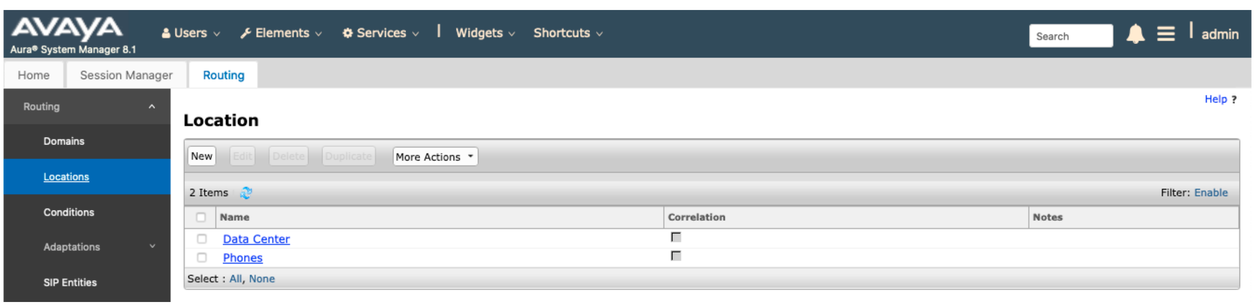
- Enter a descriptive Location name in the **Name** field (e.g. **Phones**).
- Enter a description in the **Notes** field if desired.

<u>Location Pattern section (not shown)</u>
Click **Add** and enter the following values:

- Enter the IP address information for the **IP address Pattern** field (e.g. **192.168.***).
- Enter a description in the **Notes** field if desired.

Repeat steps in the Location Pattern section if the Location has multiple IP segments. Modify the remaining values on the form, if necessary; otherwise, use all the default values. Click on the **Commit** button.

The following screen shows the Locations list used during the compliance test. Generally, servers are defined in the Data Center location, and endpoints in the Phones location.



7.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. During the compliance test, the following SIP Entities were configured:

- Session Manager itself. This entity was created prior to the compliance test.
- Communication Manager. This entity was created prior to the compliance test.

Navigate to **Routing → SIP Entities** and click on the **New** button (not shown) to create a new SIP entity. Provide the following information:

<u>General section (not shown)</u>

©2021 Avaya Inc. All Rights Reserved.

Enter the following values and use default values for remaining fields.

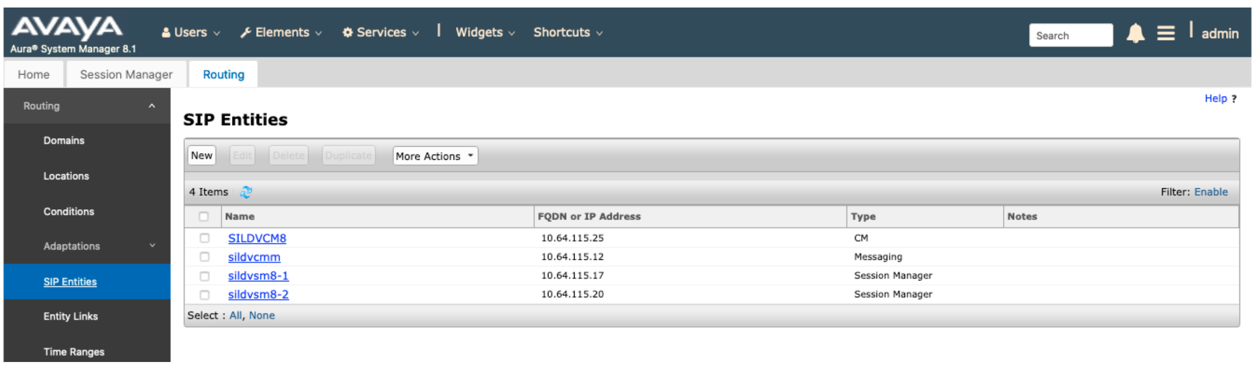
- Enter a descriptive Entity name in the **Name** field.
- Enter IP address for signaling interface on each Communication Manager, Session Manager, or 3rd party device in the **FQDN or IP Address** field.
- From the **Type** drop down menu select a type that best matches the SIP Entity.
    - For Communication Manager, select CM.
    - For Session Manager, select Session Manager.
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

<u>SIP Link Monitoring section (not shown)</u>

- Accept the other default values.

Click on the **Commit** button to save each SIP entity.
The following screen shows the SIP Entities page used during the compliance test. The **sildvcmm** (Messaging Server) and **sildvsm8-2** were not specifically used in this test.

Repeat all the steps for each new entity.



7.4. Configure Entity Links

Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ⇔ Communication Manager. This entity link was created prior to the compliance test.

Navigate to **Routing → Entity Links**, and click on the **New** button (not shown) to create a new entity link. Provide the following information:

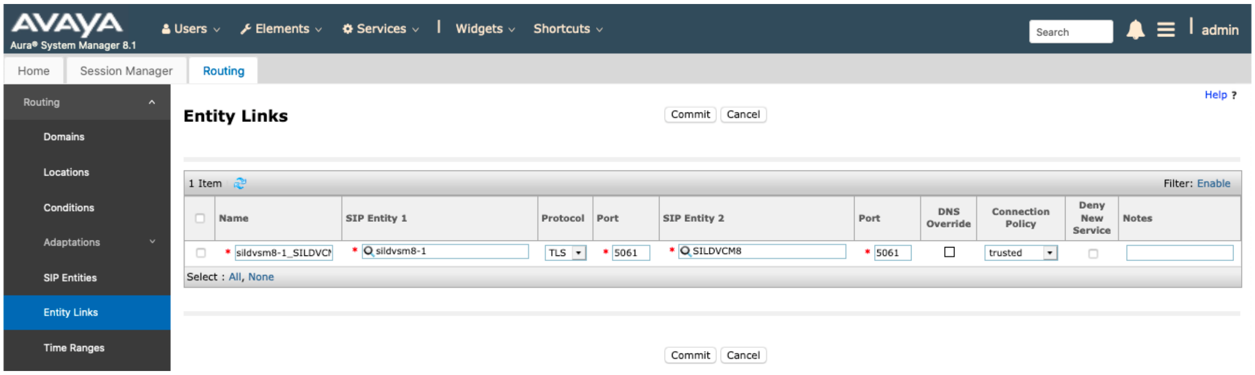
- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity shown in **Section 6.3** (e.g. **sildvsm8-1**).
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
    - TLS – 5061

©2021 Avaya Inc. All Rights Reserved.

