



Avaya Solution & Interoperability Test Lab

Application Notes for Ascom i62 Handsets with Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Session Manager R6.1 – Issue 1.0

Abstract

These Application Notes describe the compliance testing of Ascom i62 wireless handsets with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Ascom handsets communicate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager via wireless LAN using the SIP protocol. The compliance testing tested the major functions of the Ascom i62 product.

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

1. Introduction

These Application Notes describe the configuration steps required for the Ascom i62 wireless handset to successfully interoperate with Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Session Manager R6.1. Ascom i62 wireless handsets register to Session Manager as third-party SIP users. These users are configured in System Manager under User Management and are thus added to Communication Manager as SIP endpoints using the 9600 SIP template. Avaya Aura® Messaging R6.1 was used to verify DTMF and Message Waiting Indication (MWI).

2. General Test Approach and Test Results

The compliance testing of Ascom i62 interoperating with Session Manager and Communication Manager was performed manually. The tests were functional in nature, and no performance testing was done.

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.

2.1. Interoperability Compliance Testing

The compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP phones, Avaya H.323 phones, Ascom i62 endpoints, and PSTN endpoints.

- Basic call
- DTMF
- Hold, retrieve, enquiry, and brokering
- Attended, blind transfer
- Call forwarding unconditional, no reply, busy
- Call waiting
- Call park/pickup
- EC500
- Conference
- Do not disturb
- Calling line/name identification
- Connected line/name identification
- Codec support
- Voicemail and Message Waiting Indication

2.2. Test Results

The following observations were noted during compliance testing:

1. When a blind transfer is made to an Ascom i62 handset, the number of the transferring party is shown at the Ascom i62 handset instead of the original caller while the call is alerting. After the call is answered, the Ascom i62 handset display is updated correctly. This is due to a design philosophy difference between Ascom and Avaya products.
2. It is not possible to park a call from an Ascom i62 handset. However, parked calls can be retrieved from Ascom i62 handsets.
3. It is not possible to initiate Do Not Disturb from an Ascom i62 handset via Communication Manager Feature Access Code.
4. Message Waiting Indication was tested successfully during compliance testing, however due to intermittent issues reported by Ascom regarding MWI this feature is currently not supported.

With the exception of the above-described observations, all tests produced the expected result.

Section 2.1 contains a list of tests which were performed.

2.3. Support

Support from Avaya is available at <http://support.avaya.com/>.

Technical support for the Ascom wireless i62 WiFi handset can be obtained through a local Ascom supplier.

Ascom global technical support:

- Email: support@ascom.se
- Help desk: +46 31 559450

3. Reference Configuration

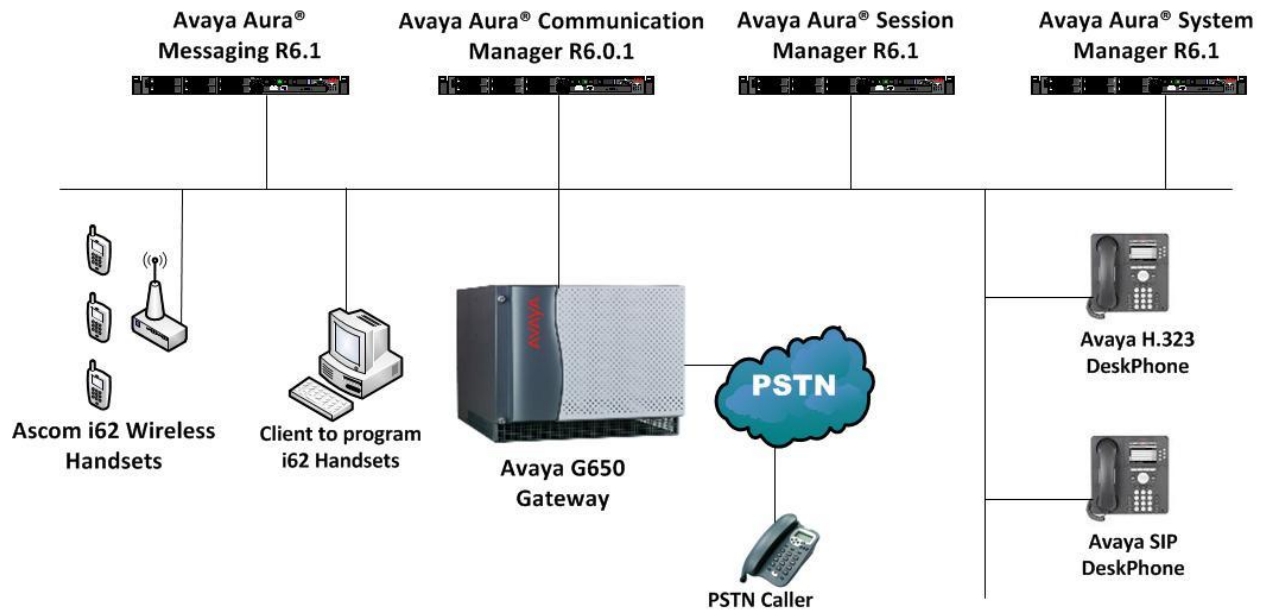


Figure 1: Reference Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on S8800 Server	R016x.00.1.510.1 Patch: 00.1.510.1-19009
Avaya Aura® Session Manager running on S8800 Server	6.1.4.0.614005
Avaya Aura® Messaging running on S8800 Server	6.1
Avaya G650 Media Gateway	31.18.1
Avaya MM710AP PRI interface	HW05 / FW021
Avaya 96x0-Series IP Phones (SIP)	2.6.4
Avaya 96x0-Series IP Phones (H.323)	3.1.1
Ascom Device Manager Platform	MS XP Professional SP3
Ascom Device Manager	3.8.1
Ascom i62 Telephone	v. 2.5.9

Table 1: Equipment and Versions Validated

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were performed using the Communication Manager System Administration Terminal (SAT).

Note: The configuration of the interface to the PSTN is out of the scope of these Application Notes.

5.1. Verify System-Parameters Customer-Options

Use the **display system-parameters customer-options** command to verify that Communication Manager is configured to meet the minimum capacity requirements to support the configuration used for these tests, as shown by the parameter values in **Table 2**. If these are not met in the configuration, please contact an Avaya representative for further assistance.

