



Application Notes for Configuring Avaya Aura™ Presence Services 6.0 with Avaya Aura™ Session Manager 6.0, and Avaya Aura™ Communication Manager for one-X™ Communicator clients as part of Avaya Unified Communication Mobile Worker Solution – Issue 1.0

Abstract

These Application Notes describe the steps required to configure Avaya Aura™ Presence Services with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager as a Feature Server and Avaya Aura™ Communication Manager as an Evolution Server as part of Avaya Unified Communication Mobile Worker Solution. Avaya Aura™ Presence Services is a single point of presence collection which provides facilities for gathering presence information from SIP one-X™ Communicator end point registered on Avaya Aura™ Session Manager.

1. Introduction

These Application Notes describe the steps required to configure Avaya Aura™ Presence Services with Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager Feature Server and Avaya Aura™ Communication Manager Feature Server as part of Avaya Unified Communication Mobile Worker Solution. **Figure 1** shows the overall context in which the testing for these Application Notes took place. The scenario was designed to test Avaya Unified Communication Mobile Worker Solution, which allows users in different locations to have full access to Avaya services. The configuration can be broken down into four types of users or locations:

- Enterprise Office User
- Remote User
- Branch1 Office User – Midsize Business Template (MBT)
- Branch2 Office User – Branch Session Manager (BSM)

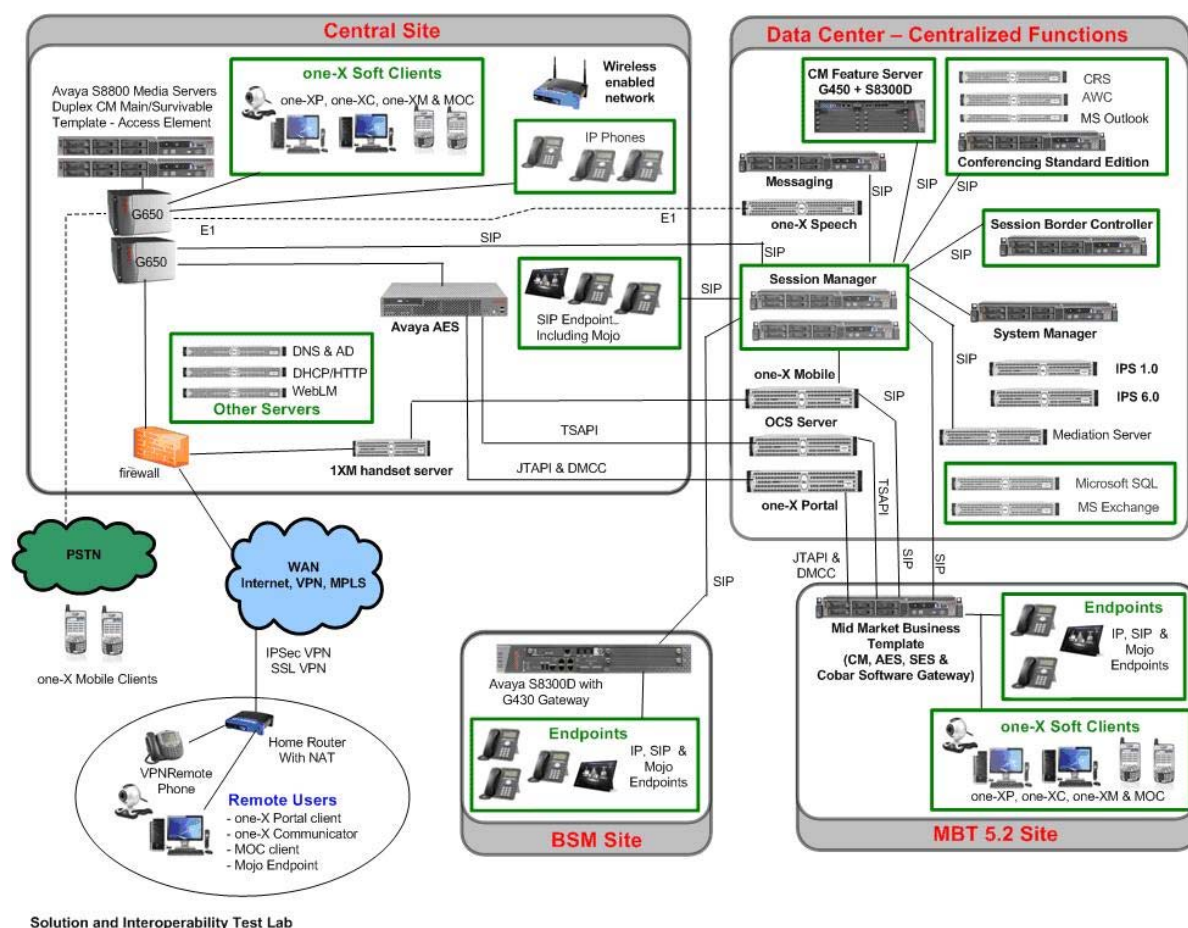


Figure 1: Sample Avaya Unified Communication Mobile Worker Solution

The Enterprise Office User has access to services via normal corporate network connections including wireless LAN. Services include access to centralized Avaya Modular Messaging

(voicemail), Avaya one-X[®] Speech functionality, Avaya Web Conferencing, Avaya Aura[™] Conferencing Standard Edition, Avaya Aura[™] Presence Services and wireless network or GSM connection for Avaya one-X[®] Mobile enabled handsets. Avaya Aura[™] Communication Managers reside on both Enterprise and Branch Sites. End users are configured to use a variety of end points including one-X[®] Communicator, one-X[®] Portal, Avaya desk phones and a selection of third party mobile phones. EC 500 and Feature Name Extensions (FNEs) are also configured.

The Remote User has access to the same services on the Enterprise Site by using either an SSL or IPSEC VPN connection. The Remote User can be located in a home office, an airport, a hotel room or anywhere with access to either a GSM or network connection. In these cases the one-X[®] Mobile, one-X[®] Communicator and Avaya 9630 VPN desk phone can be used as end points.

The Branch1 Office User is situated in a separate office location. The Branch Office uses the centralized services located at the Enterprise Office. Connection of one-X[®] Mobile to Avaya Aura[™] Communication Manager is again via GSM or wireless network depending on the location. There is Avaya Aura[™] Midsize Business Template (MBT) running Avaya Aura[™] Communication Manager in this office.

The Branch2 Office User is situated in a separate office location. The Branch2 Office again uses the centralized services located at the Enterprise Office. It however contains a Branch Session Manager (BSM) that will provide continued local connectivity and SIP phone registration in the event of an outage at the Enterprise Office.

For the purposes of these Application Notes, only the configuration relevant to Avaya Aura™ Presence Services, Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager Feature Server, Avaya Aura™ Communication Manager Evolution Server and one-X™ Communicator SIP phones will be described in detail as shown in **Figure 2**.

Avaya Aura™ Presence Services is a single point of presence collection. It provides facilities for gathering presence information from a diverse range of sources, aggregating this information on a per user basis, and then making it available to consuming or subscribing applications. In the tested solution, Avaya Aura™ Presence Services was gathering presence information from one-X® Communicator SIP phones registered on Avaya Aura™ Session Manager. Avaya Aura™ Presence Services also provides facilities which Avaya Enterprise application solutions can use to publish their own users' presence. Presence aware applications like Avaya one-X® Communicator uses the subscribe to Avaya Aura™ Presence Services, to receive presence change notifications containing aggregated presence information for a user and the communication resources that user has available to them. This information can be used to provide visual indications about a user's availability to an end user client GUI, like Avaya one-X® Communicator.