- UDP or TCP – 5060

- In the **SIP Entity 2** drop down menu, select Communication Manager SIP entity.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Enter a description in the **Notes** field if desired.
- Accept the other default values.

Click on the **Commit** button to save each Entity Link definition.



Repeat the steps to define Entity Link using a different protocol.

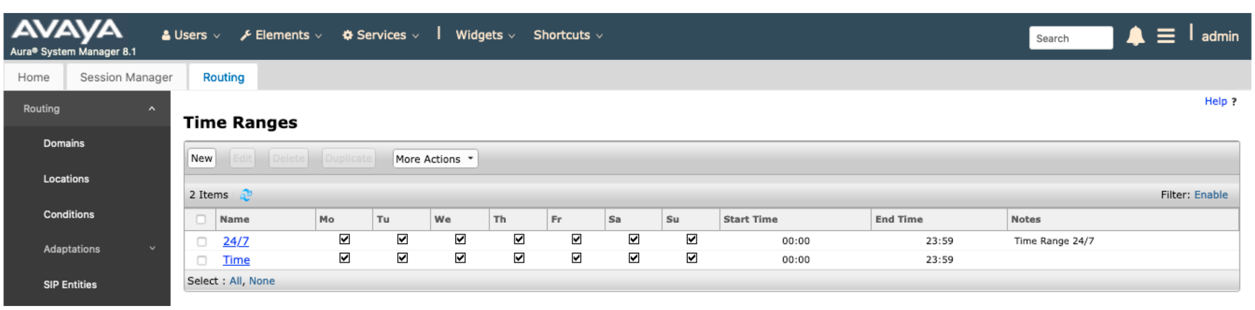
7.5. Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Section 6.6**). In the reference configuration, no restrictions were used.

To add a Time Range, navigate to **Routing → Time Ranges**, and click on the **New** button (not shown). Provide the following information:

- Enter a descriptive Time Range name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

Click the **Commit** button. The following screen shows the Time Range page used during the compliance test.



©2021 Avaya Inc. All Rights Reserved.

7.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 7.3**) with Time of Day admission control parameters (**Section 7.5**) and Dial Patterns (**Section 7.7**). In the reference configuration, Routing Policies are defined for:

- Calls to/from Communication Manager.

To add a Routing Policy, navigate to **Routing → Routing Policies**, and click on the **New** button (not shown) on the right. Provide the following information:

General section

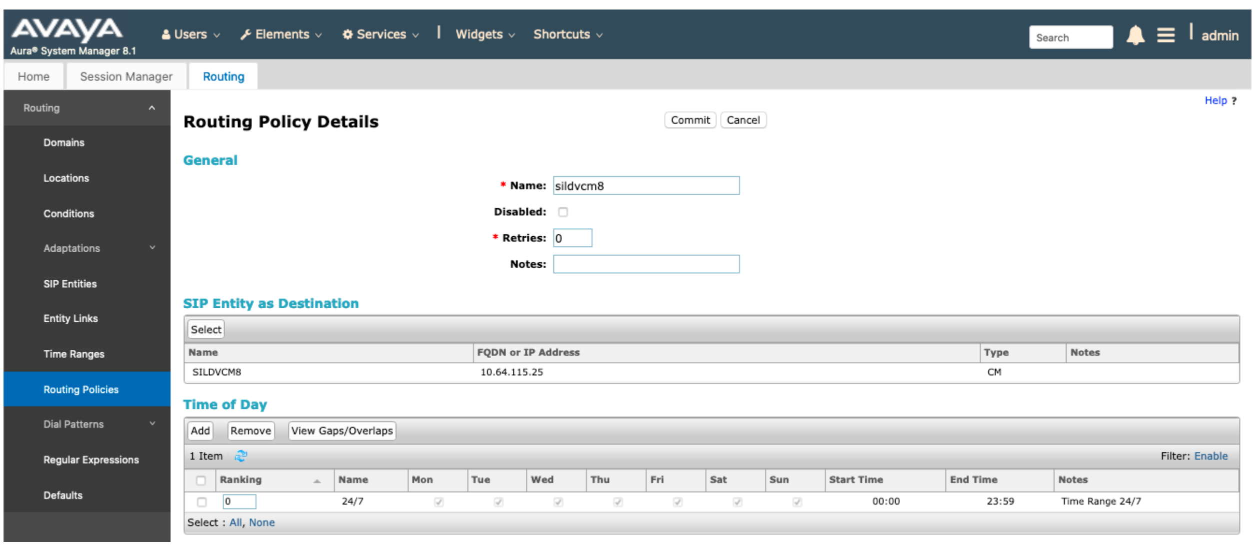
- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.

SIP Entity as Destination section

- Click the **Select** button.
- Select the SIP Entity that will be the destination for this call (not shown).
- Click the **Select** button and return to the Routing Policy Details form.

Time of Day section – Leave default values.

Click **Commit** to save Routing Policy definition. The following screen shows the Routing Policy used for the entity, **SILDVCM8**, during the compliance test.



7.7. Dial Patterns

Dial Patterns define digit strings to be matched for outbound calls. In addition, the domain in the request URI is also examined. In the compliance test, several dial patterns were defined from Session Manager.

©2021 Avaya Inc. All Rights Reserved.

To add a Dial Pattern, select **Routing → Dial Patterns,** and click on the **New** button (not shown) on the right.