Parameter	Usage
Maximum Administered SIP Trunks (Page 2)	The number of available licensed SIP trunks must be sufficient to accommodate the number of trunk members assigned to the trunk group used to interface to Session Manager in Figure 9 .

Table 2: Configuration Values for System-Parameters Customer-Options

```

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

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 50
      Maximum Concurrently Registered IP Stations: 18000 2
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 414 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 18000 0
      Maximum Video Capable IP Softphones: 1000 0
      Maximum Administered SIP Trunks: 24000 10
      Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
      Maximum Number of DS1 Boards with Echo Cancellation: 522 0
      Maximum TN2501 VAL Boards: 128 0
      Maximum Media Gateway VAL Sources: 250 1
      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
  
```

Figure 2: System-Parameters Customer-Options Form, Page 2

5.2. Dialplan

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below.

Dialed String	Usage
2	Make an entry for Avaya terminal extensions.
4	Make an entry for Ascom terminal extensions.
*2	Make an entry for feature access codes shown in Figure 4 .
*8	Make an entry for dial access codes (to be used to specify the trunk access code in the SIP trunk group defined in Figure 9).

Table 3: Dialplan Analysis Parameters

```

change dialplan analysis                                     Page 1 of 12
                                                           DIAL PLAN ANALYSIS TABLE
                                                           Location: all                                     Percent Full: 4
Dialed Total Call      Dialed Total Call      Dialed Total Call
String Length Type     String Length Type     String Length Type
2         4   ext
4         4   ext
*2        4   fac
*8        4   dac

```

Figure 3: Dialplan Analysis Form

5.3. Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be entered from Ascom handsets to initiate Communication Manager call features. These access codes must be compatible with the dial plan described in **Figure 3**.

Dialed String	Usage
Announcement Access Code	Enter an access code if announcements need to be created for the operation of the Meet-me conferencing features.
Call Forwarding Activation Busy/DA -- All -- Deactivation	Enter access codes for the operation of the call forwarding features.

Table 4: Feature Access Codes Parameters

```

change feature-access-codes                                     Page 1 of 10
                    FEATURE ACCESS CODE (FAC)
    Abbreviated Dialing List1 Access Code:
    Abbreviated Dialing List2 Access Code:
    Abbreviated Dialing List3 Access Code:
    Abbreviated Dial - Prgm Group List Access Code:
        Announcement Access Code: *200
        Answer Back Access Code: *206
        Attendant Access Code:
    Auto Alternate Routing (AAR) Access Code:
    Auto Route Selection (ARS) - Access Code 1: 0      Access Code 2:
    Automatic Callback Activation:                      Deactivation:
Call Forwarding Activation Busy/DA: *203 All: *201 Deactivation: *202
    Call Forwarding Enhanced Status:      Act:          Deactivation:
        Call Park Access Code: *205
        Call Pickup Access Code:
    CAS Remote Hold/Answer Hold-Unhold Access Code:
        CDR Account Code Access Code:
        Change COR Access Code:
        Change Coverage Access Code:
    Conditional Call Extend Activation:      Deactivation:
        Contact Closure Open Code:          Close Code:

```

Figure 4: Feature Access Codes Screen

5.4. Configure IP Interfaces

Use the **change node-names ip** command to configure the IP address of Session Manager.

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
Name          IP Address
asset       192.168.150.115
default       0.0.0.0
procr        192.168.150.118
procr6       ::
```

Figure 5: Node-Names IP Form

5.5. Configure Network Region

Use the **change ip-network-region** command to assign an appropriate domain name to be used by Communication Manager. This name is also used in **Figure 15**.

```
change ip-network-region 1                             Page 1 of 20
                                                    IP NETWORK REGION
Region: 1
Location: 1      Authoritative Domain: aura.dcffm
Name: local
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
```

Figure 6: IP Network Region Form

5.6. Configure IP-Codec

Use the **change ip-codec-set 1** command to designate a codec set compatible with the Ascom handsets, which support both G.711A and G.729A.

```
change change ip-codec-set 1 Page 1 of 2
                                IP Codec Set
Codec Set: 1
Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G. 711A      n           2          20
2: G. 729A      n           2          20
```

Figure 7: IP-Codec-Set Form

5.7. Configure SIP Interface to Session Manager

Use the **add signaling-group** command to configure the Signaling Group parameters for the SIP trunk group. Assign values for this command as shown in the following table.

Parameter	Usage
Group Type	Enter the Group Type as “sip”.
Near-end Node Name	Enter “procr” to designate the Processor Ethernet interface.
Near-end Listen Port	Enter “5060”.
Far-end Node Name	Enter the name assigned to the SIP trunk to Session Manager configured in Figure 5 .
Far-end Listen Port	Enter “5060”.
Far-end Domain Name	Enter the domain name assigned to the network region in Figure 6 .
Direct IP-IP Audio Connections	Enter “y” to turn on media shuffling.

Table 5: Signaling-Group Parameters for SIP Interface

```

add signaling-group 1                                     Page 1 of 1
                SIGNALING GROUP

Group Number: 1                Group Type: sip
  IMS Enabled? n                Transport Method: tcp
    Q-SIP? n                                SIP Enabled LSP? n
    IP Video? n                        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM

  Near-end Node Name: procr                Far-end Node Name: asset
Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                          Far-end Network Region: 1

Far-end Domain: aura.dcffm

                                          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
  
```

Figure 8: Signaling Group Form

Use the **add trunk-group** command to configure the SIP interface to Session Manager. Assign values for this command as shown in the following table.

Parameter	Usage
Group Type (page 1)	Specify the Group Type as “sip”.
Group Name (page 1)	Enter an appropriate name to identify the device.
TAC (page 1)	Specify a trunk access code that can be used to provide dial access to the trunk group.
Service Type (page 1)	Designate the trunk as a “public-ntwrk” line to a peer system.
Signaling Group (page 1)	Enter the number assigned to the SIP signaling group shown in Figure 8 .
Number of Members (page 1)	Specify sufficient number of members to support the maximum simultaneous connections required.
Preferred Minimum Session Refresh Interval (page 2)	Enter “900”.
Numbering Format (page 3)	Enter “private”.
Support Request History (page 4)	Enter “y”.

Table 6: Trunk-Group Parameters for the SIP Interface

