

Avaya Solution & Interoperability Test Lab

Application Notes for configuring Funktel DPx SIP Trunk Solution with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Funktel DPx to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Readers should pay particular attention to the scope of testing as outlined in Section 2.1, as well as 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 Funktel DPx to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager. Funktel DPx is configured to connect to Session Manager via a SIP Trunk and hosts the Funktel f.airnet IP DECT Handsets. Calls are made to and from the f.airnet DECT handsets over the SIP Trunk.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of Funktel DPx to send and receive calls using the f.airnet DECT handsets. Calls to and from Avaya H.323 and SIP deskphones were made during the testing.

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 deskphones, Avaya H.323 deskphones, Funktel f.airnet DECT endpoints and PSTN endpoints.

- Basic Calls
- Hold and Retrieve
- Attended and Blind Transfer
- Call Forwarding Unconditional, No Reply and Busy (Controlled on DPx)
- Call Waiting
- Call Park/Pickup
- Conference
- Calling Line Name/Identification
- Codec Support
- DTMF Support

2.2. Test Results

All tests carried out passed successfully.

2.3. Support

Support from Avaya is available by visiting the website <u>http://support.avaya.com</u> and a list of product documentation can be found in **Section 11** of these Application Notes.

Technical support from Funktel can be obtained through the following: Marcel Schwiebert Phone: +49 5341 223 5313 E-mail: marcel.schwiebert@funktel.com Web : www.funktel.com

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Funktel f.airnet DECT handsets connect to the Funktel f.airnet DECT base station and registered to the Funktel DPx which is placed on the LAN. The DPx connect directly with Session Manager as a SIP Trunk in order to be able to make/receive calls to and from the Avaya H.323 deskphones on Communication Manager and SIP deskphones registered with Session Manager.



Figure 1: Network Solution of Funktel DPx hosting Funktel f.airnet DECT Handsets with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version		
Avaya Aura® Communication Manager running on Virtual Server	R7.0.1.2 R017x.00.0.441.0 Version 7.0.1.2.0.441.23523 Patch: Kernel-2.6.32.3.1.e16.AV4 PLAT-rhel6.5-0050		
Avaya Aura® Session Manager running on Virtual Server	7.0.1.2.701230		
Avaya Aura® System Manager	7.0.1.2 Build No: 7.0.0.0.16266 Software Update Revision No: 7.0.1.2.086007 Service Pack 2		
Avaya G430 Gateway	37.41.0 /1		
Avaya 9611G/9641G H323 Deskphones	6.6229		
Avaya 9641G SIP Deskphone Avaya 9611G SIP Deskphone	7.0.1.1		
Funktel Equipment	Software / Firmware Version		
FC4 Handset	3.2.x		
D11 light grey	3.2.x		
FC11 (blue)	3.2.x		
FB4 IP TP	V5.1.x		
BSIP1 ikon IP DECT Basisst.	V5.1.x		
DC 200 DoIP-Controller	5.1.x		
DPx	5.30a		

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing. For further information on the configuration of Communication Manager please see **Section 11** of these Application Notes.

- Customer Options.
- Sip Trunk.
- Network Region.
- IP Codec.

5.1. Check SIP Trunk License

Use the **display system-parameters customer-options** command to check the SIP Trunk licensing. Go to page 2 and make sure that there are sufficient numbers for **Maximum Administered SIP Trunks**.

		- 01 10
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks: 4000	22	
Maximum Concurrently Registered IP Stations: 2400	4	
Maximum Administered Remote Office Trunks: 4000	0	
Maximum Concurrently Registered Remote Office Stations: 2400	0	
Maximum Concurrently Registered IP eCons: 68	0	
Max Concur Registered Unauthenticated H.323 Stations: 100	0	
Maximum Video Capable Stations: 2400	3	
Maximum Video Capable IP Softphones: 2400	5	
Maximum Administered SIP Trunks: 4000	1290	
Maximum Administered Ad-hoc Video Conferencing Ports: 4000	0	
Maximum Number of DS1 Boards with Echo Cancellation: 80	0	

5.2. Configure a SIP Trunk

To allow calls to be made between Communication Manager and the Funktel DPx a SIP Trunk must be administered. Use change node-names ip to add the Session Manager. In this example the Session Manager is called **SM1677**.

```
        change node-names ip
        Page
        1 of
        2

        IP NODE NAMES

        Name
        IP Address

        AMS1616
        10.10.16.16

        CMS1640
        10.10.16.40

        SM1677
        10.10.16.77
```