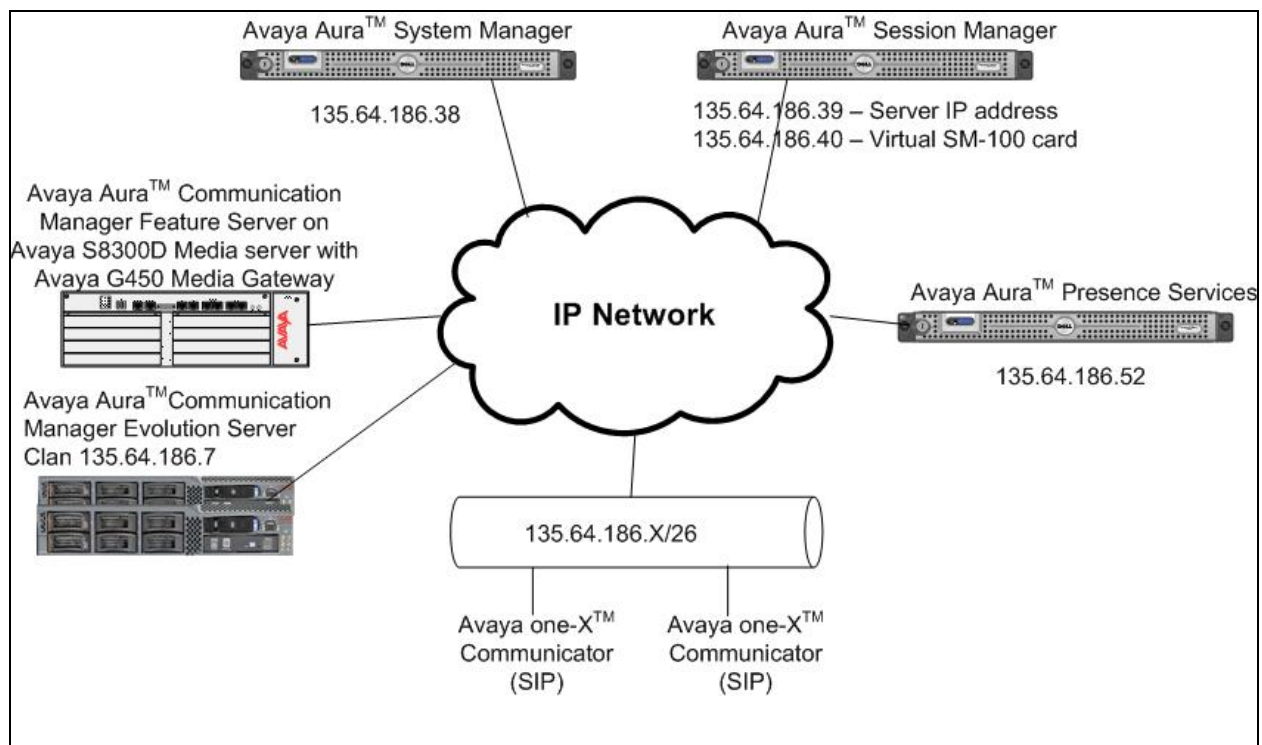


Figure 2: Test Configuration used in these Application Notes

2. Equipment and Software Validated

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

Component	Version
Avaya G450 Media Gateway with Avaya S8300D Server	Avaya Aura™ Communication Manager Feature Server 6.0 on Avaya Virtual System Platform 6.0 Patch 1002
Avaya G650 Media Gateway with S8300D Server	Avaya Aura™ Communication Manager Evolution Server 6.0 on Avaya Virtual System Platform 6.0 Patch 1002
Avaya S8510 Server	Avaya Aura™ System Manager 6.0 on Virtual System Platform 6.0 (600020)
Avaya S8510 Server	Avaya Aura™ Session Manager 6.0 on Virtual System Platform 6.1 SP1 (6.0.1.0.601009)
Avaya S8510 Server	Avaya Aura™ Presence Services 6.0 on Virtual System Platform 6.0 (6.0 06.00.00.00-0912)
Avaya one-X™ Communicator (SIP)	Avaya one-X® 6.0000-GA-23067

3. Configure Avaya Aura™ Communication Manager Feature Server

This section shows the configuration of Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assumed that the basic configuration has already been administered. For further information on Communication Manager, please see references [4] and [5]. The procedures include the following areas:

- Verify Avaya Aura™ Communication Manager License
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region
- Administer SIP Signaling Group
- Administer SIP Trunk Group
- Administer Route Pattern
- Administer Private Numbering
- Administer Dial Plan and AAR analysis
- Save Changes

3.1. Verify Avaya Aura™ Communication Manager License

Use the **display system-parameter customer options** command to compare the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

Note: The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                               Page 2 of 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 4000 0
      Maximum Concurrently Registered IP Stations: 2400 0
      Maximum Administered Remote Office Trunks: 4000 0
Maximum Concurrently Registered Remote Office Stations: 2400 0
      Maximum Concurrently Registered IP eCons: 68 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 2400 0
      Maximum Video Capable IP Softphones: 2400 1
      Maximum Administered SIP Trunks: 4000 60
Maximum Administered Ad-hoc Video Conferencing Ports: 4000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 80 0
      Maximum TN2501 VAL Boards: 10 0
      Maximum Media Gateway VAL Sources: 50 0
      Maximum TN2602 Boards with 80 VoIP Channels: 128 0
      Maximum TN2602 Boards with 320 VoIP Channels: 128 0
      Maximum Number of Expanded Meet-me Conference Ports: 300 0
```

Go to **Page 5** and enable **Private Networking**.

```
display system-parameters customer-options                               Page 5 of 11
                                OPTIONAL FEATURES

    Multinational Locations? n                Station and Trunk MSP? y
    Multiple Level Precedence & Preemption? n    Station as Virtual Extension? y
        Multiple Locations? n
    Personal Station Access (PSA)? y            System Management Data Transfer? n
        PNC Duplication? n                    Tenant Partitioning? y
        Port Network Support? n                Terminal Trans. Init. (TTI)? y
        Posted Messages? y                    Time of Day Routing? y
        Private Networking? y                TN2501 VAL Maximum Capacity? y
        Processor and System MSP? y            Uniform Dialing Plan? y
        Processor Ethernet? y                Usage Allocation Enhancements? y
        Remote Office? y                    Wideband Switching? y
    Restrict Call Forward Off Net? y            Wireless? n
        Secondary Data Module? y
```

3.2. Administer System Parameters Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to allow for transferring an incoming/outgoing call from/to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to **all** to enable all trunk-to-trunk transfers on a system wide basis.

Note: This feature poses significant security risk and must be used with caution. As an alternative, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels.

```
change system-parameters features                                       Page 1 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS
                                Self Station Display Enabled? n
                                Trunk-to-Trunk Transfer: all
    Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
        Call Park Timeout Interval (minutes): 10
    Off-Premises Tone Detect Timeout Interval (seconds): 20
        AAR/ARS Dial Tone Required? y

    Music (or Silence) on Transferred Trunk Calls? no
        DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attdd-Extended/Transferred Calls: transferred
        Automatic Circuit Assurance (ACA) Enabled? n

    Abbreviated Dial Programming by Assigned Lists? n
    Auto Abbreviated/Delayed Transition Interval (rings): 2
        Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

3.3. Administer IP Node Names

Use the **change node-names ip** command to add entries for the Communication Manager and Session Manager that will be used for connectivity. In the sample network, **procr** and **135.64.186.55** are configured as **Name** and **IP Address** for the Communication Manager running on Avaya S8300D Server. In addition, **SM** and **135.64.186.40** are entered for the virtual SM-100 interface on Session Manager.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SILStackAES	135.64.186.28	
SM	135.64.186.40	
default	0.0.0.0	
onexmobile	135.64.186.30	
procr	135.64.186.55	

3.4. Administer IP Network Region

Use the **change ip-network-region n** command, where **n** is the network region number to configure the network region being used. In the sample network, ip-network-region **1** is used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec Set** to **1** to use ip-codec-set 1.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: silstack.com	
Name: To ASM		
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		

3.5. Administer SIP Signaling Group

In the test configuration, Communication Manager acts as a Feature Server therefore an IMS enabled SIP trunk is required. Use signaling group 50 along with trunk group 50 to reach the Session Manager. Use the **add signaling-group n** command, where **n** is the signaling-group number being added to the system. The following screens show the settings configured for signaling group 50.