```

add change trunk-group 1                                     Page 1 of 21
                                TRUNK GROUP
Group Number: 1                Group Type: sip              CDR Reports: y
  Group Name: Local-to-CM      COR: 1                    TN: 1          TAC: *801
  Direction: two-way          Outgoing Display? n
  Dial Access? n              Night Service:
Queue Length: 0
Service Type: public-ntwrk    Auth Code? n
                                Member Assignment Method: auto
                                Signaling Group: 1
                                Number of Members: 10

```

Figure 9: Trunk Group Form, page 1

```

add trunk-group 1                                     Page 2 of 21
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                         Redirect On OPTIM Failure: 9000

  SCCAN? n                                           Digital Loss Group: 18
                                         Preferred Minimum Session Refresh Interval(sec): 900

Disconnect Supervision - In? y Out? y

                                         XOIP Treatment: auto   Delay Call Setup When Accessed Via IGAR? n

```

Figure 10: Trunk Group Form, page 2

```

add trunk-group 1                                     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

```

Figure 11: Trunk Group Form, page 3

```

add trunk-group 1                                     Page 4 of 21
                                         PROTOCOL VARIATIONS

  Mark Users as Phone? n
  Prepend '+' to Calling Number? n
  Send Transferring Party Information? y
  Network Call Redirection? n
  Send Diversion Header? n
  Support Request History? y
  Telephone Event Payload Type: 101