Use the **add signaling group x** command where x is an unused trunk group number from 1-999. Set the **Group Type** to **sip**, set the **Near-end Node Name** to a Communication Manager Clan entry or as below using the **procr**. The **Near-end Listen Port** is automatically set to **5060**. Set the **Far-end Node Name** to the entry added to node-names ip and set the **Far-end Listen Port** to **5060**. Set the **Far-end Network Region** to **1**

```
add signaling-group 20
                                                                       1 of
                                                                              2
                                                                Page
                                SIGNALING GROUP
Group Number: 20
                             Group Type: sip
 IMS Enabled? n
                       Transport Method: tcp
       Q-SIP? n
    IP Video? n
                                                   Enforce SIPS URI for SRTP? y
 Peer Detection Enabled? y Peer Server: Others
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y
Alert Incoming SIP Crisis Calls? n
  Near-end Node Name: procr
                                             Far-end Node Name: SM1677
Near-end Listen Port: 5060
                                           Far-end Listen Port: 5060
                                        Far-end Network Region: 1
Far-end Domain:
                                             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
```

Use **add trunk-group x** where x is a valid Trunk group number. In this test the same number was used for trunk and signaling group. On **Page 1** set the **Group Type** as **sip** and give it a descriptive **Group Name**. Set a valid **TAC** and set the **Service Type** as **tie**. Set the **Member Assignment Method** as **auto**, set the **Signaling Group** as administered above and set the **Number of Members** to the number required (max 255)

add trunk-group 2	0 TRUNH	GROUP	Page 1 of 22	
Group Number: 20 Group Name: SM1	G1	coup Type: sip COR: 1	CDR Reports: y TN: 1 TAC: 720	
Direction: two Dial Access? n Queue Length: O	-way Outgoing	g Display? n Night	Service:	
Service Type: tie		uth Code? n Member As Nu	signment Method: auto Signaling Group: 20 mber of Members: 255	

On Page 3 set the **Numbering Format** as **private** so that calls sent over this trunk will not be proceeded by a +.

add trunk-group 20 TRUNK FEATURES	Page 3 of 22
ACA Assignment? n	Measured: none Maintenance Tests? y
Suppress # Outpulsing? n Numb	Dering Format: private UUI Treatment: shared Maximum Size of UUI Contents: 128 Replace Restricted Numbers? n Replace Unavailable Numbers? n
M Send UCID? n	Hold/Unhold Notifications? y Nodify Tandem Calling Number: no

Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager, in the example below **devconnect.local** is used.

```
change ip-network-region 1
                                                           Page
                                                                  1 of
                                                                       20
                              IP NETWORK REGION
 Region: 1
Location: 1
                Authoritative Domain: devconnect.local
   Name: default NR
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? y
  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
```