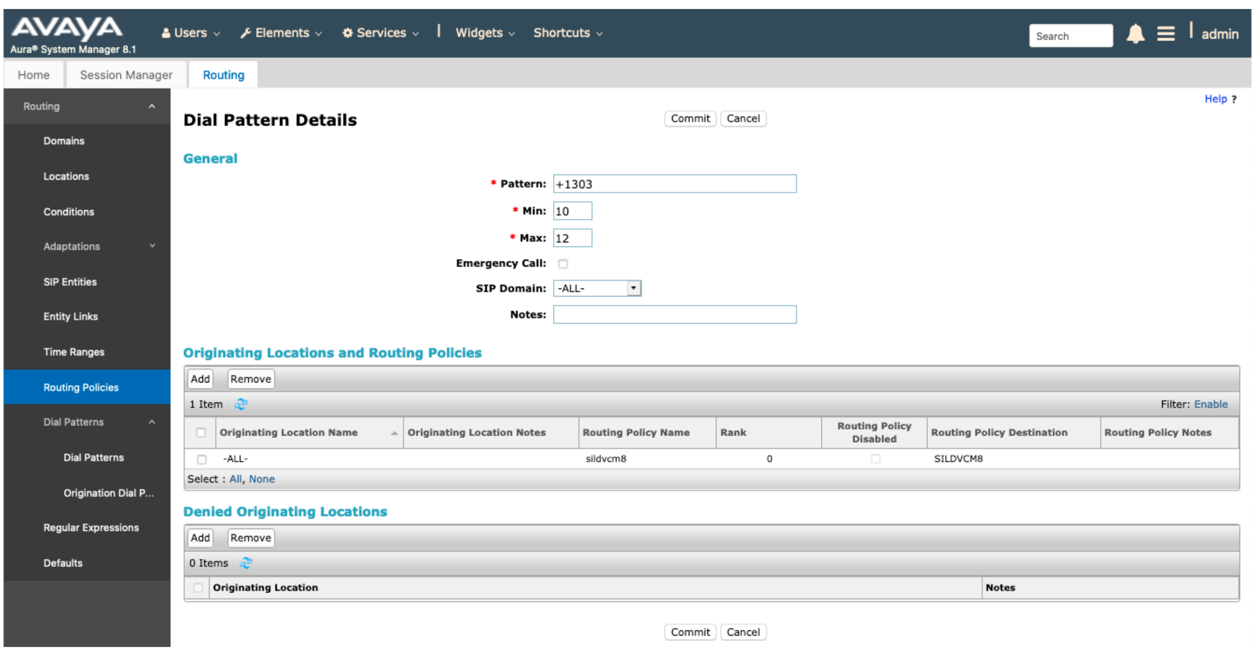
General section

- Enter a unique pattern in the **Pattern** field (e.g. **+1303**).
- In the **Min** field enter the minimum number of digits (e.g. **10**).
- In the **Max** field enter the maximum number of digits (e.g. **12**).
- In the **SIP Domain** field drop down menu select **-ALL-**
- Enter a description in the **Notes** field if desired.

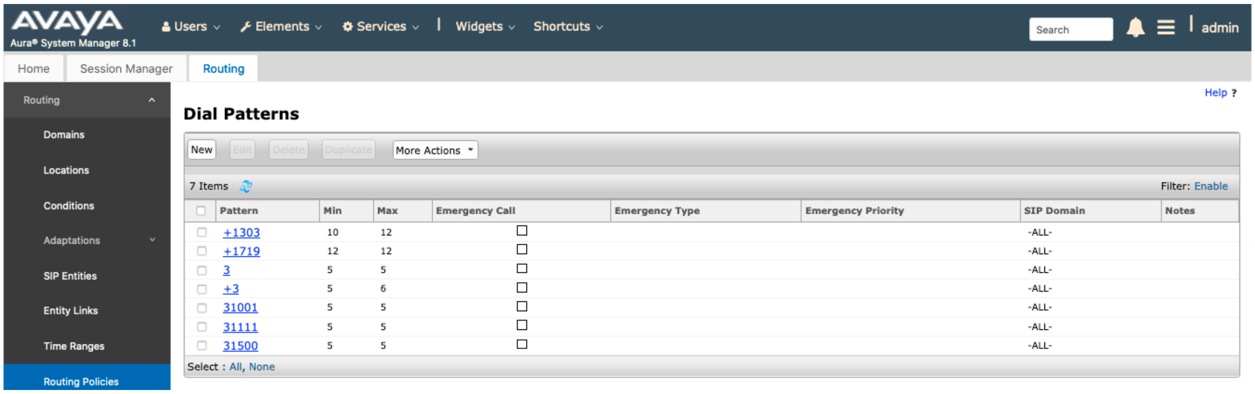
Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the boxes for the appropriate Originating Locations, and Routing Policies (see **Section 6.6**) that pertain to this Dial Pattern.
    - Originating Location –Check the **Apply The Selected Routing Policies to All Originating Locations** box (not shown).
    - Routing Policies **sildvcm8**.
    - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition. The following screen shows one of the dial patterns used for Communication Manager during the compliance test.



©2021 Avaya Inc. All Rights Reserved.

