



## DevConnect Program

---

# Application Notes for configuring Fijowave Business DECT with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

## Abstract

These Application Notes describe the configuration steps for provisioning Fijowave Business DECT to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

# 1. Introduction

These Application Notes describe the configuration steps for provisioning Fijowave Business DECT to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1. Fijowave Business DECT consists of DECT handsets and DECT Multi Cell Base Stations. The DECT handsets are configured to register with Session Manager using SIP signaling and are also subscribed to the Base Station using DECT signaling. Each handset is configured as a SIP user on Communication Manager as Avaya 9641 SIP endpoint. The DECT handsets then behave as third-party SIP extensions on Communication Manager able to make/receive internal calls and have full voicemail and other telephony facilities available on Communication Manager.

Some of the acronyms that are used throughout this document are as follows.

- IP (Internet Protocol) – Universal standard for inter-networking that maximizes scalability and interoperability.
- DECT (Digital Enhanced Cordless Telecommunications) - Secure radio communication standard that delivers superior voice quality over reserved radio frequency bands.
- SIP (Session Initiation Protocol) - A signaling protocol that enables the Voice Over Internet Protocol (VoIP) by defining the messages sent between endpoints and managing the actual elements of a call. SIP supports voice calls, video conferencing, instant messaging, and media distribution.

## 2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of DECT handsets to make and receive calls to and from Avaya H.323, SIP and Digital deskphones as well as a simulated PSTN. Avaya Messaging (Messaging) was used to allow users to leave voicemail messages and to demonstrate Message Waiting Indication working on the DECT handsets.

Fijowave can use both UDP and TCP as the SIP transport protocol; however, if TCP is chosen as the transport protocol for the Fijowave DECT then a SIP Entity and an Entity Link are required for the Fijowave DECT Master and Standby base stations. The setup of a SIP Entity must use the “Endpoint Concentrator Connection Policy”. Refer to **Section 6.2** for configuration details.

Starting with Session Manager Release 6.3.9, an “Endpoint Concentrator” can be selected as a SIP Entity type. This Endpoint Concentrator type allows up to 1000 connections from a single IP address. The single IP address can be shared by multiple Windows instances running on a Virtualized server or multiple DECT handsets sharing the same base station IP address.

A new connection policy, Endpoint Concentrator, can be assigned to a SIP entity link. The Session Manager allows up to 1000 connections on that SIP entity link. The Endpoint Concentrator policy is an untrusted policy based on the current Default (endpoint) policy. That is, the requests arriving over the SIP entity link with the connection policy Endpoint Concentrator are challenged as for any other endpoint. To identify and administer the SIP entities hosting multiple endpoints, this release introduces a new entity type, Endpoint Concentrator.

**Note:** SIP Link Monitoring is not available for SIP entities of type Endpoint Concentrator.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/handsets that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/handsets for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Fijowave DECT handsets did not include use of any specific encryption features as requested by Fijowave.

## **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 deskphones, Avaya Workplace for Windows, Avaya H.323 deskphones, Avaya Digital, Fijowave DECT endpoints and PSTN endpoints.

- Registration
- Basic Calls
- Hold, Retrieve and Brokering (Toggle)
- Feature Access Code dialing
- Attended, Semi-attended and Blind Transfer
- Three Party Conference
- Call Forwarding Unconditional, No Reply and Busy
- Call Waiting
- Call Park/Pickup

- EC500, where Avaya deskphone is the primary phone and DECT handset being the EC500 destination
- Do Not Disturb
- Calling Line Name/Identification
- Codec Support (G.711A, G.711U, G.726A-32K tested)
- DTMF Support
- Voice Mail, Message Waiting Indication
- Serviceability

**Note:** Compliance testing does not include redundancy testing as standard. Where some LAN failures were simulated, and the results observed, there were no redundancy or failover tests performed.

## 2.2. Test Results

Tests were performed to verify interoperability between Fijowave DECT handsets and Communication Manager deskphones. The tests were all functional in nature and performance testing or redundancy testing were not included.

The following observations/limitations were noted during testing.

1. All compliance testing was done using UDP (preferred) and TCP as the transport protocol.
2. One DECT handset was paired with a '330 headset' from Fijowave, this allowed calls to be heard on the headset and calls could be answered and hung up from that headset also.
3. A SIP Entity with "Endpoint Concentrator" assigned was set up for the Fijowave Business DECT Base Station, the corresponding TCP entity links were setup as type "Endpoint Concentrator".
4. In the scenario where an Avaya station calls DECT1 and DECT1 does a semi-attended transfer to DECT2. The DECT2 display shows DECT1 information instead of the Avaya station information until the call is answered.
5. When using the EC500 (concurrent call) feature, if DECT handset or an Avaya endpoint answers the call before two rings, the call is dropped. This is due to the "Cellular Voice Mail Detection" field default value seen in "off-pbx-telephone configuration-set" form of Communication Manager. The default value for this field is "timed (seconds): 4" which means that if Communication Manager receives an answer within 4 seconds, then it will be considered as the cellular voicemail picking up the call, and so call will be dropped and proceed to do Communication Manager coverage processing instead. The workaround is to answer the call after 2 rings or change the "Cellular Voice Mail Detection" field value to "none" or decrease "timed" value. Note that changing the "off-pbx-telephone configuration-set" affects all users in the same set, so if cellular users are grouped with DECT handset users, calls may be answered by a cellular user's voicemail instead of following the coverage criteria in Communication Manager.
6. A DECT handset is configured on an Avaya station as EC500. Call Avaya station, both Avaya station and DECT handset rings. Decline the call at DECT handset, Avaya station continues to ring as per normal design.

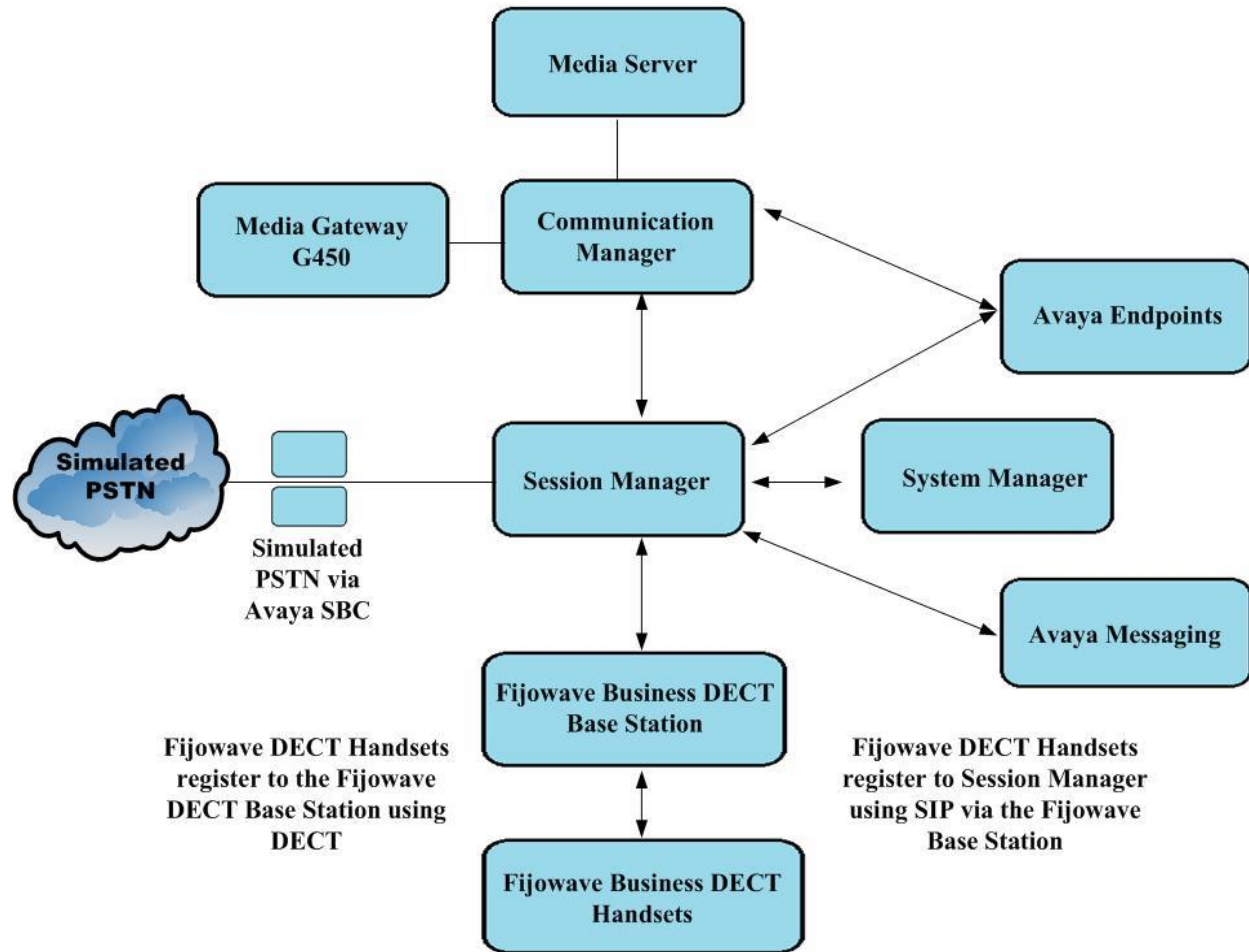
## 2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 10** of these Application Notes. Technical support for the Fijowave Business DECT product can be obtained as follows:

- Web: <http://www.fijowave.com>
- Email: [sales@fijowave.com](mailto:sales@fijowave.com)
- Help desk: +353 1 525 3072

### 3. Reference Configuration

**Figure 1** shows the network topology during compliance testing. The Fijowave DECT handsets connect to the Fijowave DECT base station which is placed on the telephony LAN. The DECT handsets register with Session Manager in order to make/receive calls to and from the Avaya H.323, SIP and Digital deskphones on Communication Manager. During compliance testing, the DECT base stations were configured by accessing them via a web interface on a Windows PC.



**Figure 1: Network Solution of Fijowave Business DECT with Avaya Aura® Communication Manager and Avaya Aura® Session Manager**

## 4. Equipment and Software Validated

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

Avaya Equipment/Software	Release/Version
Avaya Aura® System Manager	System Manager 10.1.3.0 Feature Pack 3 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.0.0715713
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.3.0.1013007
Avaya Aura® Communication Manager	R10.1.3.0 – FP3 R020x.01.0.974.0 Update ID 01.0.974.0-27893
Avaya Session Border Controller	R10.1
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G430	42.7.0 /2
Avaya J100 Series (H323) Deskphone	6.8.5.3.2
Avaya J100 Series (SIP) Deskphone	4.0.14.0.7
Avaya 9404 Digital Deskphone	17.0
Avaya Workplace for Windows (SIP)	3.33.0.96
Fijowave Equipment/Software	Release/Version
Fijowave DECT Base Station	Multi-Cell 240: s/n 23240000102 (Primary) s/n 23240000103 (Secondary) Software: V700 B100
Fijowave DECT Handsets/Headset	s/n 20310004042 (310) s/n 19315000246 (315) s/n 23318000006 (318) s/n 23330000100 (330 Headset) Software: V700 B100

All Avaya Aura® equipment are running on VMware virtual servers.

## 5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing with SIP trunks in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 10** of these Application Notes.

**Note:** A printout of the Signaling and Trunk group that were used during compliance testing can be found in the **Appendix** of these Application Notes.

The following sections go through the following.

- System Parameters
- Dial Plan Analysis
- Feature Access Codes
- Network Region
- IP Codec
- Coverage Path and Hunt Group for Voicemail

### 5.1. Configure System Parameters

Ensure that the SIP endpoints license is valid as shown below by using the command **display system-parameters customer-options**.

display system-parameters customer-options		Page	1 of 12
OPTIONAL FEATURES			
G3 Version: V20	Software Package: Enterprise		
Location: 2	System ID (SID): 1		
Platform: 28	Module ID (MID): 1		
		USED	
Platform Maximum Ports:		48000	168
Maximum Stations:		36000	44
Maximum XMOBILE Stations:		36000	0
Maximum Off-PBX Telephones - EC500:		41000	2
<b>Maximum Off-PBX Telephones - OPS:</b>		<b>41000</b>	<b>20</b>
Maximum Off-PBX Telephones - PBFMC:		41000	0
Maximum Off-PBX Telephones - PVFMC:		41000	0
Maximum Off-PBX Telephones - SCCAN:		0	0
Maximum Survivable Processors:		313	1



Note that the SIP Endpoint Managed Transfer parameter was set to n, as setting this to “y” may interfere with attended transfers. Type **change system-parameters features** and on **Page 19** ensure that the **SIP Endpoint Managed Transfer** parameter is set to **n**.

change system-parameters features	Page 19 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
IP PARAMETERS	
Direct IP-IP Audio Connections? y	IP Audio Hairpinning? n
Synchronization over IP? n	Allow SIP-H323 Video in SDES? n
Initial INVITE with SDP for secure calls? y	
<b>SIP Endpoint Managed Transfer? n</b>	
Expand ISDN Numbers to International for 1XCES? n	
CALL PICKUP	
Maximum Number of Digits for Directed Group Call Pickup: 4	
Call Pickup on Intercom Calls? y	Call Pickup Alerting? y
Temporary Bridged Appearance on Call Pickup? y	Directed Call Pickup? y
Extended Group Call Pickup: simple	
Enhanced Call Pickup Alerting? n	
Call Pickup for Call to Coverage Answer Group? y	
Display Information With Bridged Call? y	
Keep Bridged Information on Multiline Displays During Calls? y	
PIN Checking for Private Calls? n	

## 5.2. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **3**. Feature Access Codes (**fac**) use digits **8** and **9** and use characters **\*** or **#**.

change dialplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 5			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	4	udp							
2	4	udp							
3	4	ext							
4	4	ext							
5	4	udp							
666	4	ext							
8	1	fac							
9	1	fac							
*	3	fac							
*8	4	dac							
#	3	fac							

Under **aar analysis**, **31** was set to go out over the SIP trunk 11 on **Route Pattern 11**, as shown below. This is used for SIP phones to allow the connection between Session Manager and Communication Manager and would have been setup as part of the initial installation and configuration of the Aura® platform. The configuration of Signaling Group 11 and Trunk Group 11 are shown in the **Appendix**.

change aar analysis 3						Page 1 of 2
AAR DIGIT ANALYSIS TABLE						
Location: all						Percent Full: 1
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node ANI Num Req'd
<b>31</b>		<b>4</b>	<b>4</b>	<b>11</b>	<b>lev0</b>	<b>n</b>
4		7	7	999	aar	n
5		7	7	999	aar	n
666		4	4	66	aar	n
7		7	7	999	aar	n
8		7	7	999	aar	n
9		7	7	999	aar	n
						n
						n

### 5.3. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be entered from DECT handsets to initiate Communication Manager call features. These access codes must be compatible with the dial plan described in **Section 5.2**. Some of the access codes configured during compliance testing are shown below.

change feature-access-codes						Page 1 of 12
FEATURE ACCESS CODE (FAC)						
Abbreviated Dialing List1 Access Code: *11						
Abbreviated Dialing List2 Access Code: *12						
Abbreviated Dialing List3 Access Code: *13						
Abbreviated Dial - Prgm Group List Access Code: *10						
Announcement Access Code: *27						
Answer Back Access Code: #02						
Attendant Access Code:						
Auto Alternate Routing (AAR) Access Code: 8						
Auto Route Selection (ARS) - Access Code 1: 9						Access Code 2:
Automatic Callback Activation: *05						Deactivation: #05
Call Forwarding Activation Busy/DA: *03 All: *04						Deactivation: #04
Call Forwarding Enhanced Status: *73 Act: *74						Deactivation: #74
Call Park Access Code: *02						
Call Pickup Access Code: *09						
CAS Remote Hold/Answer Hold-Unhold Access Code:						
CDR Account Code Access Code: *14						
Change COR Access Code:						
Change Coverage Access Code:						
Conditional Call Extend Activation:						Deactivation:
Contact Closure Open Code:						Close Code:

## 5.4. Configure Network Region

Use **change ip-network-region x** (where x is the network region to be configured) to assign an appropriate domain name to be used by Communication Manager, in the example below **greaneyp.sil6.avaya.com** is used. Note that this domain is also configured in **Section 6.1.1**.