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the Funktel f.airnet 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:
```

6. Configure Avaya Aura® Session Manager

The Funktel DPx is added to Session Manager as a SIP Entity and an Entity Link, Routing Policy and Dial Pattern is added to route calls to the f.airnet DECT Handsets. In order make changes in Session Manager a web session to System Manager is opened. Navigate to http://<System Manager IP Address>/SMGR, enter the appropriate credentials and click on **Log On** as shown below.

Aura [®] System Manager 7.0	
Recommended access to System Manager is via FQDN.	
Go to central login for Single Sign-On	User ID: admin
If IP address access is your only option, then note that authentication will fail in the following cases:	Password:
 First time login with "admin" account Expired/Reset passwords 	Log On Cancel
Use the "Change Password" hyperlink on this page to change the password manually, and then login.	Change Password
Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.	O Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.
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.	

6.1. Configuration of a Domain

Click on **Routing** highlighted below.

AVAVA Aura [®] System Manager 7.0		Last Logged on at November 2, 2015 4:37 GO
🍇 Users	Communication Manager	Q, Services
Directory Synchronization	Communication Server 1000	Bulk Import and Export
Groups & Roles	Conferencing	Configurations
User Management	Engagement Development Platform	Events
User Provisioning Rule	IP Office	Geographic Redundancy
	Media Server	Inventory
	Meeting Exchange	Licenses
	Messaging	Replication
	Presence	Reports
	Routing	Scheduler
	Session Manager	Security
	Work Assignment	Shutdown
		Solution Deployment Manager
		Tempt Management
		- court rungement

Click on **Domains** in the left window. If there is not a domain already configured click on **New**. In the example below there exists a domain called devconnect.local which has been already configured.

AVAVA				
Aura [®] System Manager 7.0				
Home Routing X				
• Routing	Home / Elements / Routing / Domains			
Domains	Domain Management			
Locations				
Adaptations	New Edit Delete Duplicate More Actions			
SIP Entities	1 Itam 3			
Entity Links		Type	Notor	
Time Ranges	devconnect.local	sip	Default domain for Paul	
Routing Policies	Select : All, None			
Dial Patterns	<u></u>			
Regular				
Expressions				
Defaults				

Clicking on the domain name above will open the following window; this is simply to show an example of such a domain. When entering a new domain the following should be entered, once the domain name is entered click on **Commit** to save this.

AVAVA			
Aura [®] System Manager 7.0			
Home Routing X			
▼ Routing	Home / Elements / Routing / Domains		
Domains	Domain Management		
Locations	Domain Management		Commit Cancer
Adaptations			
SIP Entities	1 Item 🙃		
Entity Links	Name	Type	Notes
Time Ranges	* devconnect.local	sip 🗸	Default domain for Paul
Routing Policies			
Dial Patterns			
Regular			
Expressions			Commit Cancel
Defaults			

6.2. Configuration of a Location

Click on **Locations** in the left window and if there is no Location already configured then click on New, however in the screen below a location called **Devconnect** is already setup and configured and clicking into this will show its contents.

AVAVA Aura [®] System Manager 7.0		
Home Routing ×		
Routing	Home / Elements / Routing / Locations	
Domains	Leastion	
Locations		
Adaptations	New Edit Delete Duplicate More Actions	
SIP Entities		
Entity Links	2 Items I ಿ	
Time Ranges	Name	Correlation
Routing Policies	Devconnect	

The Location below shows a suitable **Name** with a **Location Pattern** of **10.10.16.0**. Once this is configured click on **Commit**.

	stem Manager 7.0					Last Logged on at January 24, 2017 3:01 PM Go
Home	Session Manag	er × Routing ×				
- Rou	ting	Home / Elements / Routing / Location	5			0
D	omains					Help ?
Le	ocations	Location Details			Commit Cancel	
A	daptations					
S	IP Entities	General			 	
E	ntity Links		* Name:	Devconnect	 	
Ti	me Ranges		Notes:			
		Location Pattern				
		Add Remove				
		2 Items 🛛 🍣				Filter: Enable
		IP Address Pattern			Notes	
		* 10.10.16.0				
		* 10.10.6.0				
		Select : All, None				
					Commit Cancel	

6.3. Configuration of the Funktel DPx as a SIP Entity

From the left hand menu select **SIP Entities** and click on **New.**

Home Routing X				
▼ Routing ◀	Home	/ Elements / Routing / SIP Entities		
Domains				
Locations	SIP	Entities		
Adaptations	New	Edit Delete Duplicate More Actions -		
SIP Entities				
Entity Links	24 It	ems 🛛 💝		
Time Ranges		Name	FQDN or IP Address	Туре
Routing Policies		AAEP1620	10.10.16.20	Voice Portal
Dial Dattaras		AMS1616	10.10.16.16	Media Server