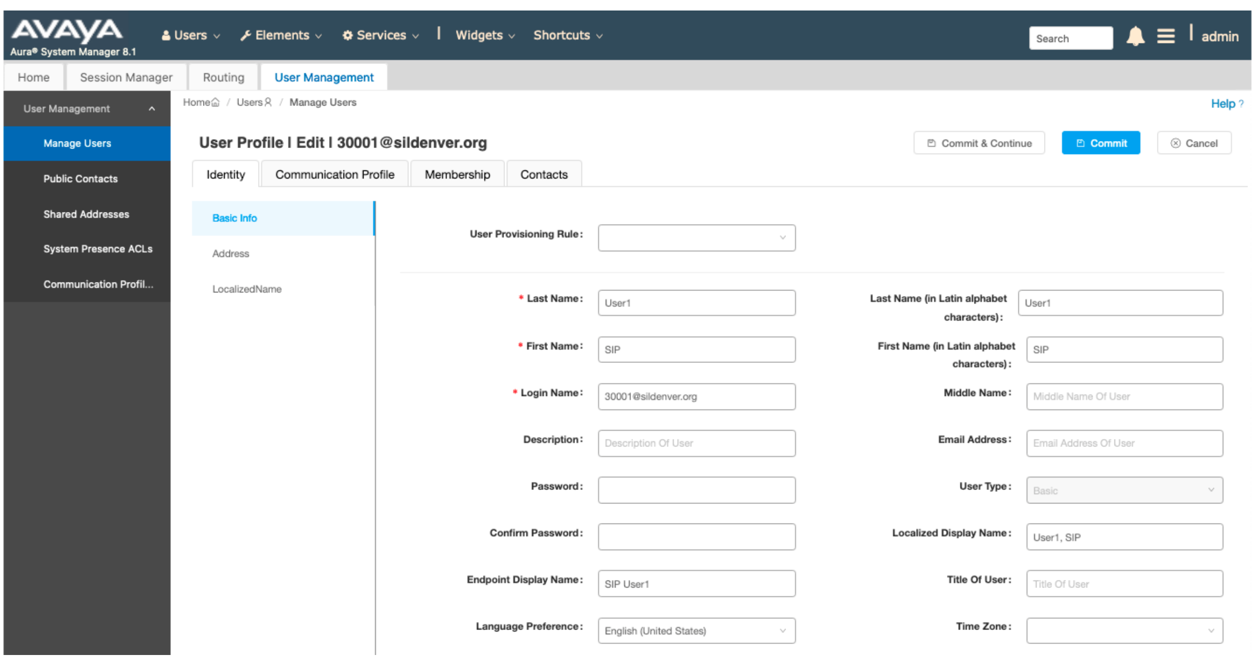


7.8. Configure SIP Users

During the compliance test, no special users were created for this solution. All users were created prior to the compliance test. However, the steps to configure a user are included.
Add new SIP users for each Synergem Evolution 911 Elite Endpoint.

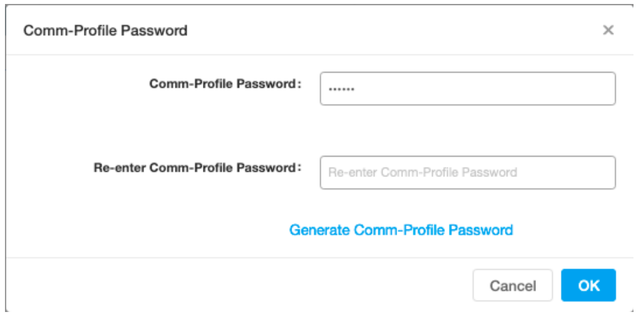
To add new SIP users, Navigate to **Home → Users → User Management→ Manage Users**. Click **New** (not shown) and provide the following information:

- Identity section
  - **Last Name –** Enter last name of user.
  - **First Name –** Enter first name of user.
  - **Login Name –** Enter extension number@sip domain name. The domain name is defined in **Section 5.3**.



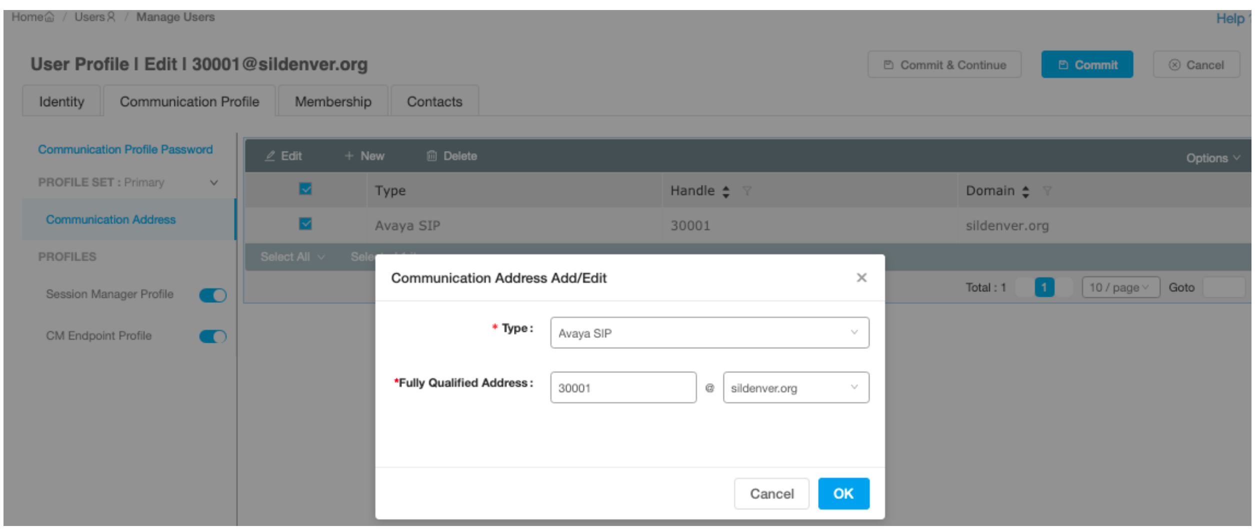
- Communication Profile section
  Provide the following information:

- **Communication Profile Password** – Enter a numeric value used to logon to SIP telephone.
- **Confirm Password** – Repeat numeric password.