<b>change ip-network-region 1</b>		Page 1 of 20
		IP NETWORK REGION
Region: 1	NR Group: 1	
Location:	Authoritative Domain: <b>greaneyp.sil6.avaya.com</b>	
Name: PGDefault	Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

## 5.5. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the DECT handsets. During compliance testing the codecs **G.711A**, **G.711MU** and **G.726A-32K** were tested.

Media Encryption is used between Avaya handsets and so **1-srtp-aescm128-hmac80** is set under **Media Encryption**. **None** is also entered to ensure that handsets that do not support Media Encryption can communicate.

change ip-codec-set 1

Page1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size (ms)
1: OPUS-WB20K		1	20
2: <b>G.726A-32K</b>		<b>2</b>	<b>20</b>
3: <b>G.711A</b>	<b>n</b>	<b>2</b>	<b>20</b>
4: <b>G.711MU</b>	<b>n</b>	<b>2</b>	<b>20</b>
5:			
6:			

Media Encryption

Encrypted SRTCP: best-effort

1: **1-srtp-aescm128-hmac80**

2: **none**

3:

4:

5:

## 5.6. Configuration of Coverage Path and Hunt Group for Voicemail

The coverage path setup used for compliance testing is illustrated below. Note the following:

**Don't Answer** is set to **y**: The coverage path will be used in the event the phone set is not answered.

**Number of Rings** is set to **3**: The coverage path will be used after 3 rings.

**Point 1** is set to **h68**: Hunt Group 68 is utilised by this coverage path.

```
display coverage path 1

                                COVERAGE PATH

                                Coverage Path Number: 1
                                Cvg Enabled for VDN Route-To Party? n      Hunt after Coverage? n
                                Next Path Number:                        Linkage

COVERAGE CRITERIA
  Station/Group Status    Inside Call    Outside Call
    Active?                n                n
    Busy?                  Y                Y
    Don't Answer?        Y            Y            Number of Rings: 3
    All?                   n                n
  DND/SAC/Goto Cover?     Y                Y
  Holiday Coverage?       n                n

COVERAGE POINTS
  Terminate to Coverage Pts. with Bridged Appearances? n
Point1: h68              Rng: 3    Point2:
Point3:                    Point4:
Point5:                    Point6:
```

The hunt group used for compliance testing is shown below. Note that on **Page 1** the **Group Extension** is **6668**, which is used to dial for messaging and **Group Type** is set to **ucd-mia**.

```
display hunt-group 68                                     Page 1 of 60

                                HUNT GROUP

                                Group Number: 68                ACD? n
                                Group Name: Messaging            Queue? n
                                Group Extension: 6668           Vector? n
                                Group Type: ucd-mia             Coverage Path:
                                TN: 1                            Night Service Destination:
                                COR: 1                           MM Early Answer? n
                                Security Code:                    Local Agent Preference? n
                                ISDN/SIP Caller Display:

SIP URI::
```

On **Page 2**, **Message Center** is set to **sip-adjunct**. The **Voice Mail Number** is set to 6668.

display hunt-group 68		Page 2 of 60
HUNT GROUP		
<b>Message Center: sip-adjunct</b>		
<b>Voice Mail Number</b>	Voice Mail Handle	Routing Digits
		(e.g., AAR/ARS Access Code)
<b>6668</b>	6668	8

## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Configure SIP Entity and Entity Link
- Adding Fijowave DECT SIP Users

To make changes on Session Manager a web session is established to System Manager. Log into System Manager by navigating to <https://<System Manager FQDN>/SMGR>. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

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

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

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:   
Password:

[Change Password](#)

**Supported Browsers:** Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

Once logged in navigate to **Elements** and click on **Routing**. This area is where the domain, location and SIP Entities are added.

Avaya Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾

Search [ ] admin

**Routing** (highlighted in the Elements menu)

Elements	Count	Sync Status
Avaya Breeze	3	■
CM	1	■
Session Manager	1	■
System Manager	1	■
UCM Applications	8	■

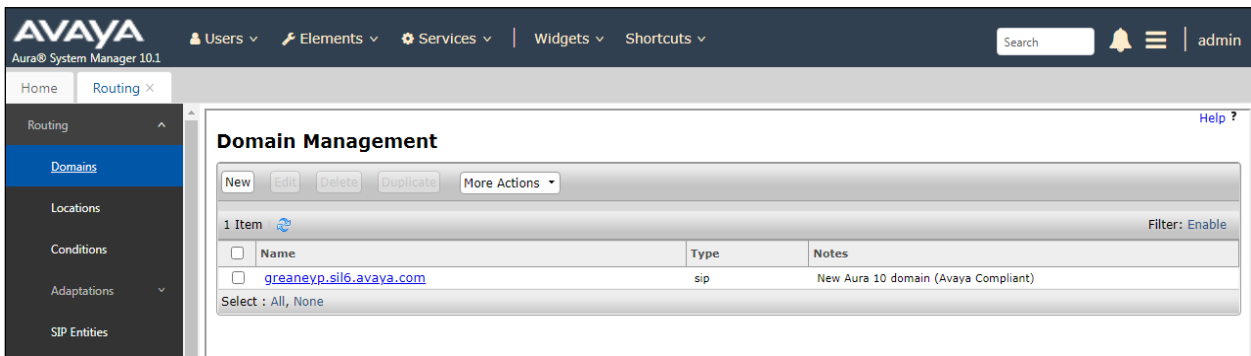
Current Usage :  
7/250000 USERS  
1/50

## 6.1. Domains and Locations

**Note:** It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

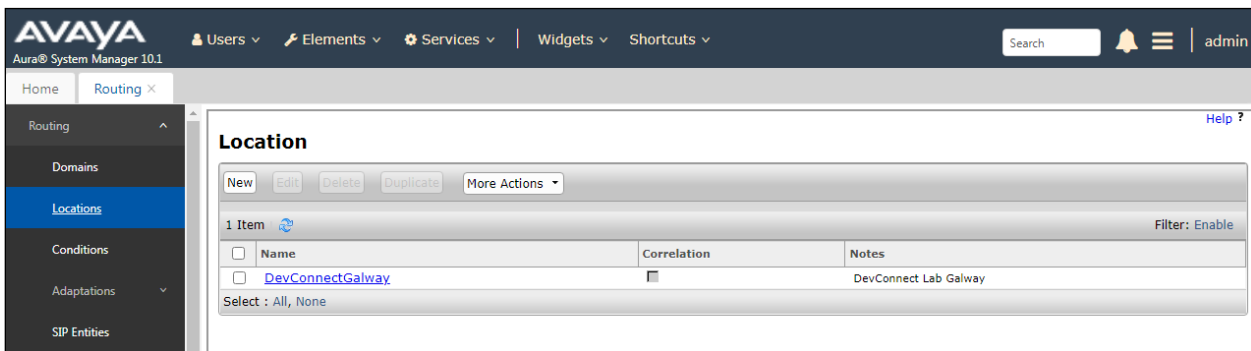
### 6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **greaneyp.sil6.avaya.com** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.



### 6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectGalway** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.





## 6.2. Configure SIP Entity and Entity Link

Clicking on **SIP Entities** in the left window shows what SIP Entities have been added to the system and allows the addition of any new SIP Entity that may be required. Please note the SIP Entities already present for the compliance testing of Fijowave's DECT handsets.

- Communication Manager SIP Entity
- Session Manager SIP Entity
- Messaging SIP Entity

There is no SIP Entity required if UDP is chosen for the transport protocol in **Section 7**, however if TCP is chosen as the transport protocol for the Fijowave DECT then a SIP Entity and an Entity Link are required for the Fijowave base station(s). Select **SIP Entities** in the left window and click on **New** in the main window.

**Note:** If there is a Primary and Secondary base station, then a SIP Entity and Entity link are required for both base stations.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The main content area is titled 'SIP Entities' and features a table with 9 items. The table has columns for Name, FQDN or IP Address, Type, and Notes. The 'New' button in the top action bar is highlighted with a red box.