Note: The **Peer Server** field is automatically populated by Communication Manager when the trunk goes in service.

```
change signaling-group 50                                     Page 1 of 1
SIGNALING GROUP
Group Number: 50      Group Type: sip
IMS Enabled? y      Transport Method: tls
Q-SIP? n
IP Video? n
Peer Detection Enabled? y Peer Server: SM
SIP Enabled LSP? n
Enforce SIPS URI for SRTP? y

Near-end Node Name: procr      Far-end Node Name: SM
Near-end Listen Port: 5065      Far-end Listen Port: 5065
Far-end Network Region: 1
Far-end Domain: silstack.com

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

3.6. Administer SIP Trunk Group

Use the **add trunk-group n** command, where **n** is the new trunk group number being added to the system. The following screens show the settings used for trunk group 50.

```
add trunk-group 50                                           Page 1 of 21
TRUNK GROUP
Group Number: 50      Group Type: sip      CDR Reports: y
Group Name: Avaya SIP Phones      COR: 1      TN: 1      TAC: 150
Direction: two-way      Outgoing Display? n
Dial Access? n      Night Service:
Queue Length: 0
Service Type: tie      Auth Code? n
Signaling Group: 50
Number of Members: 10
```

Navigate to **Page 3** and enter **private** for **Numbering Format**.

```

add trunk-group 50                                     Page 3 of 21
TRUNK FEATURES
    ACA Assignment? n                                Measured: none
                                                    Maintenance Tests? y

    Numbering Format: private
                                                    UII Treatment: service-provider

                                                    Replace Restricted Numbers? n
                                                    Replace Unavailable Numbers? n

    Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
  
```

Navigate to **Page 4** and enter **120** for **Telephone Event Payload Type**.

```

add trunk-group 50                                     Page 4 of 21

    PROTOCOL VARIATIONS

        Mark Users as Phone? n
        Prepend '+' to Calling Number? n
        Send Transferring Party Information? n

        Send Diversion Header? n
        Support Request History? y
        Telephone Event Payload Type: 120

        Convert 180 to 183 for Early Media? n
        Always Use re-INVITE for Display Updates? n
        Enable Q-SIP? n
  
```

3.7. Administer Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use the **change route-pattern n** command, where **n** is the route pattern number being added to the system. Configure this route pattern to route calls to trunk group number **50** configured in **Section 3.6**.

```

change route-pattern 50                               Page 1 of 3
    Pattern Number: 50  Pattern Name: To ASM
    SCCAN? n      Secure SIP? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted          DCS/ IXC
    No      Mrk Lmt List Del  Digits                QSIG
                                           Dgts      Intw
1: 50      0                                0          n   user
2:                                     n   user
3:                                     n   user
4:                                     n   user
5:                                     n   user
6:                                     n   user

    BCC VALUE  TSC CA-TSC  ITC BCIE Service/Feature PARM No. Numbering LAR
    0 1 2 M 4 W      Request      Dgts Format
                                           Subaddress
1: y y y y y n n      unre
2: y y y y y n n      rest
3: y y y y y n n      rest
4: y y y y y n n      rest
5: y y y y y n n      rest
6: y y y y y n n      rest
  
```

3.8. Administer Private Numbering

Use the **change private-numbering** command to define the calling party number to be sent out through the SIP trunk. In the sample network configuration, all calls originating from a 5-digit extension beginning with 34 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

```
change private-numbering 0                               Page 1 of 2
NUMBERING - PRIVATE FORMAT

Ext Len  Ext Code      Trk Grp(s)  Private Prefix  Total Len
  5   34              50                5
Total Administered: 1
Maximum Entries: 540
```

3.9. Administer Dial Plan and AAR analysis

Configure the dial plan for dialing 5-digit extensions beginning with 34 that will be registered on Session Manager. Use the **change dialplan analysis** command to define **Dialed String 34** as an **ext Call Type**.

```
change dialplan analysis                                Page 1 of 12
DIAL PLAN ANALYSIS TABLE
Location: all                                           Percent Full: 2

Dialed String  Total Length  Call Type  Dialed String  Total Length  Call Type  Dialed String  Total Length  Call Type
1              3          dac          34             5          ext          40             5          aar
2              5          ext          42             5          aar          7              5          aar
8              5          aar          80958          5          ext          9              1          fac
*              1          fac
```

Use the **change aar analysis n** command where **n** is the dial string pattern to configure an **aar** entry for **Dialed String 34** to use **Route Pattern 50**.

```
change aar analysis 34                                Page 1 of 2
AAR DIGIT ANALYSIS TABLE
Location: all                                           Percent Full: 2