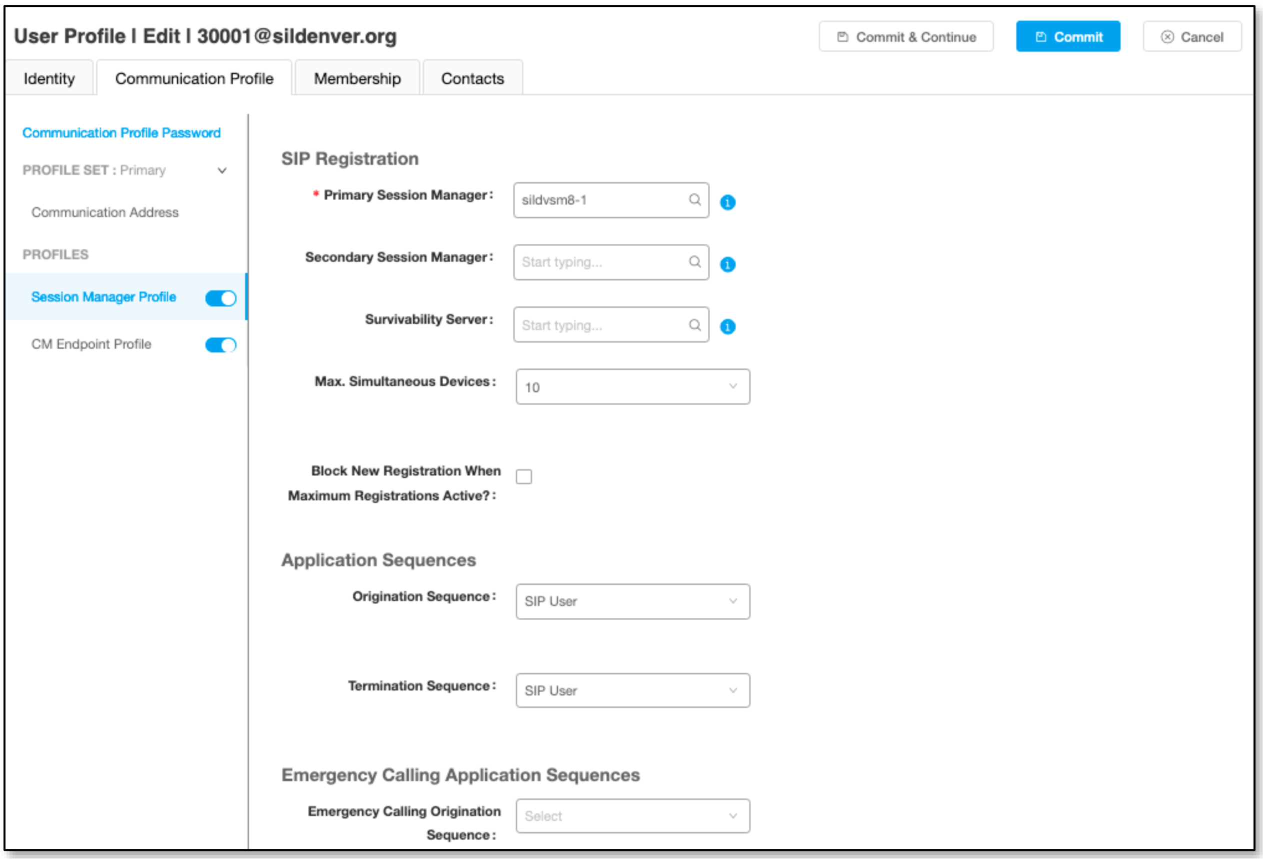
- Communication Address sub-section
  Select **New** to define a **Communication Address** for the new SIP user and provide the following information.
  - **Type** – Select **Avaya SIP** using drop-down menu.
  - **Fully Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

  Click the **Add** button to save the Communication Address for the new SIP user.



©2021 Avaya Inc. All Rights Reserved.

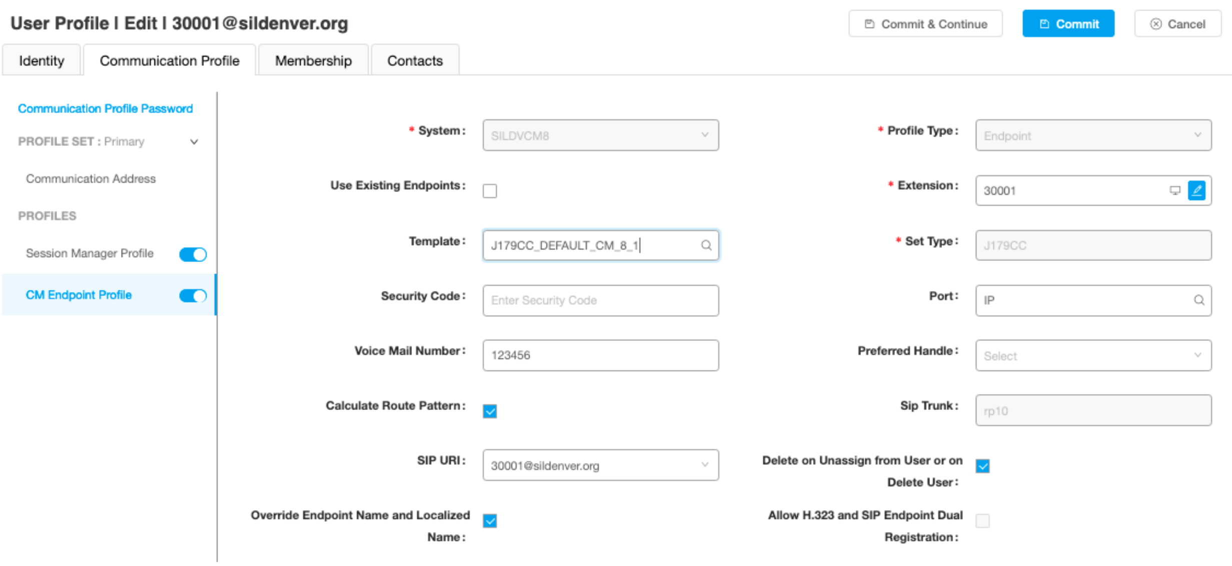
- Session Manager Profile section
    - **Primary Session Manager** – Select one of the Session Managers.
    - **Secondary Session Manager** – Select **additional servers if applicable** from drop-down menu.
    - **Origination Application Sequence –** Select Application Sequence defined (not shown) for Communication Manager.
    - **Termination Application Sequence** – Select Application Sequence defined (not shown) for Communication Manager.
    - **Home Location** – (not shown) Select Location defined in **Section 7.2**.