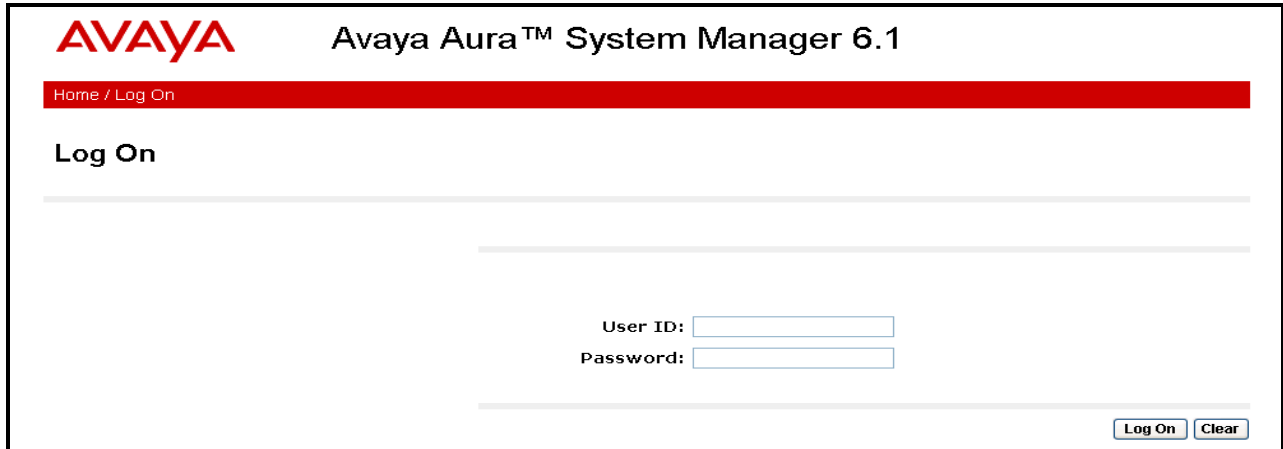
  Convert 180 to 183 for Early Media? n
  Always Use re-INVITE for Display Updates? n
  Identity for Calling Party Display: From
  Enable Q-SIP? n

```

Figure 12: Trunk Group Form, page 4

6. Configure Avaya Aura® Session Manager

This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes. Session Manager is managed via System Manager. Using a web browser, access “https://<ip-addr of System Manager>/SMGR”. In the **Log On** screen, enter appropriate **Username** and **Password** and press the **Log On** button.



AVAYA Avaya Aura™ System Manager 6.1

Home / Log On

Log On

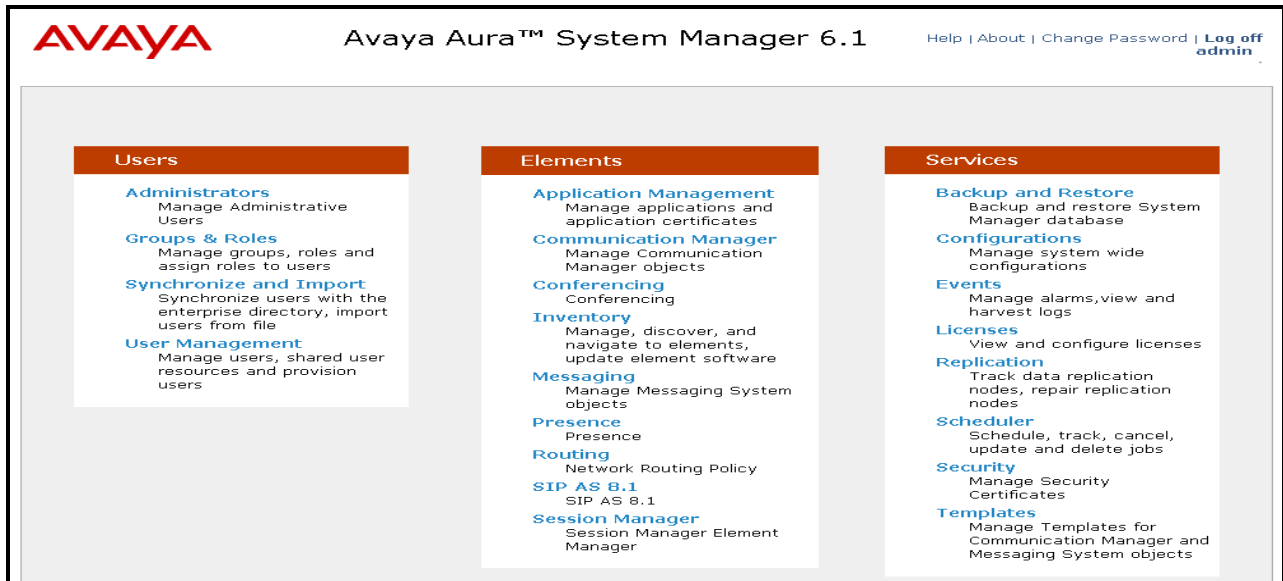
User ID:

Password:

Log On Clear

Figure 13: System Manager Login Screen

Once logged in, the **Home Screen** is displayed.



AVAYA Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin

Users	Elements	Services
Administrators Manage Administrative Users	Application Management Manage applications and application certificates	Backup and Restore Backup and restore System Manager database
Groups & Roles Manage groups, roles and assign roles to users	Communication Manager Manage Communication Manager objects	Configurations Manage system wide configurations
Synchronize and Import Synchronize users with the enterprise directory, import users from file	Conferencing Conferencing	Events Manage alarms, view and harvest logs
User Management Manage users, shared user resources and provision users	Inventory Manage, discover, and navigate to elements, update element software	Licenses View and configure licenses
	Messaging Manage Messaging System objects	Replication Track data replication nodes, repair replication nodes
	Presence Presence	Scheduler Schedule, track, cancel, update and delete jobs
	Routing Network Routing Policy	Security Manage Security Certificates
	SIP AS 8.1 SIP AS 8.1	Templates Manage Templates for Communication Manager and Messaging System objects
	Session Manager Session Manager Element Manager	

Figure 14: System Manager Home Screen

6.1. Domains

Navigate to **Routing** → **Domains** and click **New** to add a domain. Enter the domain name, and click the **Commit** button after changes are completed. The domain name should be the same as was configured in **Figure 6**.

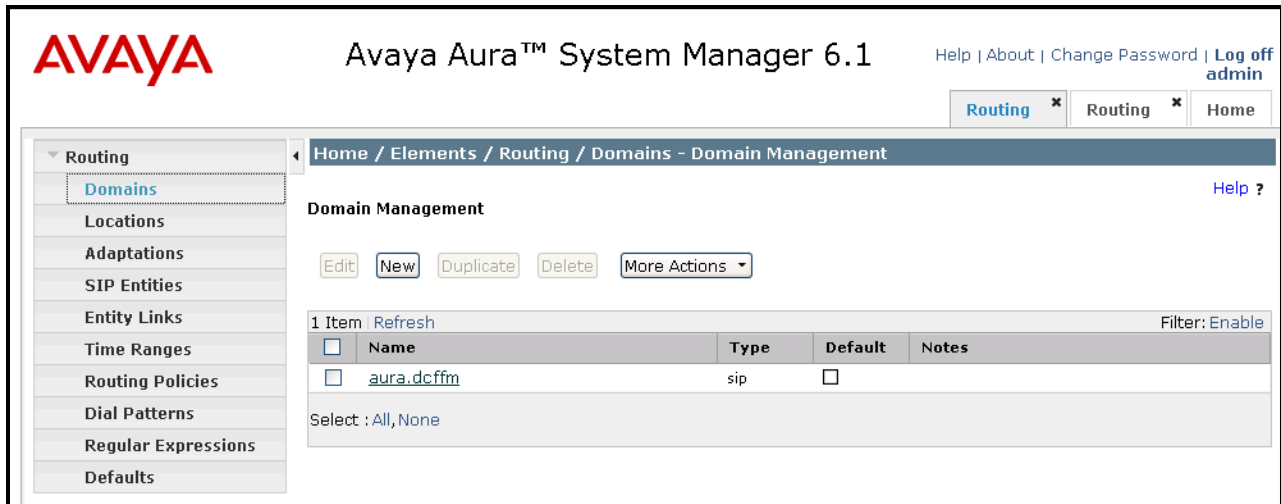


Figure 15: Domain Screen

6.2. Locations

To view or change locations, select **Routing** → **Locations**. Click the **New** button to add a location. Enter a location identifier and the IP addresses residing in the location. Click the **Commit** button after changes are completed. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.

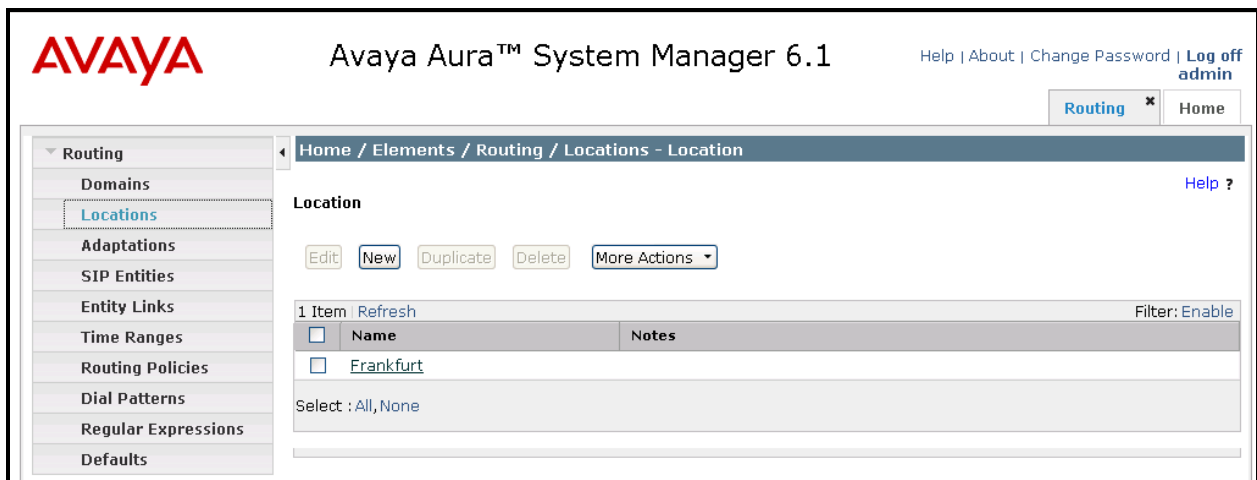


Figure 16: Locations Screen

6.3. SIP Entities

To view or change SIP entities, select **Routing → SIP Entities**. To create a SIP Entity for the Session Manager, click **New**, enter the parameters shown in the following table, and click **Commit**.

Parameter	Usage
Name	Enter an identifier to be assigned to the Session Manager SIP Entity.
FQDN or IP Address	Enter the address value to be assigned to the Session Manager signaling interface
Type	Select “Session Manager” from the drop-down menu.
Location	Select the value assigned to the Session Manager in Section 6.2
Time Zone	Select the appropriate Time Zone for the Session Manager from the drop-down menu.
Ports	Select UDP and 5060 as the port number, TCP and 5060 as the port number and TLS with 5061 as the port number.

Table 7: Session Manager SIP Entity Parameters

Routing Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

- Routing
- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Help ?
Commit
Cancel

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

Entity Links can be modified after SIP Entity is committed.

Port

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="TCP"/>	<input type="text" value="avaya.com"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	<input type="text" value="UDP"/>	<input type="text" value="avaya.com"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	<input type="text" value="TLS"/>	<input type="text" value="avaya.com"/>	<input type="text"/>

Figure 17: Session Manager SIP Entity Screen

Return to the **Routing → SIP Entities** menu to create a SIP Entity for the Communication Manager. Click **New**, enter the parameters shown in the following table, and click **Commit**.

Parameter	Usage
Name	Enter an identifier to be assigned to the Communication Manager SIP Entity.