Dialed String  Total Min  Total Max  Route Pattern  Call Type  Node Num  ANI Req'd
34             5        5        50            aar        n         n
40             5        5        50            unku       n         n
42             5        5        50            unku       n         n
6              5        5        50            unku       n         n
71111          5        5        50            lev0       n         n
8              5        5        50            unku       n         n
80958          5        5        50            aar        n         n
```

3.10. Save Changes

Use the **save translation** command to save all changes.

4. Configure Avaya Aura™ Presence Services

This section deals with the configuration of Presence Services. It is assumed that Presence Services server is installed as described in reference [6]. Presence Services interacts with several external entities like presence sources or user management services in order to gather and provide presence information. Configuration with these external entities is performed during installation of the Presence Services, therefore the steps below will only verify that the configuration in place is correct.

The configuration management is performed through the **XCP Controller** web-based GUI. Initialize the XCP Controller web interface by browsing to **https:// <ip-address>:7300/admin**, where <ip-address> is the IP address of the Presence Services server and log in with the appropriate credentials. The XCP controller web-based GUI is displayed as shown below.

XCP Controller - presence

[Home] [Logoff] Configuration view: **Basic**

System

[Summary] [Cluster] [Stop the System] [Online Help]

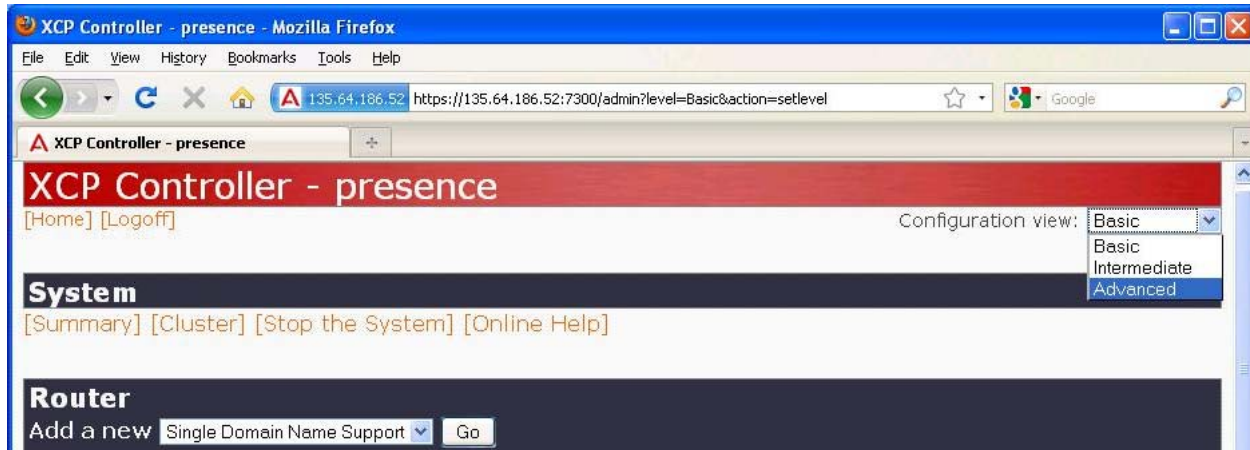
Router

Add a new

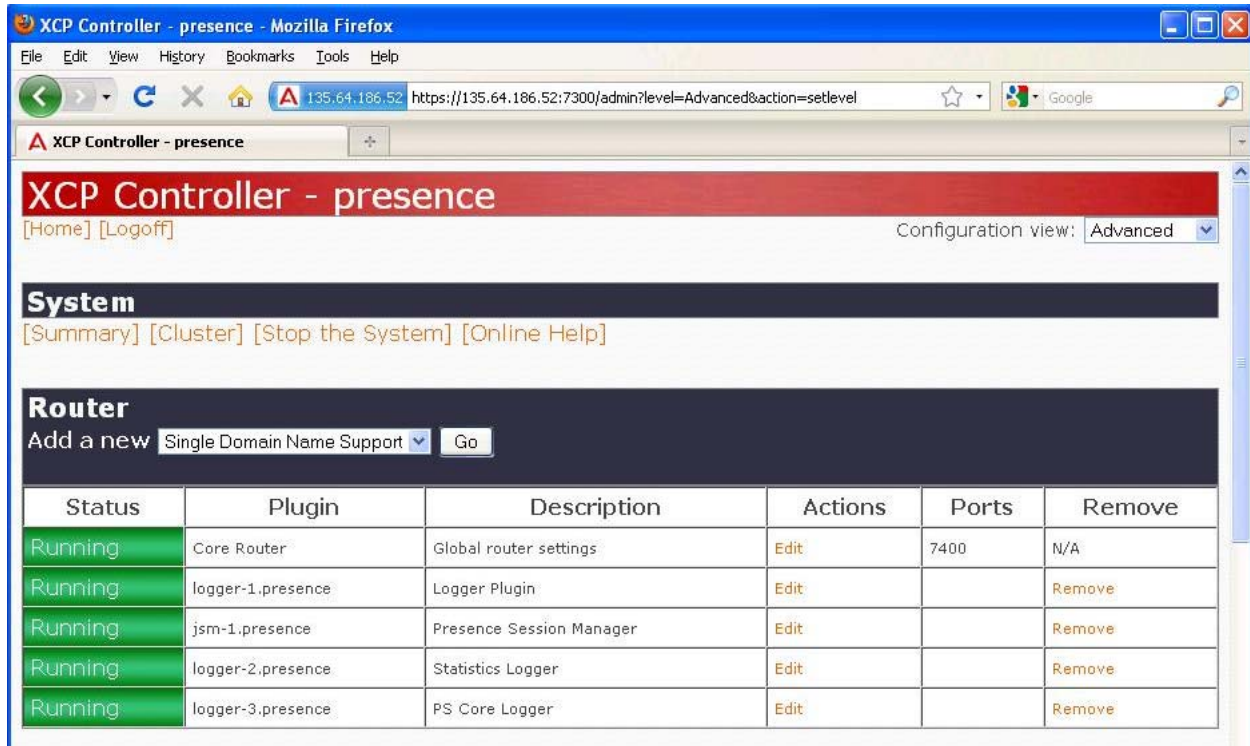
Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.presence	Logger Plugin	Edit		Remove
Running	jsm-1.presence	Presence Session Manager	Edit		Remove
Running	logger-2.presence	Statistics Logger	Edit		Remove
Running	logger-3.presence	PS Core Logger	Edit		Remove

4.1. Verify Avaya Aura™ Session Manager is configured as Trusted Host on Presence Services

The steps below document how to configure Session Manager as a trusted host on Presence Services. In the **Configuration view**, located on the right hand side of the XCP Controller, select **Advanced** from the drop down list.



After setting advanced configuration view, navigate to the **Router** section of the XCP Controller and click the **Edit** action for the **Global router settings**.



On the **Global Settings Configuration** page that appears scroll down to display **Mutually Trusted TLS Hostnames**. Ensure that IP address of the virtual SM-100 interface on Session Manager is configured in the **Host Filters**, and if not add that IP address. In this case the IP address of the virtual SM-100 interface is **135.64.186.40** as shown below. Click **Submit** to save changes.

The screenshot shows the 'XCP Controller - presence' configuration page in Mozilla Firefox. The browser's address bar shows the URL <https://135.64.186.52/admin?action=view&xpath=/jabber/global>. The page contains several configuration fields:

- Database User Name: xcp_user *
- Database User's Password: [masked] *
- Confirm Password: [masked] *
- Database Type: postgresql-odbc *
- Number of connections to the database: 20 *
- Time in seconds between database connection heartbeats: 60 *
- Is database debug logging enabled?: 0 *
- ☐ SNMP Configuration
 - Enable SNMP: Yes
 - Count errors: No
- Mutually Trusted TLS Hostnames**
 - Separate each hostname (or IP address) with a line break.
 - Host Filters**
 - host:
 - ips60
 - 135.64.186.40

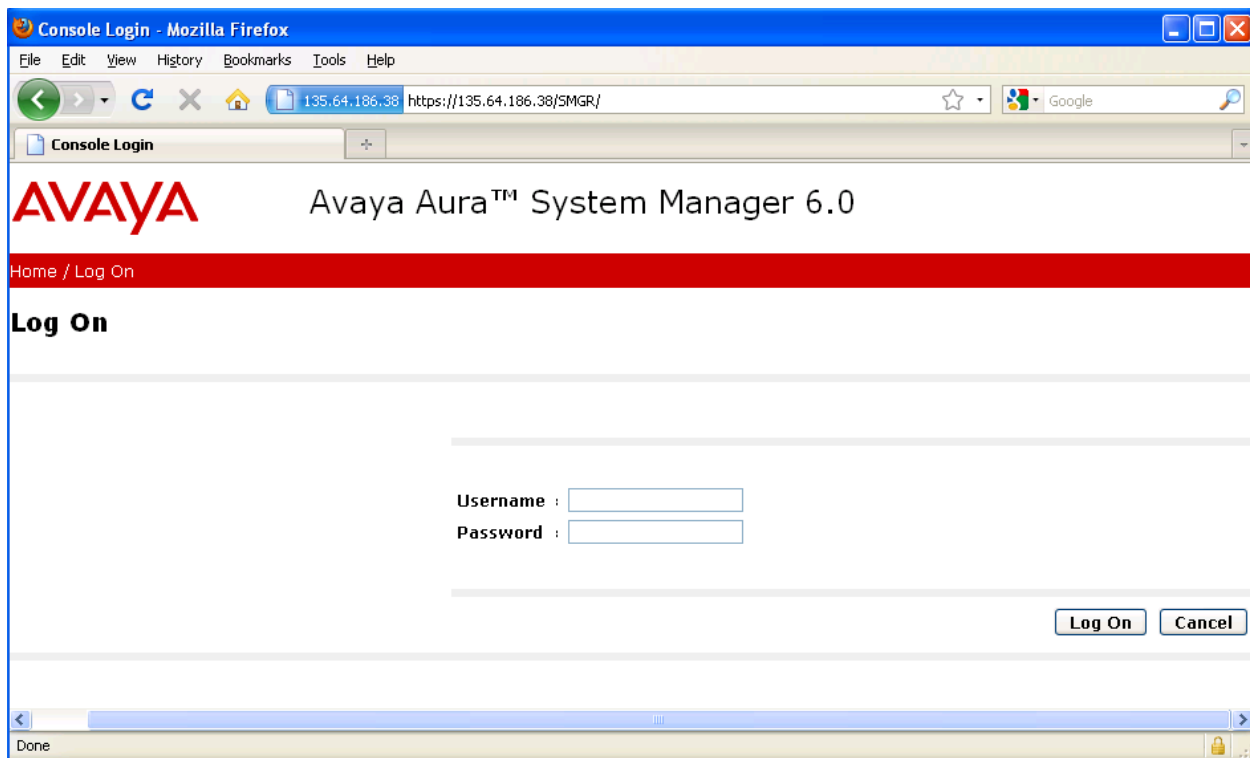
At the bottom of the page are three buttons: Submit, Reset, and Cancel.

5. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager. The configuration steps include the following areas:

- Administer SIP Domain
- Administer Domain Substitution rule for Avaya Aura™ Presence Services
- Administer SIP Elements
- Administer Element Links
- Administer Session Manager
- Add Communication Manager Feature Server as a Managed Element and define Application Sequence
- Configure Users for SIP Avaya one-X™ Communicator

For further information on configuration, please consult with references [1], [2], and [3]. Access System Manager using a Web Browser and entering **https://<ip-address>/SMGR**, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials.



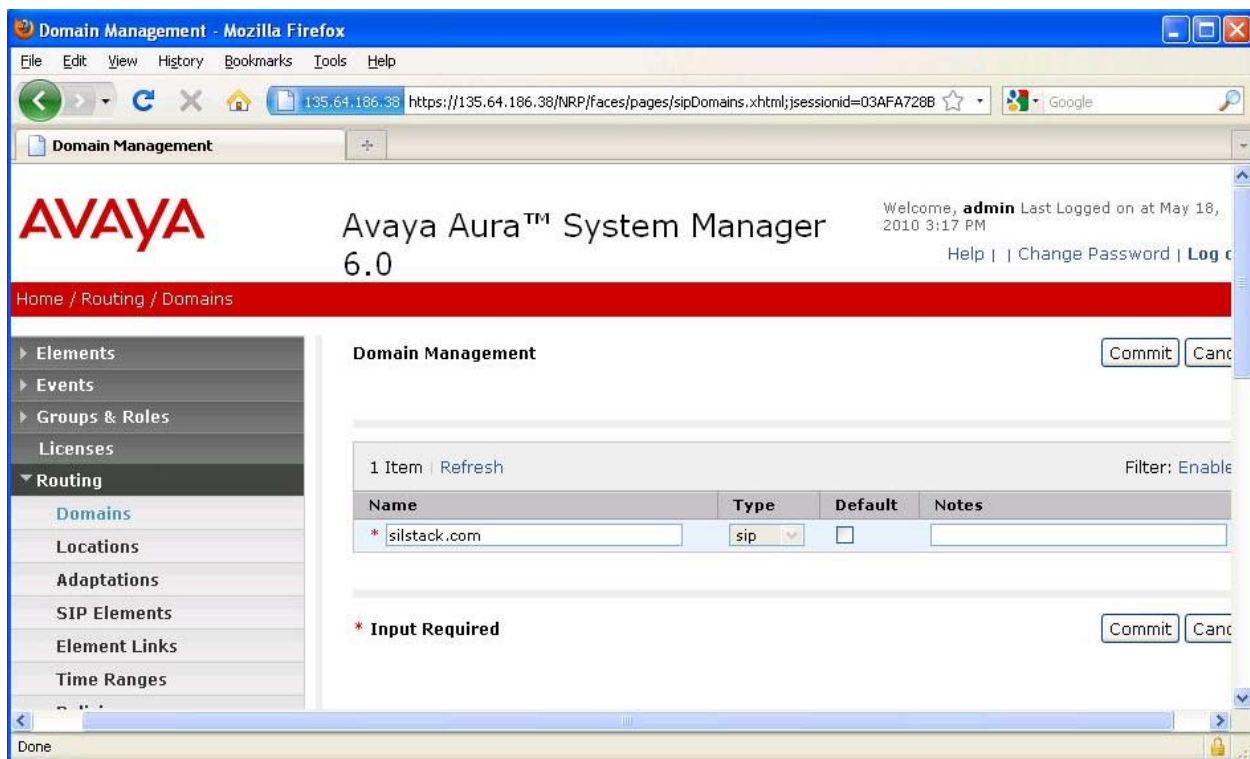
5.1. Administer SIP Domain

Add the SIP domain, for which the communications infrastructure will be authoritative, by selecting **Routing** → **Domain** on the left panel menu and clicking the **New** button (not shown) to create a new SIP domain entry. The following screen will be shown after clicking **New**.

- **Name:** Enter the authoritative domain name; in this case that is **silstack.com**
- **Notes:** Description for the domain (optional)

Click **Commit** to save changes.

Note: Since the sample network does not deal with any foreign domains, no additional SIP Domains entry is needed.

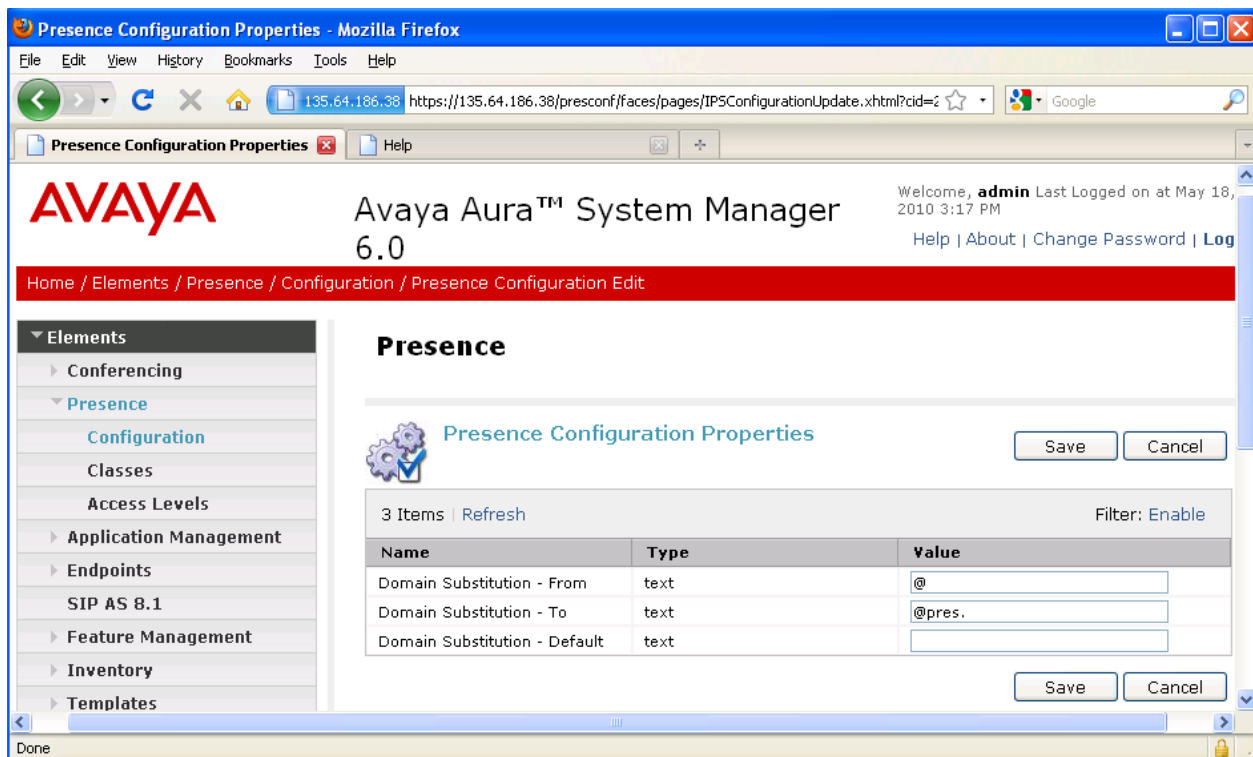


5.2. Administer Domain Substitution rule for Avaya Aura™ Presence Services

To configure a Domain Substitution rule for Presence Services, select **Element** → **Presence** → **Configuration** on the left panel menu and then click on the **Edit** button (not shown). In the **Presence Configuration Properties** page that appears set following values:

- **Domain Substitution – From:** Enter a value from which the substitution will be made; in this case that is @
- **Domain Substitution – To:** Enter a value from which the substitution will be made; in this case that is @pres.

Click **Save** to save changes.