Name	FQDN or IP Address	Type	Notes
Breeze1-wspaces-sm100	10.10.40.52	Avaya Breeze	Breeze 1 for wspaces
Breeze2-wspaces-sm100	10.10.40.53	Avaya Breeze	Breeze 2 for wspaces
Breeze3-wspaces-sm100	10.10.40.54	Avaya Breeze	Breeze 3 for wspaces
cm101x - Phones - 5061	10.10.40.13	CM	For SIP PHONES on CM
cm101x - SIM PSTN - 5063	10.10.40.13	CM	For Simulated SIP Trunk
cm101x - SIP TRUNK - 5062	10.10.40.13	CM	SIP Trunk in and out
Messaging2019	10.10.40.75	SIP Trunk	To messaging on win 2019
SBCE - SIM - PSTN	10.10.40.158	SIP Trunk	For Simulated PSTN
sm101x	10.10.40.12	Session Manager	Primary Session Manager

Enter a suitable **Name** and enter the **IP Address** of the DECT Base Station. Select **Endpoint Concentrator** as the **Type**. Under Entity Links, ensure that **TCP** is selected for the **Protocol** and **5060** for the **Port**. Click on **Commit** once completed.

SIP Entity Details

CommitCancel

General

\* Name: FijowaveDECT-Primary

\* FQDN or IP Address: 10.10.40.120

Type: Endpoint Concentrator

Notes: FijowaveDECT-Primary

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Entity Links

Override Port & Transport with DNS SRV: ☐

AddRemove

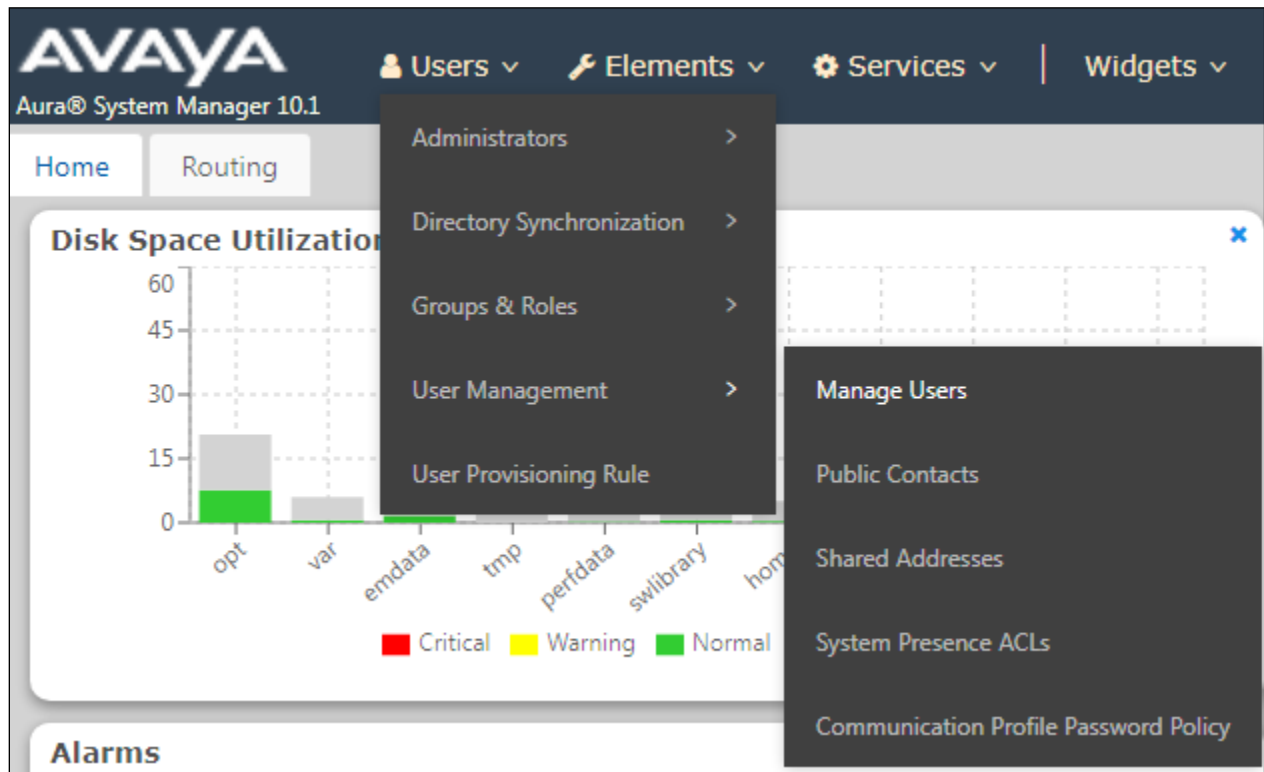
1 Item Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
<input type="checkbox"/>	* sm101x_FijowaveDECT-	sm101x	TCP	* 5060	FijowaveDECT-Primary	* 5060

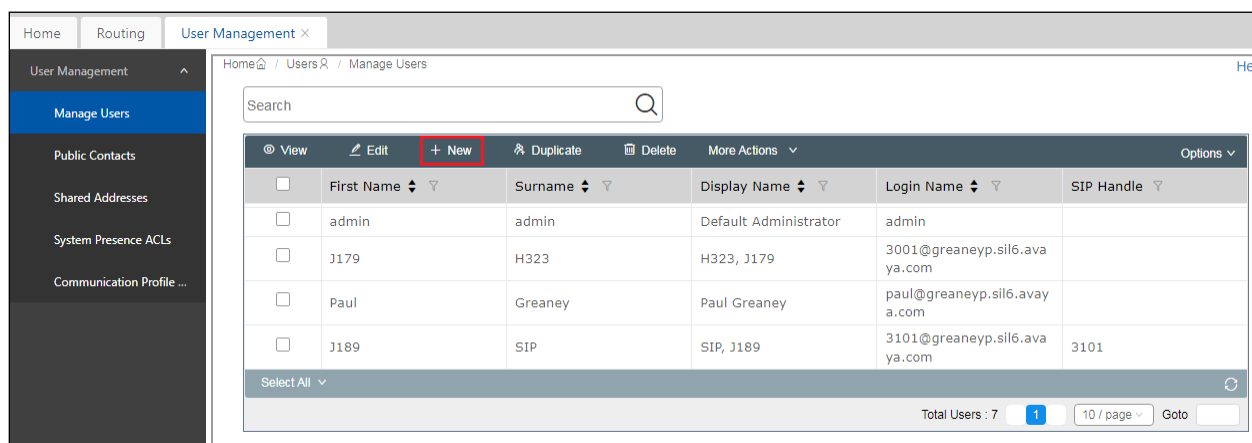
Select : All, None

## 6.3. Adding Fijowave SIP Users

From the home page click on **User Management** → **Manager Users** shown below.



From **Manager Users** section, click on **New** to add a new SIP user.



Under the **Identity** tab fill in the user's **Last Name** and **First Name** as shown below. Enter the **Login Name**, following the format of "user id@domain".

**User Profile | Edit | 3191@greanep.sil6.avaya.com**

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule: [v]

\* Last Name: 3191 Last Name (in Latin alphabet characters): 3191

\* First Name: FijowaveDECT First Name (in Latin alphabet characters): FijowaveDECT

\* Login Name: 3191@greanep.sil6.ava Middle Name: Middle Name Of User

Description: FijowaveDECT Email Address: Email Address Of User

Password: [ ] User Type: Basic [v]

Confirm Password: [ ] Localized Display Name: 3191, FijowaveDECT

Endpoint Display Name: 3191, FijowaveDECT Title Of User: Title Of User

Language Preference: English (United Stat... [v] Time Zone: (+1:0)GMT : Dublin,... [v]

Employee ID: Employee Id Of User Department: Department Of User [v]

Under the **Communication Profile** tab enter **Communication Profile Password** and **Re-enter Comm-Profile Password**, note that his password is required when configuring the DECT handset in **Section 7**Error! Reference source not found..