FQDN or IP Address	Enter the FQDN or IP address value to be assigned to the Communication Manager processor Ethernet interface.
Type	Select “CM” from the drop-down menu.
Location	Select the value assigned in Section 6.2
Time Zone	Select the appropriate Time Zone for the Communication Manager from the drop-down menu.

Table 8: Session Manager SIP Entity Parameters

The screenshot displays the Avaya Aura™ System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the product name, and links for Help, About, Change Password, and Log off admin. The breadcrumb trail is Home / Elements / Routing / SIP Entities - SIP Entity Details. The left sidebar shows a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'General' sub-section. It contains several form fields:

- Name:** entity-CM1
- FQDN or IP Address:** cm1.aura.dccfm
- Type:** CM (selected in a dropdown)
- Notes:** 192.168.150.118
- Adaptation:** (empty dropdown)
- Location:** Frankfurt (selected in a dropdown)
- Time Zone:** Europe/Berlin (selected in a dropdown)
- Override Port & Transport with DNS SRV:**
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (selected in a dropdown)
- SIP Link Monitoring:** Use Session Manager Configuration (selected in a dropdown)

 At the top right of the form area, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

Figure 18: Communication Manager SIP Entity Screen

6.4. Applications

Navigate to **Session Manager**→**Application Configuration**→**Applications**, click **New**, and enter the parameters shown in the following table, and click **View/Add CM Systems** followed by **New**.

Parameter	Usage
Name	Enter an identifier to be assigned to the Communication Manager Application.
SIP Entity	Select the Communication Manager SIP Entity configured in Figure 18 from the drop-down menu.

Table 9: Session Manager SIP Entity Parameters

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the system name, and links for Help, About, Change Password, and Log off admin. Below the navigation bar, there are tabs for Communication Manager, Session Manager, Application Management, Routing, and Home. The left sidebar contains a tree view with categories like Session Manager, Network Configuration, Device and Location, Configuration, and Applications. The main content area is titled 'Application Editor' and contains the following fields:

- Name:** Text input field containing 'CM-1 EV'.
- *SIP Entity:** Dropdown menu with 'entity-CM1' selected.
- *CM System for SIP Entity:** Dropdown menu with a 'Refresh' button and a link 'View/Add CM Systems'.
- Description:** Text input field.

Buttons for 'Commit' and 'Cancel' are located at the top right of the form area.

Figure 19: Session Manager Application Screen

In the **Application** tab, enter the parameters shown in the following table.

Parameter	Usage
Name	Enter an identifier to be assigned to the Communication Manager instance.
Node	Enter the IP address of the Communication Manager processor Ethernet interface.

Table 10: CM Instance Application Parameters

The screenshot shows the 'New CM Instance' configuration screen. At the top right, there is a 'Help ?' link and 'Commit' and 'Cancel' buttons. Below the title bar, there are two tabs: 'Application' (active) and 'Attributes'. Under the 'Application' tab, there is a dropdown menu for 'Application'. Below that are four fields: '* Name' (text input with 'cm1'), '* Type' (dropdown menu with 'CM'), 'Description' (text area), and '* Node' (text input with '192.168.150.118').

Figure 20: CM Instance Application Screen

In the **Attributes** tab, enter the parameters shown in the following table and click **Commit**.

Parameter	Usage
Login	Enter the Communication Manager login id to be used to make configuration changes to Communication Manager.
Password	Enter the password associated with the above Login.
Is SSH Connection	Check this box.
Port	Enter 5022 .

Table 11: CM Instance Attributes Parameters

The screenshot shows the 'New CM Instance' configuration interface. At the top right, there is a 'Help ?' link and 'Commit' and 'Cancel' buttons. Below the title, there are two tabs: 'Application' and 'Attributes', both marked with a red asterisk. The 'Attributes' tab is active. Underneath, there is a section for 'SNMP Attributes' with a dropdown arrow. Below that is the 'Attributes' section, which contains the following fields:

- * Login**: Text input field containing 'init'.
- Password**: Password input field with masked characters (dots).
- Confirm Password**: Password input field with masked characters (dots).