The screenshot shows the Avaya Aura System Manager 6.0 web interface. The left sidebar contains a menu with 'Elements' expanded, showing 'Conferencing', 'Presence', 'Configuration', 'Classes', 'Access Levels', 'Application Management', 'Endpoints', 'SIP AS 8.1', 'Feature Management', 'Inventory', and 'Templates'. The main content area is titled 'Presence' and shows 'Presence Configuration Properties'. It includes a table with 3 items, a 'Refresh' button, and a 'Filter: Enable' dropdown. The table has columns for Name, Type, and Value.

Name	Type	Value
Domain Substitution - From	text	@
Domain Substitution - To	text	@pres.
Domain Substitution - Default	text	

5.3. Administer SIP Elements

A SIP Element must be administered for each SIP-based telephony system that connects to Session Manager. To add a SIP Element, select **Routing** → **SIP Elements** on the left panel menu and then click the **New** button (not shown). Enter the following values when administering Presence Services as a SIP Element:

- **Name:** Enter descriptive name; in this case that is **PresenceServer**
- **FQDN or IP Address:** Enter the IP address of the Presence Services server; in this case that is **135.64.186.52**
- **Type:** Enter **Other** for Presence Services
- **Time Zone:** Select appropriate time zone for the location
- **SIP Link Monitoring:** Select **Use Session Manager Configuration** from the drop down list, which is a default value

Click **Commit** to save changes.

The screenshot shows the 'SIP Element Details' configuration window. The left sidebar contains a navigation menu with the following items: Elements, Events, Groups & Roles, Licenses, Routing (selected), Domains, Locations, Adaptations, SIP Elements (highlighted), Element Links, Time Ranges, Policies, Dial Patterns, Regular Expressions, Defaults, Security, System Manager Data, and Users. The main content area is titled 'SIP Element Details' and has 'Commit' and 'Cancel' buttons in the top right. It is divided into two sections: 'General' and 'SIP Link Monitoring'. The 'General' section contains the following fields: 'Name' (text box with 'PresenceServer'), 'FQDN or IP Address' (text box with '135.64.186.52'), 'Type' (dropdown menu with 'Other'), 'Notes' (text box), 'Adaptation' (dropdown menu), 'Location' (dropdown menu), 'Time Zone' (dropdown menu with 'Europe/Dublin'), 'Override Port & Transport with DNS SRV' (checkbox), 'SIP Timer B/F (in seconds)' (text box with '4'), 'Credential name' (text box), and 'Call Detail Recording' (dropdown menu with 'none'). The 'SIP Link Monitoring' section contains a single dropdown menu for 'SIP Link Monitoring' with the value 'Use Session Manager Configuration'. The window has a standard Windows-style title bar and a status bar at the bottom that says 'Done'.

The following screen shows the values used for configuring the SIP Element for Session Manager.

SIP Element Details

CommitCancel

General

* Name:SessionManager

* FQDN or IP Address:135.64.186.40

Type:Session Manager

Notes:

Location:Dublin Stack

Outbound Proxy:

Time Zone:Europe/Dublin

Credential name:

SIP Link Monitoring

SIP Link Monitoring:Use Session Manager Configuration

The following screen shows the values used for configuring SIP Element for Communication Manager acting as a Feature Server.

SIP Element Details

CommitCancel

General

* Name:FeatureServer

* FQDN or IP Address:135.64.186.55

Type:CM

Notes:

Adaptation:

Location:

Time Zone:Europe/Dublin

Override Port & Transport with DNS SRV:☐

* SIP Timer B/F (in seconds):4

Credential name:

Call Detail Recording:none

SIP Link Monitoring


SIP Link Monitoring:Use Session Manager Configuration

5.4. Administer Element Links

To create an Element Link, select **Routing** → **Element Links** on the left panel menu and then click the **New** button (not shown). In the new **Element Links** page that appears, enter the following values when creating the link between Presence Services and Session Manager:

- **Name:** Enter a descriptive name; in this case that is **PresenceElementLink**
- **SIP Entity 1:** Select the Session Manager SIP Element from the drop down list configured in **Section 5.3**; in this case that is **SessionManager**
- **Protocol:** Enter the transport protocol to be used for SIP requests; in this case that is **TLS**
- **Port:** Enter port number to which the Presence Services SIP Element sends its SIP requests; in this case that is **5061**
- **SIP Entity 2:** Enter Presence Services SIP Element created in **Section 5.3**; in this case that is **PresenceServer**
- **Port:** Enter the port number on which the Presence Services SIP Element expects to receive SIP requests; in this case that is **5061**
- **Trusted:** Check the checkbox in order to trust the other system
- **Notes:** Optional

Click **Commit** to save changes.

 Avaya Aura™ System Manager
6.0

Welcome, **admin** Last Logged on at May 18, 2010 3:17 PM
[Help](#) | [Change Password](#) | [Log out](#)

Home / Routing / Element Links

Element Links

Commit

Cancel

1 Item Refresh

Filter: Enable

Name	SIP Element 1	Protocol	Port	SIP Element 2	Port	Trusted	Notes
* PresenceElementLink	* SessionManager	TLS	* 5061	* PresenceServer	* 5061	<input checked="" type="checkbox"/>	

The following screen shows the Element Links used in the sample network.

<input type="checkbox"/>	PresenceElementLink	SessionManager	TLS	<input type="text" value="5061"/>	PresenceServer	<input type="text" value="5061"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SessionManager FeatureServer 5065 TLS	SessionManager	TLS	<input type="text" value="5065"/>	FeatureServer	<input type="text" value="5065"/>	<input checked="" type="checkbox"/>

5.5. Administer Session Manager

Add the Session Manager to provide the link between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Click **New** (not shown) and fill in the fields as described below.

Under **General**:

- **SIP Entity Name:** Select the name of the SIP Element added for Session Manager in **Section 5.3**