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary [v]

Communication Address

PROFILES

Session Manager Profile [ ]

Avaya Breeze® Profile [ ]

CM Endpoint Profile [ ]

Comm-Profile Password

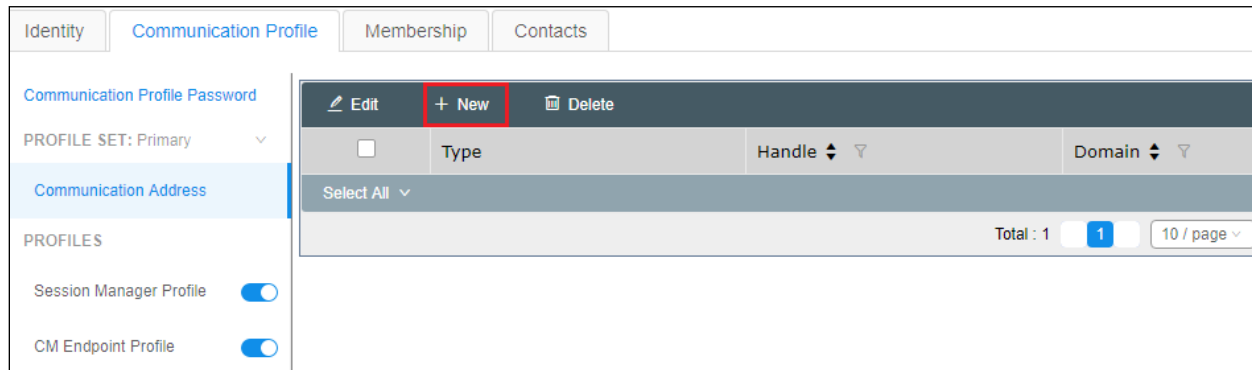
Comm-Profile Password: [ ]

\* Re-enter Comm-Profile Password: [ ]

Generate Comm-Profile Password

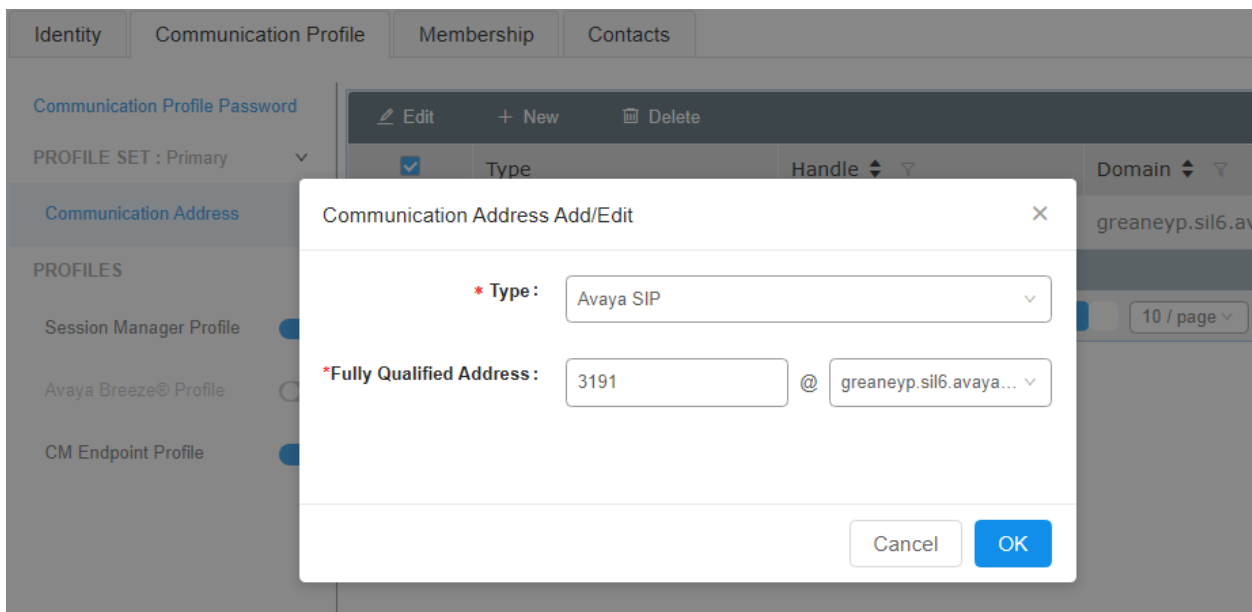
Cancel OK

Staying on the **Communication Profile** tab, click on **New** to add a new **Communication Address**.



The screenshot shows the 'Communication Profile' tab in a web interface. On the left sidebar, 'Communication Address' is selected under the 'PROFILES' section. The main area has a dark header with 'Edit', '+ New' (highlighted with a red box), and 'Delete' buttons. Below this is a table with columns 'Type', 'Handle', and 'Domain'. A 'Select All' dropdown is on the left of the table. At the bottom right of the table area, it says 'Total : 1' with a blue box containing '1' and '10 / page'.

Enter the extension number and the domain for the **Fully Qualified Address** and click on **OK** once finished.



The screenshot shows the 'Communication Address Add/Edit' dialog box. It has a close button (X) in the top right. The form contains two fields: '\* Type :' with a dropdown menu showing 'Avaya SIP', and '\*Fully Qualified Address :' with two input boxes. The first box contains '3191' and the second box contains 'greanep.sil6.avaya...' with a dropdown arrow. At the bottom right are 'Cancel' and 'OK' buttons.

Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details, enter the **Origination Sequence** and the **Termination Sequence**. Scroll down to complete the profile. Enter the **Home Location**, this should be the location configured in **Section 6.1.2**. Click on Commit at the top of the page (not shown).

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

SIP Registration

\* Primary Session Manager :

sm101x

Secondary Session Manager :

Start typing...

Survivability Server :

Start typing...

Max. Simultaneous Devices :

1

Block New Registration When Maximum Registrations

Active?

Application Sequences

Origination Sequence :

CM-APP-SEQ

Termination Sequence :

CM-APP-SEQ

Emergency Calling Application Sequences

Emergency Calling Origination Sequence :

Select

Emergency Calling Termination Sequence :

Select

Call Routing Settings

\* Home Location :

DevConnectGalway

Conference Factory Set :

Select

PG; Reviewed:  
SPOC 9/27/2023

Avaya DevConnect Application Notes  
©2023 Avaya LLC. All Rights Reserved.

22 of 36  
FijoDECT\_CM101

Click on the **CM Endpoint Profile** in the left window. Select the Communication Manager that is configured for the **System** and choose the **9641SIP\_DEFAULT\_CM\_10\_1** as the **Template**. Enter the appropriate **Voice Mail Number** and **Sip Trunk** should be set to **aar**, providing that the routing is setup correctly on Communication Manager. The **Profile Type** should be set to **Endpoint** and the **Extension** is the number assigned to the DECT handset. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

User Profile | Edit | 3191@greaney.sil6.avaya.com

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

\* System :

cm101x

\* Profile Type :

Endpoint

Use Existing Endpoints :

☐

\* Extension :

3191

Template :

9641SIP\_DEFAULT\_C

\* Set Type :

9641SIP

Security Code :

Enter Security Code

Port :

S000010

Voice Mail Number :

6668

Preferred Handle :

Select

Calculate Route Pattern :

☐

Sip Trunk :

aar

SIP URI :

Select

Enhanced Callr-Info Display for 1-line phones :

☐

Delete on Unassign from User or on Delete User :

☒

Override Endpoint Name and Localized Name :

☒

Under the **General Options** tab ensure that **Coverage Path 1** is set to that configured in **Section 5.6**. Also ensure that **Message Lamp Ext.** is showing the correct extension number. The **Class of Restriction** and **Class of Service** should be set to the appropriate values for the DECT handset. This may vary depending on what level of access/permissions the handset has been given. Other tabs can be checked but for compliance testing the values were left as default. Click on **Done** (not shown) to complete.

**Note:** For compliance testing the default value of three call appearance buttons were used. This can be changed under the **Button Assignment** tab.