Enter a descriptive **Name:**, The **IP address** of the Funktel DPx and Select **SIP Trunk** from the **Type:** drop down. Select the Location added in **Section 6.2**and Click on Commit to save the changes

Home Routing X	
▼ Routing	Home / Elements / Routing / SIP Entities
Domains	
Locations	SIP Entity Details
Adaptations	General
SIP Entities	* Name: Funktel
Entity Links	* FQDN or IP Address: 10.10.16.7
Time Ranges	Type: SIP Trunk 🔻
Routing Policies	Notes:
Dial Patterns	
Regular Expressions	Adaptation:
Defaults	Location: Devconnect v
	Time Zone: Europe/Dublin T
	* SIP Timer B/F (in seconds): 4
	Credential name:
	Securable:
	Call Detail Recording: egress 🔻
	Loop Detection
	Loop Detection Mode: On V
	Loop Count Threshold: 5
	Loop Detection Interval (in msec): 200

6.4. Configuration of the entity Link between Session Manager and the Funktel DPx

From the left hand menu select **Entity Links.** Click on **New.**

Home Routing ×										
▼ Routing 4	Routing Home / Elements / Routing / Entity Links									
Domains										
Locations	Entity Links									
Adaptations	New Edit Delete Duplicate More Actions -									
SIP Entities										
Entity Links	21 It	ems 🛛 🥲								
Time Ranges		Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Po	
Routing Policies		AAEP1620 EL	SM71676	тср	5060	AAEP1620		5060	trusted	
Dial Dattorne		AMS1616 EL	SM71676	TCP	5060	AMS1616		5060	trusted	

Enter a descriptive **Name**. Select the Session Manager entity connected to the Communication manager as **SIP Entity 1**. Select the SIP entity added in **Section 6.3** as **SIP Entity 2**. Set the protocol to **TCP** and the default port will update automatically.

SIP Entities	1 Itom - M						Filter: Enable
Entity Links	1 Item 🤯		_	1			Filter, Enable
Time Ranges	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port
Routing Policies		-					
Dial Patterns	* Funktel_EL	• Q SM71676	TCP V	* 5060	* Q Funktel		* 5060
Regular Expressions	Select : All, None						,
Defaults							
					Commit Cancel		

6.5. Configuration of the Routing Policy

Select **Routing Policies** from the left hand menu and click on **New**.

Home Routing X				
▼ Routing 4	Home / Elements / Routing / Routing Policies			
Domains	Deutin a Delisies			
Locations	Routing Policies			
Adaptations	New Edit Delete Duplicate More Actions -			
SIP Entities				
Entity Links	16 Items 🛛 🥲			
Time Ranges	Name	Disabled	Retries	Destination
Routing Policies	AAEP1620 RP		0	AAEP1620
Dial Patterns	AMS1616 RP		0	AMS1616

Home Routing *				
▼ Routing 4	Home / Elements / Routing / Routin	g Policies		
Domains		-		
Locations	Routing Policy Detail	S		Commit Cancel
Adaptations	General			
SIP Entities		* Name:	Funktel RP	
Entity Links		Disabled:		
Time Ranges		* Potrios:		
Routing Policies		Retries.	<u> </u>	
Dial Patterns		Notes:		
Regular Expressions	SIP Entity as Destination			
Defaults	Select			
	Name	FQDN or IP Address	;	

Enter a descriptive Name: and click on Select under SIP entity as Destination.

Select the **SIP Entity** added in **Section 6.3** and click on **Select**.

Home Routing ×						
▼ Routing 4	Home / Elements / Routing / Rou	uting Policies				
Domains						
Locations	SIP Entities		Select Cancel			
Adaptations						
SIP Entities	SIP Entities					
Entity Links	SIT Entities					
Time Ranges	24 Items 🛛 💝					
- Pouting Policies	Name	FQDN or IP Address	Туре			
	AAEP1620	10.10.16.20	Voice Portal			
Dial Patterns	AMS1616	10.10.16.16	Media Server			
Regular Expressions	Funktel	10.10.16.7	SIP Trunk			

Click on **Commit**.

Home Routing X			
▼ Routing 4	Home / Elements / Routing / Routin	g Policies	
Domains	Routing Policy Detail	s Commit	Cancel
Locations	Routing Folicy Detail		
Adaptations	General		
SIP Entities		* Name: Funktel_RP	
Entity Links		Disabled:	
Time Ranges			
Routing Policies			
Dial Patterns		Notes:	
Regular Expressions	SIP Entity as Destination		
Defaults	Select		
	Name	FQDN or IP Address	Туре
	Funktel	10.10.16.7	SIP Trunk

6.6. Configuration of a Dial Pattern to route calls to the Funktel DPx

From the left hand menu select **Dial Patterns** and click on **New**.

Home Routing X								
▼ Routing	Home	/ Elements / Routing /	Dial Patterns					
Domains								
Locations	Dia	l Patterns						
Adaptations	New	Edit Delete D	uplicate Mor	e Action	IS 🔻			
SIP Entities								
Entity Links	31 I	tems I 🍣						
Time Ranges		Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Dom
Routing Policies		0131827xxxx	11	11				-ALL-
Dial Patterns		01418230xxx	11	11				-ALL-
Describe Freedomics -		0141827xxxx	11	11				-ALL-
Regular Expressions		<u>091737xxx</u>	9	9				-ALL-
Defaults		<u>207xxxx</u>	7	7				-ALL-
		220xxxx	7	7				-ALL-

Enter the **Pattern:** that corresponds with the Extension numbers administered in **Section 7.4**. Enter the **Min** and **Max** digits for the extensions. Click on **Add** under **Originating Locations and Routing Policies**.