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface
- **Direct Routing to Endpoints:** Select **Enable**

Under **Security Module**:

- **Network Mask:** Enter the network mask corresponding to the IP address of **Session Manager**
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to save changes (not shown).

Home / Elements / Session Manager / Session Manager Administration / Edit Session Manager

▼ Elements

► Conferencing

► Presence

► Application Management

► Endpoints

SIP AS 8.1

► Feature Management

► Inventory

► Templates

▼ Session Manager

Dashboard

Session Manager Administration

Communication Profile Editor

► Network Configuration

► Device and Location Configuration

► Application Configuration

► System Status

► System Tools

Edit Session Manager

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Cc
Expand All | Collapse All

General ▼

SIP Entity Name

SessionManager

Description

Enterprise ASM 1

*Management Access Point Host Name/IP

135.64.186.39

*Direct Routing to Endpoints

Enable ▼

Security Module ▼

SIP Entity IP Address

135.64.186.40

*Network Mask

255.255.255.224

*Default Gateway

135.64.186.33

*Call Control PHB

46

*QOS Priority

6

5.6. Add Avaya Aura™ Communication Manager as a Managed Element

In order for Communication Manager to provide configuration and Feature Server support to SIP Avaya one-X Communicator when they register to Session Manager, Communication Manager must be added as a Managed Element and an application sequence should be defined.

5.6.1. Create a Managed Element

Select **Elements** → **Inventory** → **Manage Elements** on the left. Click **New** (not shown) and for the **Type** select **CM** from the drop down list. In the **New CM Instance** page that appears specify the following and use defaults for the remaining fields:

- **Name:** A descriptive name for the Communication Manager Feature Server
- **Node:** Enter the IP address for Communication Manager SAT access

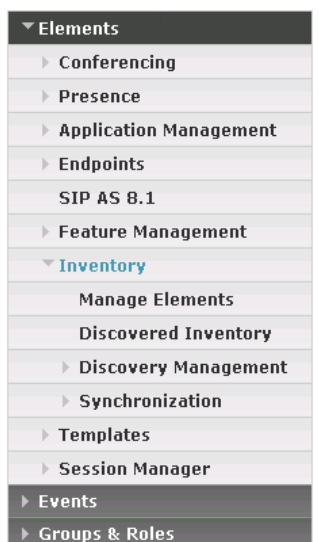


Avaya Aura™ System Manager
6.0

Welcome, **admin** Last Logged on at May 19, 2010 1:41 PM

[Help](#) | [About](#) | [Change Password](#) | [Log](#)

[Home](#) / [Elements](#) / [Application Management](#) / [Applications](#) / [Applications Details](#)



New CM Instance

[Application](#) | [Port](#) | [Access Point](#) | [SNMP Attributes](#) | [Attributes](#) | [Expand All](#) | [Collapse All](#)

Application ▾

* **Name**

* **Type** [Reset](#)

Description

* **Node**

Navigate to the **Attributes** section and enter the following:

- **Login:** Login used for SAT access
- **Password:** Password used for SAT access
- **Confirm Password:** Password used for SAT access

Click **Commit** to save.

Attributes ▼

*** Login**

Password

Confirm Password

Is SSH Connection ☒

*** Port**

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled ☐

ASG Key

Confirm ASG Key

Location

*** Required**

5.6.2. Create an Application for Avaya Aura™ Communication Manager Feature Server

Select **Elements** → **Session Manager** → **Application Configuration** → **Applications** on the left. Click **New** (not shown) and configure the following fields:

- **Name:** A descriptive name
- **SIP Entity:** Select the SIP Element configured in **Section 5.3** for Communication Manager acting as a Feature Server
- **CM System for SIP Entity:** Select the Managed Element configured in **Section 5.6.1** for Communication Manager acting as a Feature Server

Use defaults for the remaining fields and click **Commit** to save.

Home / Elements / Session Manager / Application Configuration / Application Editor

▼ Elements

► Conferencing

► Presence

► Application Management

► Endpoints

SIP AS 8.1

► Feature Management

► Inventory

► Templates

▼ Session Manager

Dashboard

Session Manager

Administration

Communication Profile

Editor

► Network Configuration

► Device and Location

Configuration

▼ Application Configuration

Applications

Application Editor

Application Editor

Name

* SIP Entity

* CM System for SIP Entity [View/Add CM Systems](#)

Description

Application Attributes (optional)

Name	Value
Application Handle	<input type="text"/>
URI Parameters	<input type="text"/>

* Required

5.6.3. Create a Avaya Aura™ Communication Manager Feature Server Application Sequence

Select **Elements** → **Session Manager** → **Application Configuration** → **Application Sequences** on the left. Click **New** (not shown) and enter a descriptive **Name**; in this case that is **APP Sequence**. Click the + sign next to the appropriate application in **Available Applications** and it will move up to the **Applications in this Sequence** section. Click **Commit** to save (not shown).

► Conferencing

► Presence

► Application Management

► Endpoints

SIP AS 8.1

► Feature Management

► Inventory

► Templates

▼ Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

► Network Configuration

► Device and Location Configuration

▼ Application Configuration

Applications

Application Sequences

Implicit Users

► System Status

► System Tools

Application Sequence Editor

Sequence Name

Name

Description

Applications in this Sequence

Move First

Move Last

Remove

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	<div>▲ ▼ ✕</div>	FeatureServer	FeatureServer	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

1 Item | Refresh Filter

	Name	SIP Entity	Description
+	FeatureServer	FeatureServer	

5.6.4. Synchronize Avaya Aura™ Communication Manager Feature and Evolution Server Data

Select **Elements** → **Inventory** → **Manage Elements** → **Synchronization** → **Communication System** on the left. Check the appropriate **Element Name**, click **Initialize data for selected devices** and click **Now**. This may take some time.

▼ Elements

► Conferencing

► Presence

► Application Management

► Endpoints

SIP AS 8.1

► Feature Management