- Is SSH Connection**: Checkable box, currently checked with a green checkmark.
- * Port**: Text input field containing '5022'.
- Alternate IP Address**: Text input field.
- RSA SSH Fingerprint (Primary IP)**: Text input field.
- RSA SSH Fingerprint (Alternate IP)**: Text input field.
- Is ASG Enabled**: Checkable box, currently unchecked.
- ASG Key**: Text input field.
- Confirm ASG Key**: Text input field.
- Location**: Text input field.

Figure 21: CM Instance Attributes Screen

6.5. Application Sequences

Use the menu hierarchy at the left of the screen to navigate to **Session Manager**→**Application Configuration**→**Application Sequences**, click **New**. Click the “+” icon at the bottom of the screen to add the application which was created in **section 6.4**, and click **Commit**.

Parameter	Usage
Name	Enter an identifier to be assigned to the Application Sequence.

Table 12: Application Sequences Parameters

The screenshot displays the Avaya Aura™ System Manager 6.1 interface for the Application Sequence Editor. The left-hand navigation pane shows the path: Session Manager > Application Configuration > Application Sequences. The main content area is titled "Application Sequence Editor" and includes a "Commit" button and a "Cancel" button. The "Application Sequence" section contains a form with a required "Name" field (containing "CM-1 EV 1") and an optional "Description" field. Below this, the "Applications in this Sequence" section shows a table with 0 items and buttons for "Move First", "Move Last", and "Remove". The "Available Applications" section shows a table with 1 item:

Name	SIP Entity	Description
CM-1 EV	entity-CM1	

Figure 22: Application Sequences Screen

6.6. Users

Use the menu hierarchy at the left of the screen to navigate to **User Management**→**Manage Users**, and click **New**.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the product name, and links for Help, About, Change Password, and Log off admin. Below this is a breadcrumb trail: Home / Users / User Management / Manage Users - User Management. The left sidebar contains a menu with 'User Management' expanded to show 'Manage Users', 'Public Contacts', 'Shared Addresses', and 'System Presence ACLs'. The main content area is titled 'User Management' and features a 'Users' section with a toolbar containing 'View', 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below the toolbar is a table with 2 items, a 'Refresh' button, and a 'Show ALL' dropdown. The table has columns for Status, Name, Login Name, E164 Handle, and Last Login. The status of both users is 'Enable'. At the bottom of the table area, there is a 'Select : All, None' option.

<input type="checkbox"/>	Status	Name	Login Name	E164 Handle	Last Login
<input type="checkbox"/>	Enable	extn 2370	2370@aura.dcffm	2370	
<input type="checkbox"/>	Enable	extn 2371	2371@aura.dcffm	2371	

Figure 23: User Management Screen

Enter the values shown in the following table for Ascom handset A shown in Error! Reference source not found., and click **Communication Profile**. This procedure must be repeated for each of the remaining Ascom handsets shown in Error! Reference source not found..

Parameter	Usage
Last Name	Enter a “last” name to identify the endpoint.
First Name	Enter a “first” name to identify the endpoint.
Login Name	Enter a login name of the form<extension>.<domain>.
Authentication Type	Select “Basic” from the drop-down menu.

Table 13: User Identity Parameters

AVAYA Avaya Aura™ System Manager 6.1

User Management * Home

Home / Users / User Management / Manage Users - User Profile Edit

Manage Users
Public Contacts
Shared Addresses
System Presence ACLs

Status

User Profile Edit: 4003@aura.dcffm Commit Cancel

Identity * Communication Profile * Membership Contacts

Identity

* Last Name: 4003

* First Name: Extn

Middle Name:

Description:

Status: Offline

Update Time: May 2, 2011 9:59:24 A

* Login Name: 4003@aura.dcffm

* Authentication Type: Basic

[Change Password](#)

Source: local

Localized Display Name: ASCOM WIFI 4003

Endpoint Display Name: ASCOM WIFI 4003

Honorific:

Language Preference: English

Time Zone: (+2:0)Amsterdam, Berlin, Rome, Belgrade, Prague, Brussels, Sarajevo

Figure 24: User Identity Screen

In the **Communication Profile** tab, click **Edit** for **Communication Profile Password** to enter the password to be assigned to the endpoint. Note that the **Communication Address**, **Session Manager Profile**, and **Endpoint Profile** menu points shown at the bottom of the screen can be expanded and configured individually, as shown by subsequent screens.