<b>System</b>	cm101x	<b>Extension</b>	3191
<b>Template</b>	9641SIP_DEFAULT_CM_10_1	<b>Set Type</b>	9641SIP
<b>Port</b>	S000010	<b>Security Code</b>	
<b>Name</b>	3191, FijowaveDECT		

<b>General Options (G)</b> *	<b>Feature Options (F)</b>	<b>Site Data (S)</b>	<b>Abbreviated Call Dialing (A)</b>	<b>Enhanced Call Fwd (E)</b>
<b>Button Assignment (B)</b>	<b>Profile Settings (P)</b>	<b>Group Membership (M)</b>		

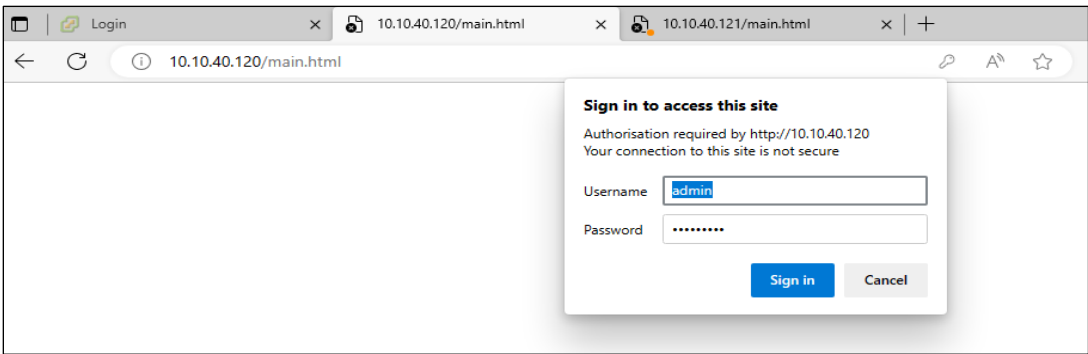
* <b>Class of Restriction (COR)</b>	1	* <b>Class Of Service (COS)</b>	1
* <b>Emergency Location Ext</b>	3191	* <b>Message Lamp Ext.</b>	3191
* <b>Tenant Number</b>	1		
* <b>SIP Trunk</b>	Qaar	<b>Type of 3PCC Enabled</b>	None
<b>Coverage Path 1</b>	3	<b>Coverage Path 2</b>	
<b>Lock Message</b>	<input type="checkbox"/>	<b>Localized Display Name</b>	3191, FijowaveDECT
<b>Multibyte Language</b>	Not Applicable	<b>Enable Reachability for Station Domain Control</b>	system
<b>SIP URI</b>			
<b>Attendant</b>	<input type="checkbox"/>		
<b>Primary Session Manager</b>			
<b>IPv4:</b>	10.10.40.12	<b>IPv6:</b>	
<b>Secondary Session Manager</b>			
<b>IPv4:</b>		<b>IPv6:</b>	

Once the **CM Endpoint Profile** is completed correctly, click on **Commit** to save the new user (not shown).

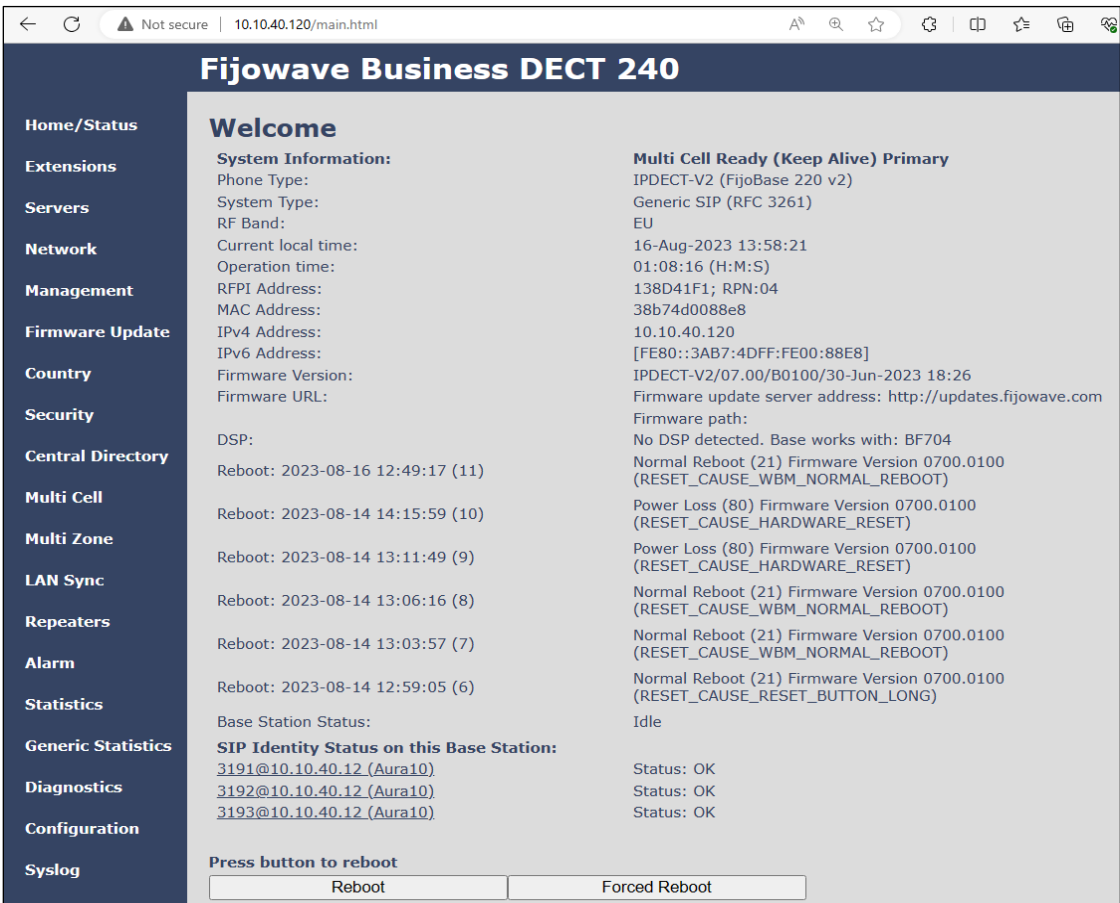


## 7. Configure Fijowave DECT Base Station and Handsets

The configuration of the DECT base station and the DECT handsets is carried out by opening a web browser to the IP address of the DECT base station acting as Master. Once the web page is accessed the following login popup appears. Enter the appropriate credentials for **Username** and **Password** and click on **Sign in**.



The following window is opened, the connection to Session Manager is configured using the menus along the left side.



Click on **Servers** in the left window and click on **Add Server**. Enter a suitable name for the **Server Alias**. The IP address of the Session Managers SM100 (SIP address) is entered for both **Registrar** and **Outbound Server**. For compliance testing **SIP Transport** was set to **UDP**. **DTMF Signaling** was set to **RFC 2833** but this can be changed should it be required. The **Codec Priority** can be changed as per the requirement of the site in question.

Click on **Save** at the bottom of the screen (not shown).

<a href="#">Home/Status</a> <a href="#">Extensions</a> <a href="#">Servers</a> <a href="#">Network</a> <a href="#">Management</a> <a href="#">Firmware Update</a> <a href="#">Country</a> <a href="#">Security</a> <a href="#">Central Directory</a> <a href="#">Multi Cell</a> <a href="#">Multi Zone</a> <a href="#">LAN Sync</a> <a href="#">Repeaters</a> <a href="#">Alarm</a> <a href="#">Statistics</a> <a href="#">Generic Statistics</a> <a href="#">Diagnostics</a> <a href="#">Configuration</a> <a href="#">Syslog</a> <a href="#">SIP Log</a> <a href="#">Emergency Call</a>	Servers	<h3 style="margin: 0;">Aura10:</h3> <p style="margin: 0;">10.10.40.12</p> <p style="margin: 0;"><a href="#">Add Server</a></p> <p style="margin: 0;"><a href="#">Remove Server</a></p>	
		<b>Aura10:</b> Server Alias: NAT Adaption: Registrar: Outbound Proxy: Conference Server: Call Log Server: Reregistration time (s): SIP Session Timers: Session Timer Value (s): SIP Transport: Signal TCP Source Port: Use One TCP Connection per SIP Extension: RTP from own base station: Keep Alive: Show Extension on Handset Idle Screen: Remote Ring Tone Control: Attended Transfer Behaviour: Semi-Attended Transfer Behaviour: Directed Call Pickup: Directed Call Pickup Code: Group Call Pickup: Group Call Pickup Code: DTMF Signalling: Remote Caller ID Source Priority:  Codec Priority: - Max number of codecs is 5	<div style="border: 1px solid #ccc; padding: 2px;">Aura10</div> <div style="border: 1px solid #ccc; padding: 2px;">Disabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">10.10.40.12</div> <div style="border: 1px solid #ccc; padding: 2px;">10.10.40.12</div> <div style="border: 1px solid #ccc; padding: 2px;"></div> <div style="border: 1px solid #ccc; padding: 2px;"></div> <div style="border: 1px solid #ccc; padding: 2px;">600</div> <div style="border: 1px solid #ccc; padding: 2px;">Disabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">1800</div> <div style="border: 1px solid #ccc; padding: 2px;">UDP ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">Enabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">Disabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">Disabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">Enabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">Enabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">Enabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">Hold 2nd Call ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">Allow Semi-Attended Transfer ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">Disabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;"></div> <div style="border: 1px solid #ccc; padding: 2px;">Disabled ▼</div> <div style="border: 1px solid #ccc; padding: 2px;"></div> <div style="border: 1px solid #ccc; padding: 2px;">RFC 2833 ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">PAI - FROM ▼</div> <div style="border: 1px solid #ccc; padding: 2px;">         G711A          G711U          G726       </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 10px;">Up</div> <div style="border: 1px solid #ccc; padding: 2px 10px;">Down</div> </div>