▼ Inventory

Manage Elements

Discovered Inventory

► Discovery Management

▼ Synchronization

Communication System

Messaging System

► Templates

► Session Manager

► Events

► Groups & Roles

Licenses

► Routing

► Security

► System Manager Data

Synchronize CM Data and Configure Options

Synchronize CM Data/Launch Element Cut Through | Configuration Options | Expand All | Collapse All

Synchronize CM Data/Launch Element Cut Through ▼

Synchronization Status Summary Close

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type
<input type="checkbox"/>	CMES60	135.64.186.70	May 31, 2010 12:00:37 PM +01:00	10:00 pm SUN MAY 30, 2010	Incremental
<input checked="" type="checkbox"/>	FeatureServer	135.64.186.55	May 31, 2010 12:00:23 PM +01:00	10:00 pm SUN MAY 30, 2010	Incremental

Select : All, None

☒ Initialize data for selected devices
☐ Incremental Sync data for selected devices
☐ Save Translations for selected devices

Now

Schedule

Cancel

Launch Element Cut Through

Note: Repeat all the **Steps** described in **Sections 5.3, 5.4** and **5.6** to configure Communication Manager as an Evolution Server. Administrator will also have to define a SIP Entity and Entity Link for the CM Evolution Server.

5.7. Configure Users for one-X™ Communicator End Point

Users must be added via System Manager, which will automatically update Communication Manager. Select **Users** → **Manage Users** on the left. Then click on **New** (not shown). In the New User Profile page that appears enter a **First Name** and **Last Name**.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at May 19, 2010 10:02 AM
Help | About | Change Password | Log out

Home / Users / Manage Users / New User

New User Profile

General | Identity | Communication Profile | Roles | Override Permissions | Group Membership | Default Contacts | Private Contacts | Expand All | Collapse All

General

* Last Name: Vera

* First Name: Mijatovic

Middle Name:

Description:

Navigate to the **Identity** section and enter the following and use defaults for other fields:

- **Login Name:** The desired phone extension number @domain.com where domain was defined in **Section 5.1**
- **Password:** Password for user to log into System Manager
- **Shared Communication Profile Password**
Password for user to log into the phone

Identity

* Login Name: 34001@silstack.com

* Authentication Type: Basic

SMGR Login Password:

* Password:

* Confirm Password:

Shared Communication Profile Password:

Confirm Password:

Localized Display Name:

Endpoint Display Name:

Honorific:

Language Preference:

Time Zone:

Navigate to and click on **Communication Profile** section to expand. Then click on **Communication Address** to expand that section and click **New**. Enter the following values:

- **Type:** Select **Avaya SIP**
- **Fully Qualified Address:** Enter the extension number

Keep defaults for the remaining fields and click **Add**.

Communication Profile ▼

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary

Default : ☒

Communication Address ▼

New Edit Delete

	Type	Handle	Domain
No Records found			

Type: Avaya SIP ▼

* Fully Qualified Address: 34001 @ silstack.com ▼

Add Cancel

Navigate to and click on the **Session Manager Profile** section to expand it. Select the appropriate Session Manager server for the **Primary Session Manager**. For **Origination Application Sequence** and **Termination Application Sequence** select the application sequence created in **Section 5.6.3**. For the **Home Location** select appropriate value from the drop down list.

☒ **Session Manager Profile** ▼

* Primary Session Manager SessionManager ▼

Secondary Session Manager (None) ▼

Origination Application Sequence App Sequence ▼

Termination Application Sequence App Sequence ▼

Survivability Server (None) ▼

* Home Location Dublin Stack ▼

Primary	Secondary	Maximum
8	0	8

Primary	Secondary	Maximum

Click on **Endpoint Profile** to expand that section. Enter the following fields and use defaults for the remaining fields:

- **System:** Select the Communication Manager Element defined in **Section 5.6.2**
- **Extension:** Enter a desired extension number
- **Template:** Select a telephone type template
- **Port:** Select **IP**

Click **Commit** to save (not shown).

☒ **Endpoint Profile** ▼

* **System**

FeatureServer ▼

Use Existing Endpoints

☐

* **Extension**

Endpoint Editor

* **Template**

DEFAULT_9630SIP_CM_6_0 ▼

Set Type

Security Code

* **Port**

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User

☐

5.8. Configure one-X™ Communicator SIP End Point

The SIP one-X Communicator needs to be configured to use a specific protocol and port when registering to Session Manager. To configure these settings on the telephone navigate to **Settings→General Settings→ Phone** and specify the following values:

- **Server List:** Enter the IP address of the Session Manager virtual SM-100 card configured in **Section 5.3** for Session Manager SIP Element
- **Transport Type:** Enter **TLS** as configured in **Section 5.4** for SIP Element Link between Presence Services and Session Manager
- **SIP Port:** Enter 5061 as configured in **Section 5.4** for SIP Element Link between Presence Services and Session Manager

Navigate to **Settings→General Settings→ IM and Presence** and specify the following values:

- **Enable Instant Messaging and Presence:** Tick the check box
- **Server:** Enter the IP address of the Presence Services Server

6. Verification Steps

This section provides the tests that can be performed on Communication Manager, Session Manager and Presence Services to verify proper configuration.

6.1. Avaya Aura™ Communication Manager

Verify the status of the SIP trunk group by using the **status trunk n** command, where **n** is the trunk group number being investigated. Verify that all trunks are in the **in-service/idle** state as shown below.