Home Routing ×					
▼ Routing 4	Home / Elements / Routing / Dial Pa	tterns			
Domains	Dial Dattaux Dataila			Com	with Company
Locations	Dial Pattern Details			Con	imit Cancel
Adaptations	General				
SIP Entities		* Pattern: 807	xxxx		
Entity Links		* Min: 7			
Time Ranges		· ····· ,			
Routing Policies		* Max: /			
Dial Patterns		Emergency Call: 📃			
Regular Expressions	E	mergency Priority: 1			
Defaults		Emergency Type:			
		SIP Domain: -AL	L- 🔻		
		Notes:			
	Originating Locations and I	Routing Policies			
	Add Remove				
	1 Item				
	Originating Location Name 🔺	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled

Select **Apply the Selected Routing Policies to All Originating Locations**. Select the Routing Policy administered in **Section 6.5**

Home Routing *			
▼ Routing ◀	Home / Elements / Routing / Dial Patterns		
Domains			
Locations	Originating Location		Select Cancel
Adaptations			
SIP Entities	Originating Location		
Entity Links	Apply The Selected Routing Policies to All Originating I	locations	
Time Ranges	Appry The Selected Routing Policies to All Originating I	Locations	
Routing Policies	5 Items 🖓		
Dial Patterns	Name		Note
Regular Expressions	CM63Loc		
Defaults	Devconnect		
	Select : All, None		
	Routing Policies		
	16 Items 🛛 🥲		
	Name	Disabled	Destination
	AAEP1620_RP		AAEP1620
	AMS1616_RP		AMS1616
	Funktel_RP		Funktel

Click on Commit.

Home Routing X						
▼ Routing ◀	Home / Elements / Routing / Dial Patterns					
Domains						
Locations	Dial Pattern Details			Com	mit Cancel	
Adaptations	General					
SIP Entities	* Pattern:	807xx	(XX			
Entity Links	* Min-	7				
Time Ranges		-				
Routing Policies	* Max:	/				
Dial Patterns	Emergency Call:					
Regular Expressions	Emergency Priority:	1				
Defaults	Emergency Type:					
	SIP Domain:	-ALL-	•			
	Notes:					
	Origination Leasting and Deutine Deliving					
	Originating Eccations and Routing Policies	•				
	Add Remove					
	1 Item 🧬					
	Originating Location Name Originating Location Notes	n I	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
	-ALL-		Funktel_RP	0		Funktel
	Select : All, None					

7. Configure DPx SIP Trunk

7.1. About the configuration software

The Java-based DPx Admin configuration software has the following system requirements:

- Windows-PC or Linux-PC
- Java Version 8 (tested with Oracle JRE)

The configuration screens are grouped in topics, for the sake of greater clarity. Each screen presents a clear list structure, which can be further enhanced with the aid of filters. "Tool tips" are built into the configuration screens... If you place the cursor on a term, a tool tip regarding this term is soon superimposed, which will facilitate configuration. All configured data sets can be deactivated individually on a temporary basis without the respective data set being lost.

7.2. Network

As standard, the first Ethernet interface NET 1 is configured with the IP address 192.168.0.253 and the network mask with 255.255.255.0. No DHCP server is configured on this interface. **DHCP-Server**

The second Ethernet interface NET 2, if available, serves as a DHCP server and makes numbers 172.20.153.x available in the IP network, with the network mask 255.255.255.0 Its own address is 172.20.153.1. Addresses 172.20.153.2 to 172.20.153.9 are not allocated via DHCP. Ensure that no other DHCP server is operating on the network. The operation of the two DHCP servers in the same network is not supported!

7.3. Exclusive Ethernet connection to a PC

This connection is required if you wish to configure the DPx, before integrating into the network. This is also the recommended method.

Use an Ethernet cable (CAT-5, crossed), to connect a PC to interface NET2 of the appliance. In order to be able to establish an exclusive Ethernet connection with the appliance, the PC must satisfy the following requirements.

- The TCP/IP protocol must be installed on the PC. Check the TCP/IP settings
- The network addresses of both systems must match each other. In doing so the following options are available:
- No change to the network settings of the appliance is required as the PC will acquire its IP address dynamically. This will be a fixed IP address in the 172.20.153.10–172.20.153.254 range and set the sub-network mask to 255.255.255.0
- The IP address of the DPx appliance is changed in the course of the basic configuration and have adapted the conditions according to the circumstances of the network. Set the same sub-network mask and a fixed IP address in the same address range on the PC. The IP addresses of both systems may only differ from each other in the final address block. 172.20.153.1 and PC: 172.20.153.20). Call up the DPx Admin Interface by means of your web browser and start the configuration.