- CM Endpoint Profile section
    - **System** – Select Managed Element defined in **System Manager** (not shown) for Communication Manager.
    - **Use Existing Endpoints -** Leave unchecked to automatically create a new endpoint on Communication Manager when the new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
    - **Extension** - Enter same extension number used in this section.
    - **Template** – Select template for type of SIP phone. During the compliance test, J179CC_DEFAULT_CM_8_1 was selected. Note that SIPCC represents that ACD functionality can be used by the endpoint.

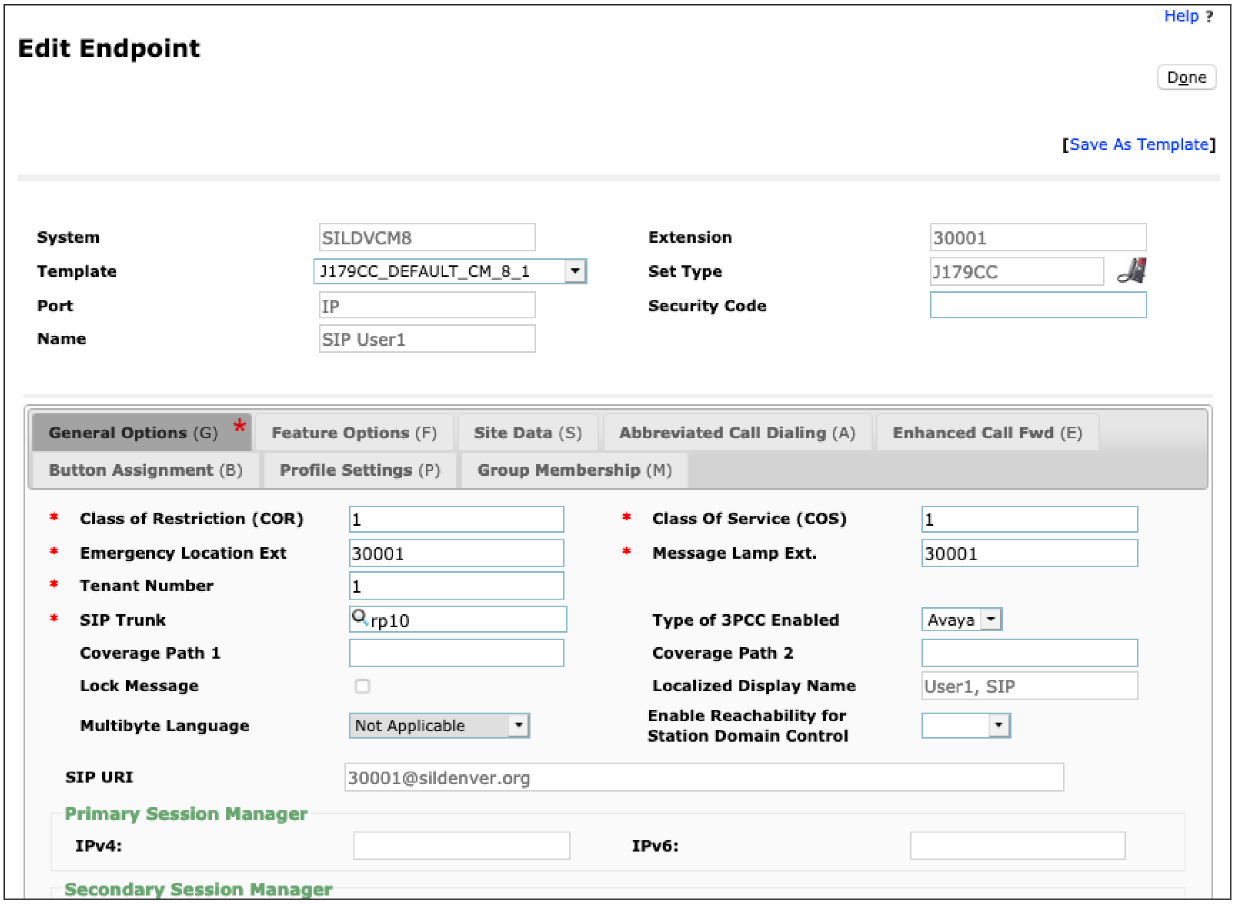
©2021 Avaya Inc. All Rights Reserved.

- **Security Code** – Enter numeric value.
- **Port** – Select **IP** from the drop-down menu
- **Voice Mail Number –** Enter **Pilot Number** for Avaya Modular Messaging if installed. Or else, leave field blank. This feature is not used during the compliance test.
- **Delete on Unassign from User or on Delete User** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.