```
status trunk 50
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0050/001	T00001	in-service/idle	no
0050/002	T00002	in-service/idle	no
0050/003	T00003	in-service/idle	no
0050/004	T00004	in-service/idle	no
0050/005	T00005	in-service/idle	no
0050/006	T00006	in-service/idle	no
0050/007	T00007	in-service/idle	no
0050/008	T00008	in-service/idle	no
0050/009	T00009	in-service/idle	no
0050/010	T00010	in-service/idle	no

Verify the status of the SIP signaling-group by using the **status signaling-group n** command, where **n** is the signaling group number being investigated. Verify that the signaling group is in the **in-service** state as shown below.

```
status signaling-group 50
STATUS SIGNALING GROUP

Group ID: 50
Group Type: sip
Group State: in-service
```

6.2. Avaya Aura™ Session Manager

Select **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**. On the **SIP Entity Link Monitoring Status Summary** page that appears verify that none of the SIP entities for Communication Manager or Presence Services links are down, indicating that they are all reachable for routing.

▼ Elements

▶ Conferencing

▶ Presence

▶ Application Management

▶ Endpoints

SIP AS 8.1

▶ Feature Management

▶ Inventory

▶ Templates

▼ Session Manager

Dashboard

Session Manager

Administration

Communication Profile

Editor

▶ Network Configuration

▶ Device and Location

Configuration

▶ Application Configuration

▼ System Status

System State

Administration

SIP Entity Monitoring

Managed Bandwidth

Usage

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

Refresh

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities Not Monitor
SessionManager	3/16	0	0	1


All Monitored SIP Entities

Refresh

15 Items Filter: Enable

SIP Entity Name
AudioCodesM2K
Branch CM
Bridge 6.0
Enterprise Evolution CM
FeatureServer
IMG1010
MX 5.2 Mick
MX52
MX_DavidH
MXStack6.0
OCS
PresenceServer

Select the **SIP Entity Name** for the **PresenceServer** configured in **Section 5.3** and verify that the **Connection Status** is **Up**, as shown on the screen below.



Avaya Aura™ System Manager
6.0

Welcome, **admin** Last Logged on at May 20, 2010 11:46 AM
[Help](#) | [Change Password](#) | [Log of](#)

Home / Elements / Session Manager / System Status / SIP Entity Monitoring / SIP Entity Link Status

▼ Elements

- ▶ Conferencing
- ▶ Presence
- ▶ Application Management
- ▶ Endpoints
- SIP AS 8.1
- ▶ Feature Management
- ▶ Inventory
- ▶ Templates
- ▼ Session Manager

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: PresenceServer

Refresh
Summary View

1 Item
Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	SessionManager	135.64.186.52	5061	TLS	Up	200 OK	Up

Select the **SIP Entity Name** for the **FeatureServer** configured in **Section 5.3** and verify that the **Connection Status** is **Up**, as shown on the screen below.



Avaya Aura™ System Manager
6.0

Welcome, **admin** Last Logged on at May 20, 2010 11:46 AM
[Help](#) | [Change Password](#) | [Log of](#)

Home / Elements / Session Manager / System Status / SIP Entity Monitoring / SIP Entity Link Status

▼ Elements

- ▶ Conferencing
- ▶ Presence
- ▶ Application Management
- ▶ Endpoints
- SIP AS 8.1
- ▶ Feature Management
- ▶ Inventory
- ▶ Templates
- ▼ Session Manager

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: FeatureServer

Refresh
Summary View

1 Item
Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	SessionManager	135.64.186.55	5065	TLS	Up	200 OK	Up

6.3. Avaya Aura™ Presence Services

Verify Presence Services are **Running** using the **XCP Controller** web interface on the Presence server. To access the XCP Controller web interface follow the steps described in **Section 4**.

XCP Controller - presence
[\[Home\]](#) [\[Logoff\]](#) Configuration view: **Advanced** ▼

System
[\[Summary\]](#) [\[Cluster\]](#) [\[Stop the System\]](#) [\[Online Help\]](#)

Router
Add a new

Status	Plugin	Description	Actions	Ports	Remove
Running	Core Router	Global router settings	Edit	7400	N/A
Running	logger-1.presence	Logger Plugin	Edit		Remove
Running	jsm-1.presence	Presence Session Manager	Edit		Remove
Running	logger-2.presence	Statistics Logger	Edit		Remove
Running	logger-3.presence	PS Core Logger	Edit		Remove

Components
Add a new

Status	Component	Description	Actions	Ports	Remove
Running	sip-ps-1.presence	SIP Presence Server	Edit , Stop	15061	N/A
Running	sip-proxy-1.presence	SIP Proxy	Edit , Stop	5061 15061 25061	N/A
Running	sip-bulksb-1.presence	SIP Bulk Subscription Server	Edit , Stop	25061	N/A

6.4. Obtaining Presence data from Avaya one-X™ Communicator

6.4.1. Verify Data Replication from Avaya Aura™ System Manager to Avaya Aura™ Presence Server

Users created in System Manager as described in **Section 5.7**, are replicated in the **presence** database of the Presence server. To verify that user data is successfully replicated to the Presence server run following command on the ssh connection to the Presence server:

```
psql -d presence -U postgres -c "select * from csuser"
```

Below is the screen with results showing that users with **loginname 34001@silstack.com** and **34002@silstack.com** are successfully replicated to Presence server.

```
[root@ips60 craft]# psql -d presence -U postgres -c "select * from csuser"
```

id	updatedatetime	version	isdeleted	isenabled	loginname
51	2009-12-25 17:09:41	0	f	t	system
50	2010-02-09 10:56:17	1	f	t	admin
152	2010-03-16 11:50:32	0	f	t	34001@silstack.com
153	2010-03-16 12:24:29	0	f	t	34002@silstack.com

6.4.2. Verify User's presence data is obtainable

After a user publishes its presence for the first time, it gets added in the **xcp** Presence database. To verify this, login the user with extension **34001** on a SIP one-X™ Communicator. Once the user is successfully logged in, the user data is updated in the xcp database. At the same time the domain substitution rule described in **Section 5.2** is applied for that user. To verify this update is successful run following command on the ssh connection to the Presence server:

```
psql -d xcp -U postgres -c "select * from users"
```

Below is the screen with results showing that user with **jid 34001@pres.silstack.com** has successfully published its presence.

```
[root@ips60 craft]# psql -d xcp -U postgres -c "select * from users"
```

user_id	jid	auth_pwd	disabled	login_stamp
10311	34001@pres.silstack.com	-	F	2010-05-11 12:38:49
13:20:59	29	2010-04-22	Disconnected.	2010-05-11
10002	user20003@pres.silstack.com	-	F	2010-04-12 12:03:40
12:03:43	7	2010-04-01	Disconnected.	2010-04-12
10818	40001@pres.silstack.com	-	F	2010-05-19 11:14:56
16:55:57	11	2010-04-29	Disconnected.	2010-05-19
10312	34002@pres.silstack.com	-	F	2010-05-19 17:43:05
08:25:55	27	2010-04-26	Disconnected.	2010-05-20

7. Conclusion

As illustrated in these Application Notes, Avaya one-X™ Communicator SIP users registered on Avaya Aura™ Session Manager can publish presence, once the described configuration is completed on Avaya Aura™ Presence Services, Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager.

8. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

- [1] *Avaya Aura™ Session Manager Overview*, Doc # 03-603323, Issue 2
- [2] *Administering Avaya Aura™ Session Manager*, Doc # 03-603324, Issue 2
- [3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc # 03-603325, Issue 2
- [4] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, Issue 9
- [5] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, Issue 5
- [6] *Installing Avaya Aura™ Presence Services*, Release 6.0, March 2010, CID 146045

©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabinotes@list.avaya.com