Further information in this regard can be found in the chapter titled "Calling up the DPx as Administrator".

7.3.1. Calling up DPx as Administrator (DPx Admin)

Start your web browser (e.g. MS Internet Explorer, Firefox, Chrome or Safari) and enter the IP number of the system in the address line (see previous section). The DPx Admin program is downloaded from DPx and started.

The login screen appears:

Login		
	Username Password	Login

As the administrator, use an appropriate login and password.

The default password must be changed during the initial installation. Make a note of the new password and store it in a safe place. Should you forget the password, the system must be reset to the factory settings by the customer service department.

After clicking on **Login** access is granted to the DPx.

The main menu is always in the top blue bar. Pull-down sub-menus will be shown when clicking on the menu items.

		and the second s					
Settings	Numbers	Modules	Reports	System	Help	Languages	

7.3.2. Settings

Under Settings for the drop-down menu shows Administrators, Options, Network, Music on Hold, LDAP, Dial helper, Security, Licenses, Time Setting and Certificate sub menus.



7.3.2.1 Default

Defaul <u>t</u> Perr	missions ACD Monitor Queues Callgroups	
Active	1	
Data:		
Vame	Administrator	
Description	Administrator	
Jsername	admin	
assword		
assword		
mail		
tartmask	System info	~
Extension		
ctive	Select the checkbox, if this administrator is to b deactivating, login by means of the stored acces	e active. By ss data is not
ata:	possiole.	

Name	Enter a name for this administrator.
Description	Enter a description for this administrator if necessary.
Username	Enter the username for the login process.
Password	The password required for the login process.
Email	An e-mail address can be stored for the administrator.
Startmask	the start screen stored at this point appears after a successful login.
Extension	An extension can be allocated to the administrator. This is
	necessary if the administrator has SiMo (silent monitoring) rights
	for the ACD monitor, among others.

7.3.2.2 Network

Multiple configurations can be defined, of which only one can be active at any one time. Usually, only one configuration data set is required.

Filter off	~]			
Active	Name	Description	Country code	Area code	Number
	fairnet	Standardkonfiguration	49	69	90739886

By double-clicking the entry above the Standard entry screen is opened. By clicking on **New** an entry screens opens and new entries can be added as follows.

7.3.2.3 Standard

Data:			
Name	fairnet	Description	Standardkonfiguration
PBX:			
Country code	49	Area code	69
Number	90739886		
ENUM:			
ENUM		ENUM standby time	30
ENUM Fallthrough			
BMS contact cente	r:		
BMS IP		BMS port	80
BMS user		BMS password	[]
REST:			
REST session timeout	15		
Voicemailbox:			
Min length	1	 Max length 	180 🗸
Silence detection	0	 Charset 	UTF-8 🗸

Active	Mark the checkbox, if this setting is to be active.
Data:	
Name	Enter a name for this configuration in the field.
Description	Enter a description for this configuration if necessary.
PBX:	
Country code	Entry of the international country code (Germany = 49 , Austria = 43 , Switzerland = 41 etc.).
Area code	Entry of the area code without a zero prefix (example: $Kiel = 431$).
Number	The fixed line or connection number supplied by your telephone service provider.
ENUM:	-
ENUM	Mark the checkbox to switch on the ENUM functionality.
ENUM standby time	Here the time (in seconds) can be set.
ENUM Fallthrough	Mark the checkbox if in the case of a non-existent ENUM entry,
	the calls is to be made via the configured IP provider.
BMS Contact Centre:	
BMS IP	IP address of the DPx BMS Contact Centre application server.
BMS port	User port of the DPx BMS Contact Centre application server.

SJW; Reviewed: SPOC 6/14/2017

BMS user	The user name for the DPx BMS server. The BMS server must use this data to log in to the DPx IP DPx
BMS password REST:	The password for the DPx BMS server.
REST session timeout	The automatic session end of a connection by means of the REST API is set here. If an exchange of data no longer takes place via this connection, then the connection is disconnected automatically after the preset number of minutes.
Voice mailbox:	
Min length	Enter the minimum duration in seconds of a voice message here. The minimum duration must always be greater than the time required for the detection of silence.
Max length	Enter the maximum duration of a voice message here. The maximum duration must always be greater than the minimum duration.