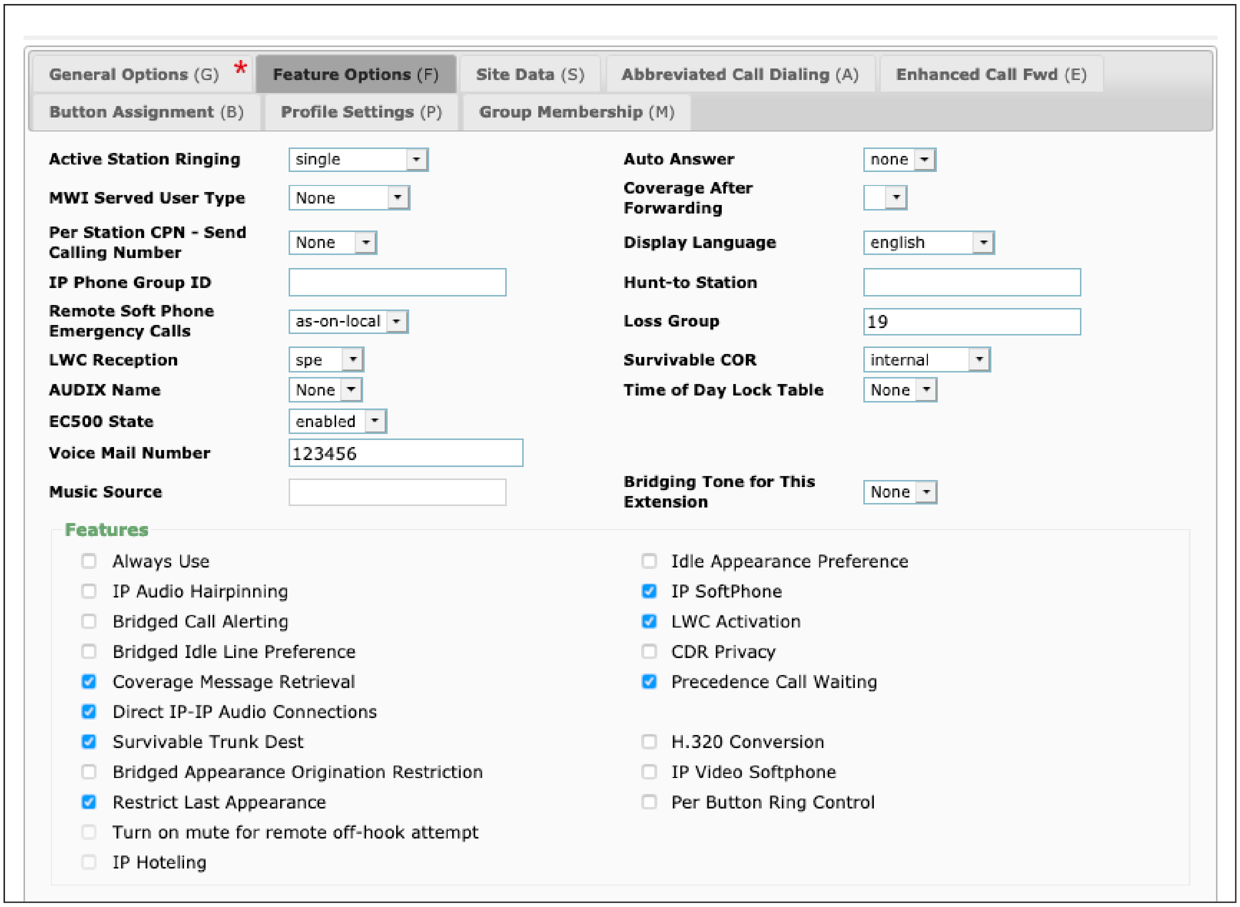
©2021 Avaya Inc. All Rights Reserved.

- Endpoint Editor:
    - Under the **General Options** tab**, Type of 3PCC Enabled –** Select **Avaya**, which enabled 3PCC functionality for DMCC.



©2021 Avaya Inc. All Rights Reserved.

- Endpoint Editor:
    - Under the **Feature Options** tab, check box for **IP SoftPhone**.



Select **Done** followed by **Commit** (not shown) to save the changes. Repeat for all SIP users included in the integration. Four endpoints were used in the compliance testing.

©2021 Avaya Inc. All Rights Reserved.

8. Configure Synergem Evolution 911 Elite™

The configuration of Evolution 911 Elite is performed by Synergem for the customer when the customer purchases Evolution 911 Elite. The information in this section is included simply as a reference. Notes that for the Supervisor Service Observation function, an H.323 DMCC station is used to join the agent calls using Service Observe Feature Access Codes. During testing, the Listen Only method was used.

AvayaAESDMCC	1
AvayaAESIPAddress	10.64.115.28
AvayaAESIPPort	4721
AvayaAESLogin	Synergem
AvayaAESPassword	***********
AvayaAESProtocol	7.0
AvayaAgentID	32000
AvayaFormSupervisorButtonFAC01Tag	*57
AvayaFormSupervisorButtonFAC01Text	Listen Only
AvayaFormSupervisorButtonFAC01Visible	1
AvayaFormSupervisorButtonFAC02Tag	*58
AvayaFormSupervisorButtonFAC02Text	Listen / Talk
AvayaFormSupervisorButtonFAC02Visible	1
AvayaFormSupervisorButtonFAC03Tag	*59
AvayaFormSupervisorButtonFAC03Text	No Talk
AvayaFormSupervisorButtonFAC03Visible	1
AvayaFormSupervisorButtonFAC04Tag	*60
AvayaFormSupervisorButtonFAC04Text	Next Call Listen Only
AvayaFormSupervisorButtonFAC04Visible	1
AvayaFormSupervisorButtonFAC05Tag	*61
AvayaFormSupervisorButtonFAC05Text	By Location Listen Only
AvayaFormSupervisorButtonFAC05Visible	1
AvayaFormSupervisorButtonFAC06Tag	*62
AvayaFormSupervisorButtonFAC06Text	By Location Listen Talk
AvayaFormSupervisorButtonFAC06Visible	1
AvayaH323Extension	30055
AvayaH323ExtensionPassword	******
AvayaSIPDomain	10.64.115.17

©2021 Avaya Inc. All Rights Reserved.

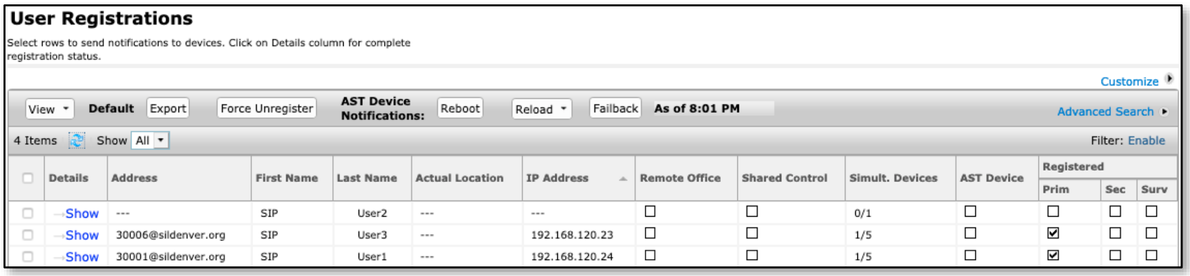
AvayaSIPLocalIP	192.168.120.21
AvayaSIPServer	10.64.115.17
AvayaSIPUserName	30001
AvayaSIPUserPassword	******
AvayaSwitchIP	10.64.115.25
AvayaSwitchName	SILDVCM8

©2021 Avaya Inc. All Rights Reserved.

9. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Evolution 911 Elite successfully registers with Session Manager by following the **Session Manager → System Status → User Registrations** link on the System Manager Web Interface.



User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

Customize

View | Default | Export | Force Unregister | AST Device Notifications: | Reboot | Reload | Failback | As of 8:01 PM | Advanced Search

4 Items | Show All | Filter: Enable

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered Prim	Registered Sec	Registered Surv
Show	---	SIP	User2	---	---	☐	☐	0/1	☐	☐	☐	☐
Show	30006@sildenver.org	SIP	User3	---	192.168.120.23	☐	☐	1/5	☐	☑	☐	☐
Show	30001@sildenver.org	SIP	User1	---	192.168.120.24	☐	☐	1/5	☐	☑	☐	☐

- Place calls to and from Synergem Evolution 911 Elite and verify that the ACD calls are successfully established with two-way talk path.
- While calls are established, enter **status trunk <t:n>** command on Communication Manager, where **t** is the SIP trunk group configured in **Section 5.6**, and **n** is trunk group member. This will verify whether the call is shuffled or not.

```
status trunk 10/1                                               Page    3 of    3
                      SRC PORT TO DEST PORT TALKPATH
src port: T000001
T000001:TX:192.168.4.132:5004/g722-64/20ms/1-srtp-aescm128-hmac80
AMS1:RX:10.64.115.3:6022/g722-64/20ms/1-srtp-aescm128-hmac80:TX:cnfID:0
AMS1:RX:cnfID:0:TX:10.64.115.3:6024/g711u/20ms
T000006:RX:192.168.120.24:27000/g711u/20ms
```

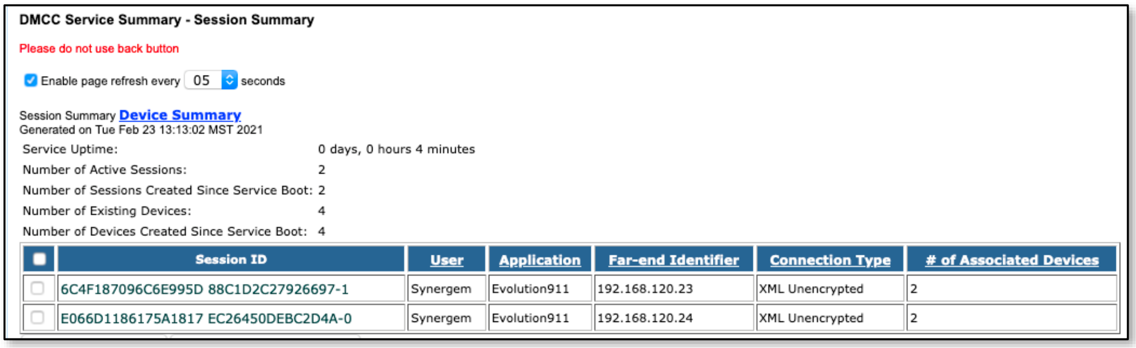
- To verify agent login status, use **status station <n>** where **n** is the Agent ID.

```
status station 32002                                            Page    7 of    7
                                   ACD STATUS

 Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod
   1/MI      /        /        /        /        /        /     On ACD Call? no
    /        /        /        /        /        /        /
    /        /        /        /        /        /        /      Occupancy: 73.3
```


©2021 Avaya Inc. All Rights Reserved.

- To verify DMCC registrations, view the **Status → DMCC Service Summary** on AES. The following shows two active registrations, each session has two associated devices, the agent or supervisor extension and the DMCC Service Observe port. Normally, agents would only show one association but for testing, both clients were configured to be able to Service Observe.



DMCC Service Summary - Session Summary

Please do not use back button

Enable page refresh every 05 seconds

Session Summary Device Summary
Generated on Tue Feb 23 13:13:02 MST 2021

Service Uptime:	0 days, 0 hours 4 minutes
Number of Active Sessions:	2
Number of Sessions Created Since Service Boot:	2
Number of Existing Devices:	4
Number of Devices Created Since Service Boot:	4

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
	6C4F187096C6E995D 88C1D2C27926697-1	Synergem	Evolution911	192.168.120.23	XML Unencrypted	2
	E066D1186175A1817 EC26450DEBC2D4A-0	Synergem	Evolution911	192.168.120.24	XML Unencrypted	2

- Verify the Evolution 911 Elite successfully starts monitors for stations via DMCC on the CTI link by using **list monitored-station** command.

```
list monitored-station

                              MONITORED STATION

   Associations:      1        2        3        4        5        6        7        8
                 CTI      CTI      CTI      CTI      CTI      CTI      CTI      CTI
Station Ext      Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV Lnk  CRV
---------------- -------- -------- -------- -------- -------- -------- -------- --------
30001            1   0004
30006            1   0008
```

10. Conclusion

Evolution 911 Elite was compliance tested with Communication Manager and Session Manager, and Application Enablement Services Synergem Evolution 911 Elite functioned properly for feature and serviceability. During compliance testing, Evolution 911 Elite successfully registered with Session Manager, placed and received calls to and from SIP and non-SIP telephones, and executed other telephony features like three-way conference, hold, etc.

11. Additional References

The following Avaya product documentation can be found at http://support.avaya.com

[1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x
[2] *Administering Avaya® Session Manager*, Release 8.1.x
[3] *Administering Avaya® System Manager*, Release 8.1.x
[4] *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x

©2021 Avaya Inc. All Rights Reserved.

©2021 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.