Click on **Extensions** in the left window. Click on **Add extension** in the main window.

**Fijowave Business DECT 240**

**Extensions**

AC: 0000

Save Cancel

Add extension  
Stop Registration

	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress	VoIP Idx	Extension	Display Name	Server
<input type="checkbox"/>	1	0298DC381F	Present@RPN04	315 700.100	Off	<input type="checkbox"/> 3	3193	3193	10.10.40.12
<input type="checkbox"/>	2	02E6900F64	Present@RPN04	330 700.100	Off	<input type="checkbox"/> 3	3193	3193	10.10.40.12

Check All / Check All Extensions /  
Uncheck All Uncheck All Extensions

With selected: Delete Handset(s) Register Handset(s) Deregister Handset(s) Start SIP Registration(s) SIP Delete Extension(s)

**Handset** is set to the DECT configured handset (**New Handset** when adding a new extension). **Line name**, **Extension** and **Mailbox Name** were all set to the SIP user extension as per **Section 6.3**. **Authentication User Name** and **Authentication Password** are set as per **Section 6.3**. **Mailbox Number** is set to that configured in **Section 5.6**. Server is set to that configured on the previous page. Features such as 'Call Waiting', and 'Call Forward' are set on a per extension basis, for compliance testing **Call waiting feature** was **Enabled**. Click on **Save** once all is configured. A reboot may be required.

Line name: 3191

Handset: New Handset

Push-To-Talk: Disabled

Extension: 3191

Authentication User Name: 3191

Authentication Password: .....

Display Name: 3191

Mailbox Name: 3191

Mailbox Number: 6668

Server: Aura10: 10.10.40.12

Call waiting feature: Enabled

BroadWorks Busy Lamp Field List URI:

BroadWorks Shared Call Appearance: Disabled

BroadWorks Feature Event Package: Disabled

UaCSTA: Disabled

Forwarding Unconditional Number: Disabled

Forwarding No Answer Number: Disabled 90 s

Forwarding on Busy Number: Disabled

Reject anonymous calls: Disabled

Save Cancel

## 8. Verification Steps

The following steps can be taken to ensure that connections between Fijowave DECT handsets and Session Manager and Communication Manager are up.

### 8.1. Session Manager Registration

Log into System Manager as done previously in **Section 6**, select **Elements** → **Session Manager** → **Dashboard**.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The 'Elements' menu is open, showing a list of system components: Avaya Breeze®, Communication Manager, Communication Server 1000, Device Adapter, Device Services, IP Office, Media Server, Meeting Exchange, Messaging, Presence, Routing, Session Manager, and Web Gateway. The 'Session Manager' option is highlighted. Below the menu, the 'Session Manager' dashboard is visible, featuring a 'Disk Space Utilization' bar chart, an 'Alarms' pie chart, and an 'Information' table. The 'Information' table lists elements and their sync status:

Elements	Count	Sync Status
Avaya Breeze	3	Green
CM	1	Green
Session Manager	1	Green
Manager	1	Green
Notifications	8	Green

Under **System Status** in the left window, select **User Registrations** to display all the SIP users that are currently registered with Session Manager.

The screenshot shows the Session Manager interface. On the left is a dark sidebar with a menu. The 'System Status' item is expanded, and 'User Registrations' is highlighted with a red rectangle. The main content area is titled 'System Status' and contains a table of sub-pages.

System Status	
Sub Pages	
Action	Description
<a href="#">SIP Entity Monitoring</a>	View Session Manager SIP Entity Link monitoring status.
<a href="#">Managed Bandwidth Usage</a>	Displays system-wide bandwidth usage information for locations where usage is managed. The details expansion shows the breakdown of usage among Session Manager Instances.
<a href="#">Security Module Status</a>	View Security Module status and perform actions on Security Modules for Core and Branch Session Manager instances.
<a href="#">SIP Firewall Status</a>	View SIP Firewall rule execution status from Security Modules
<a href="#">Registration Summary</a>	View per-Session Manager registration status and send notifications to AST devices.
<a href="#">User Registrations</a>	View detailed user registration status and send notifications to AST devices.
<a href="#">Session Counts</a>	View per-Session Manager and system wide session counts.
<a href="#">User Data Storage</a>	View status, backup and restore Session Manager User Data Storage

The Fijowave DECT users should show as being registered as shown below.

User Registrations											
Select rows to send notifications to devices. Click on Details column for complete registration status.											
<div> <div>View</div> <div>Default</div> <div>Export</div> <div>Force Unregister</div> <div>AST Device Notifications:</div> <div>Reboot</div> <div>Reload</div> <div>Fallback</div> <div>As of 1:51 PM</div> <div>Advanced Search</div> </div>											
<div> <div>19 Items</div> <div>Show 15</div> <div>Filter: Enable</div> </div>											
<input type="checkbox"/>	Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Reg Pri
<input type="checkbox"/>	Show	3193@greaneyp.sil6.avaya.com	FijowaveDECT	3193	DevConnectGalway	10.10.40.120	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3192@greaneyp.sil6.avaya.com	FijowaveDECT	3192	DevConnectGalway	10.10.40.120	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3191@greaneyp.sil6.avaya.com	FijowaveDECT	3191	DevConnectGalway	10.10.40.120	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3112@greaneyp.sil6.avaya.com	AAfD - two	SIP	DevConnectGalway	10.10.40.159	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3110@greaneyp.sil6.avaya.com	Workplace	Windows	DevConnectGalway	10.10.40.242	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	3101@greaneyp.sil6.avaya.com	Agent One	Workspaces	DevConnectGalway	10.10.40.187	fixed	<input type="checkbox"/>	1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Show	---	AAfD - one	SIP	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	Vantage01	K175	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	EliteSIPCC	SIP Phone	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>

## 8.2. Fijowave DECT Registration

To verify that Fijowave DECT Handsets are registered to the Fijowave Base Station correctly, log in as per **Section 7** and click on **Extensions** in the left column (not shown). The **State** column shows that all three DECT extensions are registered. Note that extension **3193** is shown twice below as there was a headset paired with this DECT handset extension.