Detection of silence	Here how many seconds the voice mailbox must recognise the end of a voice message is set. If, for example, nothing is said for the set period of time, then the recording is ended automatically. The time required for recognition of silence must always be less than the minimum duration.
Charset	Select the character set coding for e-mail notifications of the voice mailbox.

Note:ENUM stands for telephone number mapping and can be understood to be similar to the domain name system (DNS). A completely normal telephone number is entered into database at DENIC and can then be accessed by Internet via the IP protocol. This can only happen if the connection also controls IP telephony. Should this not be the case, then the DPx DPx will simply dial in the conventional way via the telephone network.

ENUM has the advantage that the subscriber does not have to remember various numbers. Nowadays, service providers offer a cross-over from IP telephony to the fixed line network. However, if a customer of one operator now wishes to call a subscriber of the other, then he/she must know the other's VoIP number. The interconnection of the networks does not help in this instance. Use ENUM here. You simply dial the known fixed-line number and the DPx looks up the desired route automatically. If the ENUM entry is positive, then a purely Internet-based connection is used; if the entry is negative, then dialling takes place via one of the configured VoIP providers.

7.3.2.4 Advanced

Phonebook:			
Telephone directoy resolution			
Default values:			
Language	English 🗸		
External call forwarding		CDR expiry	180 🗸
Login or logoff main ringer			
SIP:			
reinvite		IP external	[]
STUN		STUN server	
Call-Info		Call-Info IP	[]
P-Asserted-Identity	Caller Number > Called N 🗸		
T.38:			
Error correction	FEC 🗸	Max packet size	400 🗸
Telephone connection:			
Automatic exchange identifikation		Exchange identification code	0
E-mail:			
Email domain		Relay host	[]
Email address			
SMTP user		SMTP password	[]
TLS		Port	25

Phonebook:

Phone directory resolution Mark the checkbox, if a name entered in the phone book is to be shown in the telephone display.

Default values:

Language	Select the default language for voice messages. If, for example, another language has been selected for a voice mailbox, then the
External call forwarding	language that has been configured for the voice mailbox is used. Activate this function if every extension to be able to set the call forwarding function of any other extension. Call forwarding is set
CDR expiry	Set the number of days after which the CDR data is to be deleted automatically.
Recording storage period	Set the number of days after which the recordings are to be deleted automatically.
Login or logoff main ringer	When using secondary extensions, the main extension can be logged in or logged out by calling on its own extension number. Activate this option, if you wish to allow this function.

SJW; Reviewed:
SPOC 6/14/2017

SIP:	
Reinvite	Mark the checkbox, to allow this function.
Reinvite	By using this SIP option one can ensure that the RTP data of a VoIP call can be transferred directly between the terminals. This can reduce the data packet propagation times and free up the DPx One should be careful when using this option on networks that are operated behind a NAT gateway to the Internet and via which IP phone calls are also made
IP external	This IP address is used for all outgoing SIP connections. This is helpful if the DPx is operated behind a NAT gateway and, for example, calls are to be made via an SIP service provider This IP address is not used in IP sub-networks, for which the DPx has his own IP address.
STUN	Activate this function, if the DPx is operated behind a NAT gateway and a STUN server is to be used. The IP external function is thereby deactivated.
STUN Server	Enter the IP address or the host name of a STUN server.
Call-Info	Activate this function to activate the Call-Info header in SIP notifications. The DPx uses this, for example, to transfer an image to the terminal when a call is made.
Call-Info IP	As an option, the IP address of the image source that is to be used in the Call-Info header can be entered here. If no IP address is stored, then the IP address of network interface NET 1 is used. Normally, nothing needs to be entered here.
P-Asserted-Identify	In the case of calls to an extension, the P-Asserted-Identity header is transferred to the terminals in SIP. Here you can determine the content that is to be conveyed by this header. Most terminals are in a position to evaluate and further process this header.
T.38	
Error correction	Select between the various errors corrections for the T.38 protocol Standard: FEC Maximum packet size set the maximum permissible packet size. Standard: 400
Telephone connection	