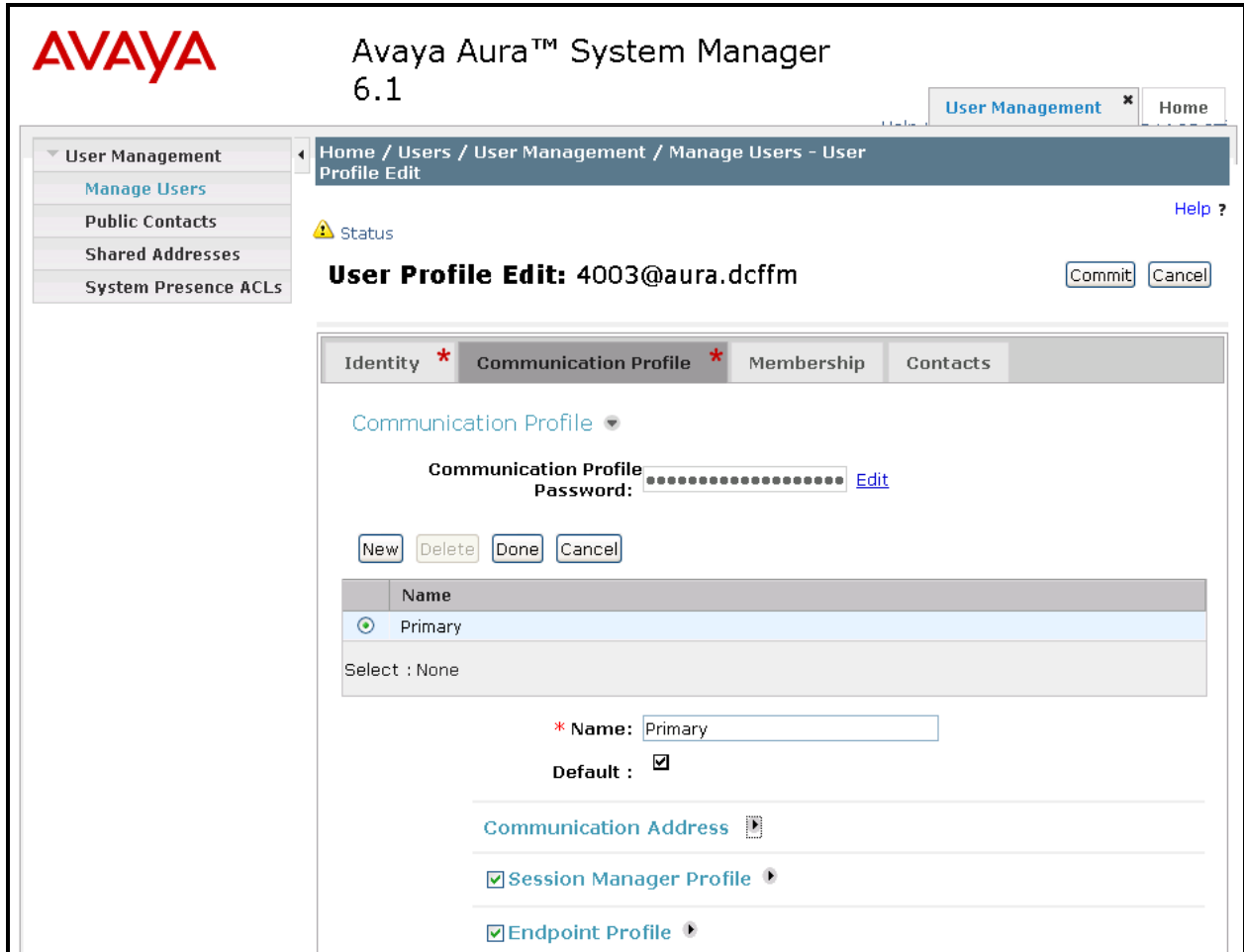


Figure 25: Communication Profile Screen

Expand the **Communication Address** menu. Click **New** and allocate a communication address for the endpoint as shown below.

The screenshot displays a web-based configuration interface for communication addresses. At the top, there are four buttons: 'New', 'Delete', 'Done', and 'Cancel'. Below these is a table with a header 'Name' and one row containing 'Primary', which is highlighted in blue. Underneath the table, it says 'Select : None'. Further down, there is a field labeled '* Name:' containing the text 'Primary'. Below that is a 'Default:' label with a checked checkbox. A horizontal line separates this from the 'Communication Address' section, which has a dropdown arrow next to its title. Underneath, there are three buttons: 'New', 'Edit', and 'Delete'. Below these buttons is a table with the following data:

<input type="checkbox"/>	Type	Handle	Domain
<input type="checkbox"/>	Avaya SIP	4003	aura.dcfm

At the bottom of the table area, it says 'Select : All, None'.

Figure 26: Communications Address Screen

Expand the **Session Manager Profile** menu, and enter the parameters shown in the following table.

Parameter	Usage
Primary Session Manager	Select the Session Manager which was configured in Figure 17 .
Origination Application Sequence	Select the Application Sequence which was assigned in Figure 22 .
Termination Application Sequence	Select the same Application Sequence which was assigned above.
Home Location	Select the location which was created in Figure 16 .

Table 14: Session Manager Profile Parameters

Session Manager Profile ▾

* **Primary Session Manager** ▾

Primary	Secondary	Maximum
8	0	8

Secondary Session Manager ▾

Primary	Secondary	Maximum

Origination Application Sequence ▾

Termination Application Sequence ▾

Survivability Server ▾

* **Home Location** ▾

Figure 27: Session Manager Profile Screen

Expand **Endpoint Profile**, and enter the parameters shown in the following table.

Parameter	Usage
Extension	Enter the extension which is to be assigned to the endpoint.
Template	Select the DEFAULT_9600SIP_CM_6_0 template from the drop-down menu.
Port	Select the IP port from the drop-down menu.

Table 15: Endpoint Profile Parameters

Endpoint Profile

* **System**

* **Profile Type**

Use Existing Endpoints

* **Extension**

Template

Set Type

Security Code

* **Port**

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User or on Delete User.

Figure 28: Endpoint Profile Screen

Upon completion, click the **Commit** button shown in **Figure 25**.

7. Configure Ascom Handsets

Attach the Ascom DP1 USB Cradle to a PC on which the Ascom Device Manager has been installed. Insert the handset to be configured in the DP1 USB cradle, start the Ascom Device Manager, and select the **Numbers** tab.

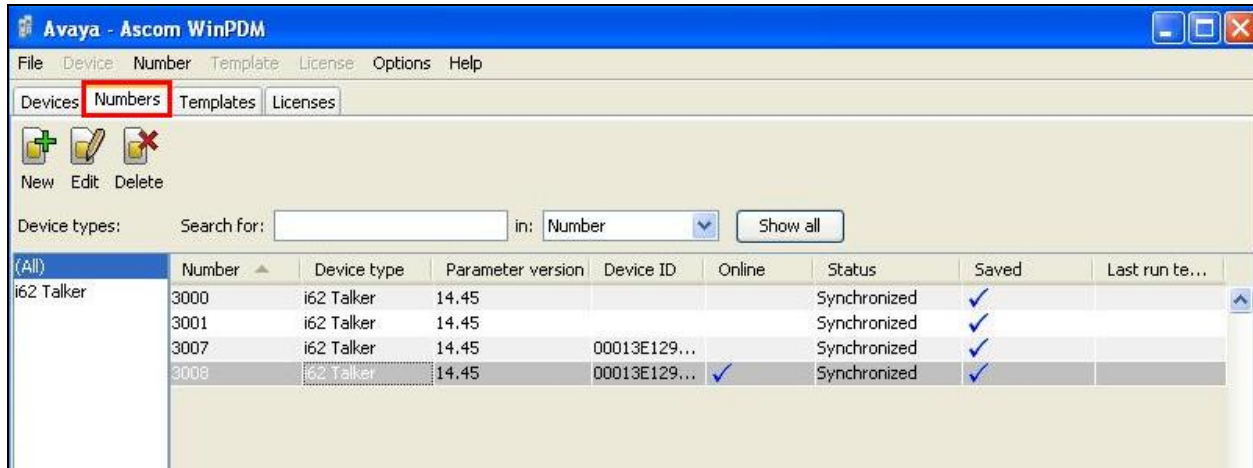


Figure 29: Ascom Device Manager Numbers Tab

Double click the entry for the handset which is to be configured, select the **VoIP→General** menu point, and enter the values shown in the following table.

Parameter	Usage
Replace Call Rejected with User Busy	Enable.
VoIP Protocol	Enter SIP .
Codec configuration	Enter a codec which is contained in the codec list specified in Figure 7 .
Codec packetization time	Enter 20.
Internal call number length	Enter the length of the local extension assigned to the handset.
Endpoint number	Enter the extension assigned to the handset.
Endpoint ID	Enter the extension assigned to the handset.

Table 16: i62 Numbers Tab, VoIP→General Parameters

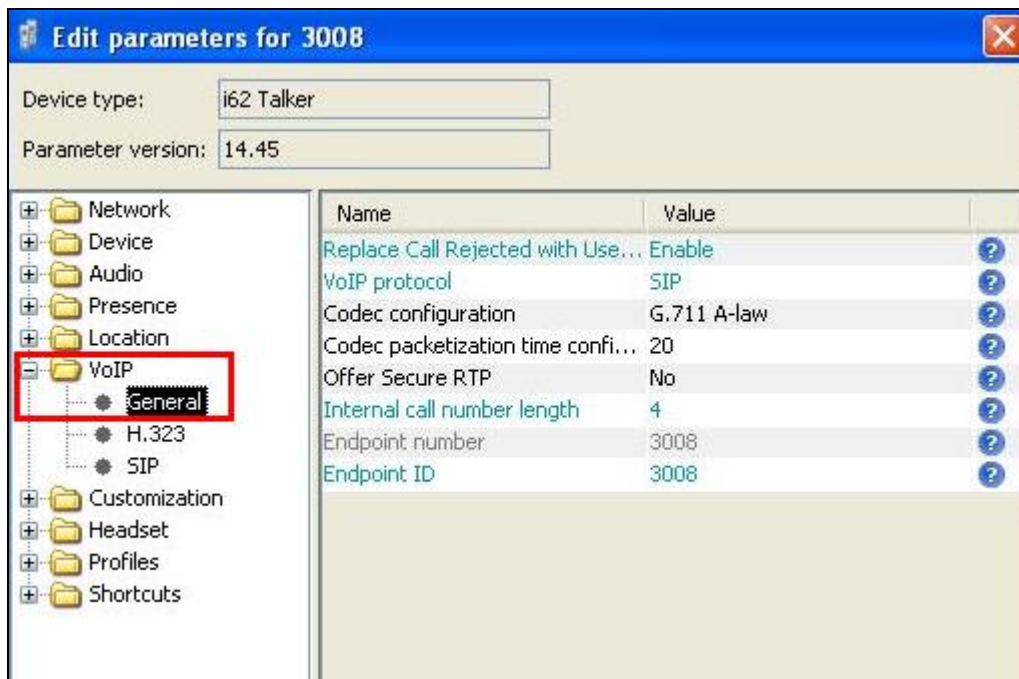


Figure 30: i62 Numbers Tab, VoIP→General Screen

Select the **VoIP→SIP** menu point, and enter the values shown in the following table.

Parameter	Usage
SIP proxy IP address	Enter the IP address of Session Manager.
SIP proxy password	Enter the password assigned to the endpoint in Figure 25 .
Registration identity	Enter Endpoint ID .
Authentication identity	Enter Endpoint ID .
Call forwarding locally	Enter Enabled .
SIP Register Expiration	Enter 120 .

Table 17: i62 Numbers Tab, VoIP→SIP Parameters



Figure 31: i62 Numbers Tab, VoIP→SIP Screen

8. Verification Steps

Correct installation and configuration can be verified by performing the steps shown below.

8.1. Verify Avaya Aura® Communication Manager SIP Connection

Enter the “status signaling-group” command from the Communication Manager SAT terminal and verify that the signaling group is in the “in-service” state.