Fijowave Business DECT 240

Extensions

AC: 0000

Save

Cancel

[Add extension](#)  
[Stop Registration](#)

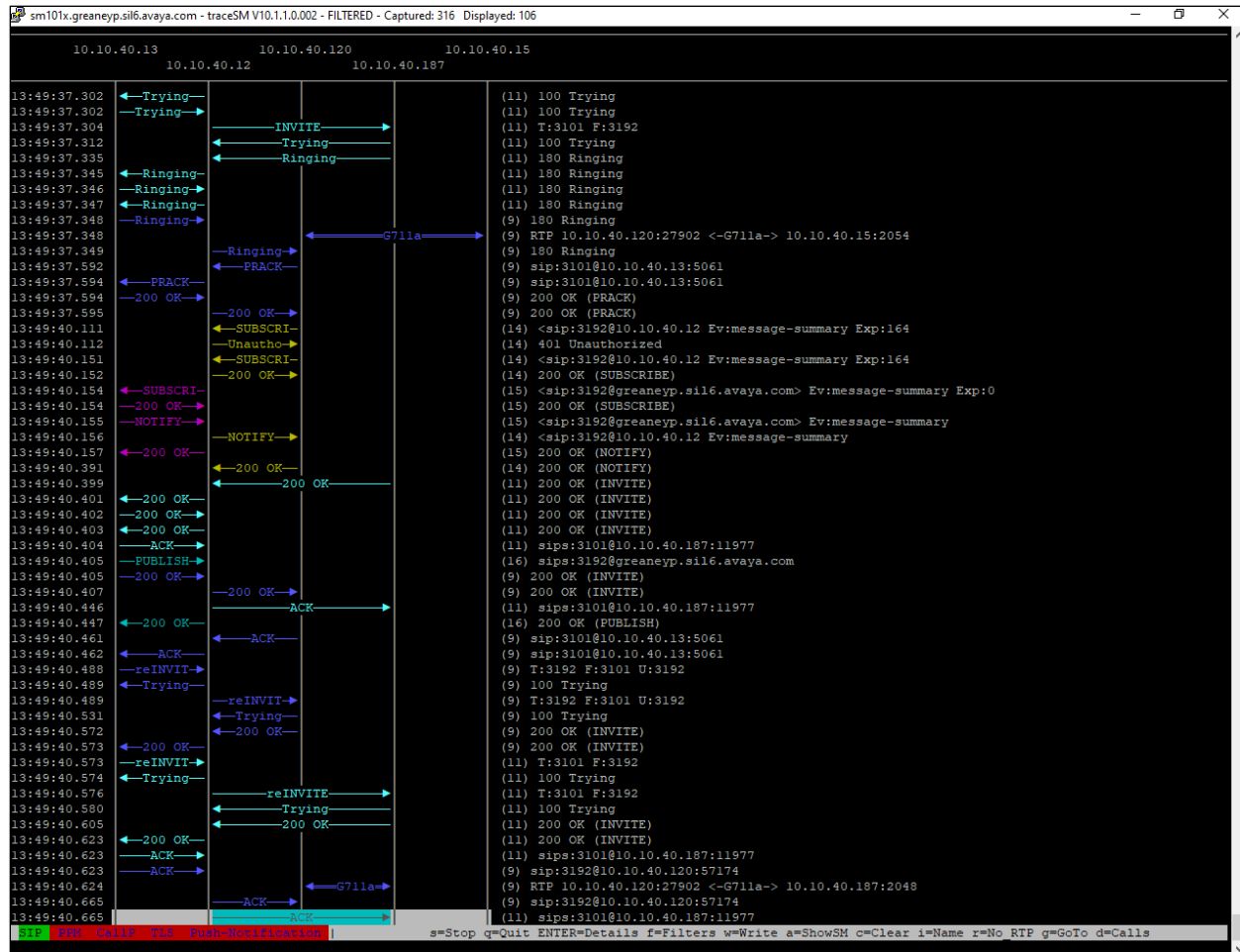
Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress	VoIP Idx	Extension	Display Name	Server	Server Alias	State		
<input type="checkbox"/>	1	0328DEF6EC	Present@RPN04	310 700.100	Off	<input type="checkbox"/>	1	<a href="#">3191</a>	3191	10.10.40.12	Aura10	SIP Registered@RPN04
<input type="checkbox"/>	2	0328D37E35	Present@RPN04	318 700.100	Off	<input type="checkbox"/>	2	<a href="#">3192</a>	3192	10.10.40.12	Aura10	SIP Registered@RPN04
<input type="checkbox"/>	3	0298DC381E	Present@RPN04	315 700.100	Off	<input type="checkbox"/>	3	<a href="#">3193</a>	3193	10.10.40.12	Aura10	SIP Registered@RPN04
<input type="checkbox"/>	4	02E6900F64	Present@RPN04	330 700.100	Off	<input type="checkbox"/>	3	<a href="#">3193</a>	3193	10.10.40.12	Aura10	SIP Registered@RPN04

[Check All /](#)  
[Uncheck All](#)

[Check All Extensions /](#)  
[Uncheck All Extensions](#)

With selected: [Delete Handset\(s\)](#) [Register Handset\(s\)](#) [Deregister Handset\(s\)](#) [Start SIP Registration\(s\)](#) [SIP Delete Extension\(s\)](#)

To troubleshoot any SIP calls “traceSM” on Session Manager can help. Using a tool such as PuTTY, open a connection to the Session Managers management IP address and run **traceSM**. This opens the window like the example below and the SIP messages can be scrutinised should an issue arise.



## 9. Conclusion

These Application Notes describe the configuration steps required for Fijowave's Business DECT to successfully interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Session Manager R10.1 by registering the Fijowave handsets with Session Manager as third-party SIP phones. Please refer to **Section 2.2** for test results and observations.

## 10. Additional References

This section references the product documentation relevant to these Application Notes. Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1 Issue 6 June 2023
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1 Issue 9 May 2023
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1 Issue 6 May 2023

Documentation for the Fijowave Business DECT product can be obtained as follows:

- Web: <http://www.fijowave.com>
- Email: [sales@fijowave.com](mailto:sales@fijowave.com)
- Help desk: +353 1 525 3072



# Appendix

## Signaling Group

display signaling-group 11	Page 1 of 3
SIGNALING GROUP	
Group Number: 11	Group Type: sip
IMS Enabled? n	Transport Method: tls
Q-SIP? n	
IP Video? n	Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y	Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y	Clustered? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n	
Alert Incoming SIP Crisis Calls? n	
Near-end Node Name: procr	Far-end Node Name: sm101x
Near-end Listen Port: 5061	Far-end Listen Port: 5061
	Far-end Network Region: 1
Far-end Domain: greanep.sil6.avaya.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

## Trunk Group Page 1

display trunk-group 11	Page 1 of 5
TRUNK GROUP	
Group Number: 11	Group Type: sip
Group Name: SIP PHONES	CDR Reports: y
Direction: two-way	COR: 1
Dial Access? n	TN: 1
Queue Length: 0	TAC: *811
Service Type: tie	Night Service:
	Auth Code? n
	Member Assignment Method: auto
	Signaling Group: 11
	Number of Members: 10

## Page 2

```
display trunk-group 11                                     Page 2 of 5
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                         Redirect On OPTIM Failure: 5000

  SCCAN? n                                         Digital Loss Group: 18
    Preferred Minimum Session Refresh Interval(sec): 600

Disconnect Supervision - In? y Out? y

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

Caller ID for Service Link Call to H.323 1xC: station-extension
```

## Page 3

```
display trunk-group 11                                     Page 3 of 5
TRUNK FEATURES

  ACA Assignment? n          Measured: none          Maintenance Tests? y

Suppress # Outpulsing? n    Numbering Format: private
                               UII Treatment: shared
                               Maximum Size of UII Contents: 128
                               Replace Restricted Numbers? n
                               Replace Unavailable Numbers? n

                               Modify Tandem Calling Number: no

  Send UCID? y

Show ANSWERED BY on Display? y

DSN Term? n
```

## Page 4

```
display trunk-group 11                                     Page 4 of 5
                                     SHARED UI FEATURE PRIORITIES
                                     ASAI: 1
                                     Universal Call ID (UCID): 2
MULTI SITE ROUTING (MSR)
                                     In-VDN Time: 3
                                     VDN Name: 4
                                     Collected Digits: 5
                                     Other LAI Information: 6
                                     Held Call UCID: 7
                                     ECD UII: 8
```

## Page 5

```
display trunk-group 11                                     Page 5 of 5
                                     PROTOCOL VARIATIONS
                                     Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                                     Send Transferring Party Information? y
                                     Network Call Redirection? y
Build Refer-To URI of REFER From Contact For NCR? 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
Resend Display UPDATE Once on Receipt of 481 Response? n
                                     Identity for Calling Party Display: From
Block Sending Calling Party Location in INVITE? n
                                     Accept Redirect to Blank User Destination? n
Enable Q-SIP? n
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                     Request URI Contents: may-have-extra-digits
```

---

**©2023 Avaya LLC All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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](mailto:devconnect@avaya.com).