```
status signaling-group 8
                        STATUS SIGNALING GROUP

      Group ID: 8                Active NCA-TSC Count: 0
      Group Type: h.323          Active CA-TSC Count: 0
      Signaling Type: facility associated signaling
      Group State: in-service
```

Figure 32: Signaling Group Status

Enter the “status trunk” command from the Communication Manager SAT terminal and verify that the all of the trunk members are in the “in-service/idle” state.

```
status trunk 8
                        TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                          Busy
0008/001 T00019   in-service/idle   no
0008/002 T00020   in-service/idle   no
0008/003 T00021   in-service/idle   no
0008/004 T00022   in-service/idle   no
0008/005 T00023   in-service/idle   no
0008/006 T00024   in-service/idle   no
0008/007 T00025   in-service/idle   no
0008/008 T00026   in-service/idle   no
0008/009 T00027   in-service/idle   no
0008/010 T00028   in-service/idle   no
```

Figure 33: Trunk Status

8.2. Verify Ascom i62 Handset

The i62 handset connection to Session Manager can be verified by absence of an error message on the handset display just above the red line at the bottom of the display, as shown in the following illustration.

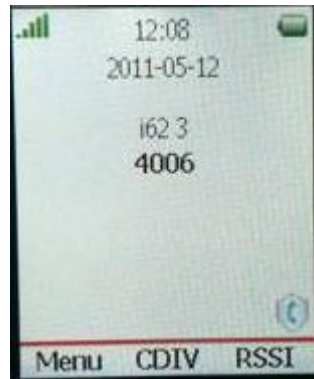


Figure 34: i62 Display Screen

9. Conclusion

These Application Notes contain instructions for configuring a solution with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Ascom i62 wireless handsets. A list of instructions is provided to enable the user to verify that the various components have been correctly configured.

10. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Installing and Configuring Avaya Aura® Communication Manager*,
- [2] *Administering Avaya Aura® Communication Manager*
- [3] *Administering Avaya Aura® Session Manager*
- [4] *Installing and Configuring Avaya Aura® Session Manager*
- [5] *Maintaining and Troubleshooting Avaya Aura® Session Manager*

Ascom's technical documentation is available through a local supplier.

- [1] *User Manual Ascom i62 VoWiFi Handset (TD 92599GB)*
- [2] *Configuration Manual Ascom i62 VoWiFi Handset (TD 92675GB)*
- [3] *System Description Ascom VoWiFi System (TD 92313GB)*
- [4] *System Planning Ascom VoWiFi System (TD 92408GB)*

©2012 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.