Automatic exchange ID	Mark the checkbox, if an external dial-up line is to be assigned automatically (without the input of an exchange code). Internal connections must then begin with *
Exchange ID code	Configure an alternative exchange code here. Exchange codes may contain up to 3 digits. The 0 exchange code is always active.
E-mail	
Email domain	Domain name that is to be entered as the sender when sending voice messages.
Relay host	A relay host determines the default mail server to which the DPx sends e-mail. Here, the host must be entered with the full domain name (FQDN) or with the IP address.
SJW; Reviewed: SPOC 6/14/2017	Solution & Interoperability Test Lab Application Notes26 of 71©2017 Avaya Inc. All Rights Reserved.FtelDPx_CM7_SM7

	Take care that the name has been entered in the DNS server under
	Network options, is entered and that the DPx can resolve this as
	an IP address.
Email address	E-mail address that is to be used as the sender in the case of voice messages and system notifications.
SMTP user	Only to be filled in if the SMTP Server requires authentication.
SMTP password	Only to be filled in if the SMTP Server requires authentication.
TLS	Activate the TLS to set up a TLS-encrypted connection with the mail server.
Port	Enter the port number for the SMTP connections of the mail
	server. Port 25 is used as standard.

7.3.3. Network

Settings for configuration of the network interfaces and the DHCP server can be found in the menu below.

05	Jintenace	S Doog seconds				
-5	Filter off		*			
	Active	Name	IP	Netmask	DHCP NET 1	802.1q
	0	NET1	135.124.84.67	255.255.255.0	8	8
		NET2	10.10.16.7	255.255.255.0	8	8

Depending on the type of system, from 1 to 6 individual interfaces can be configured. In addition, there is the option of IEEE 802.1q-compliant VLAN tagging.

The network interfaces available in each case are listed. These are opened for editing by doubleclicking on the respective entry.

The list of network interfaces can be printed by clicking on **Print**.

7.3.3.1 Standard

Active				
802.1q				
Data:				
Name	NET2	Description	[
IP	10.10.16.7	Netmask	255.255.255.0	
DHCP:				
DHCP NET 1				
Start IP	172.20.153.10	End IP	172.20.153.200	
DNS 1	127.0.0.1	DNS 2		
		Gateway	172.20.153.253	
Domain				-

Active

802.1q

Mark the checkbox, if this network interface is to be active. Activate VLAN tagging here. A new tab marked 802.1q then appears, in which individual VLANs can configured. Network addresses can then only be configured in this tab. At least one VLAN ID must be present.

Data	
Name	Enter a name for this network interface in the field.
Description	Enter a description for this network interface if necessary.
IP	Enter the IP address for this network interface.
Netmask	The corresponding network screen for this network interface is configured here.
DHCP	
DHCP NET 1	A DHCP server can be activated on the network interface.
Start IP	The first IP address of the DHCP pool is configured here.
End IP	The last IP address of the DHCP pool is configured here.
DNS 12	The DNS server to which the DHCP clients are to be assigned must be entered here.
Domain	The domain name of the network interfaces is configured here.
Gateway	Enter the standard gateway to which the DHCP clients are to be assigned, here.
NTP 12	Enter the NTP server that is to be used by the clients, here.
Not all interfaces mus	the configured in the ages of the DDy up to 6 interfaces At least one

Not all interfaces must be configured In the case of the DPx, up to 6 interfaces. At least one interface must, however, show a valid configuration.

To save the information, click on **Save** on the lower bar. An instruction follows, that the system must be restarted.

SJW; Reviewed:	Solution & Interoperability Test Lab Application Notes	
SPOC 6/14/2017	©2017 Avaya Inc. All Rights Reserved.	FtelDP

7.3.3.2 Global settings

TETP				
Network:				
Hostname	fairnet	Domain	localdomain.com	
Gateway	135.124.84.1			
DNS 1 IP	127.0.0.1	DNS 2 IP		
NTP 1		NTP 2		
QoS-Setting	IS:			
SIP TOS	cs3 🗸	IAX TOS	cs3 🗸	
RTP TOS	ef 🗸 🗸	Video TOS	af41 🗸	
Video bitrate	384 🗸			
SNMP:				
SNMP		SNMP version	SNMPv2c 🗸	
SNMP user		SNMP password		

- ___

TFTP-Server

TFTP	Activate the integrated TFTP server of the DPx here. For example,
	firmware files for terminals can be made available by means of the
	TFTP server.
Network	
Hostname	Name of the DPx
Domain	Internet Domain, if available
Gateway	The gateway of the IP-network. The data traffic of the DPx is
	routed further via this gateway.
DSN 12 IP	IP addresses of 1. and 2. respectively Name server. Two
	independent DNS servers must always be entered.
NTP 12	IP address or host name of the time server (an alternative can be
	entered for NTP 2), from which the system must request the
	current time. The 127.0.0.1 setting refers to the internal clock of
	the system.
QoS settings	

Data traffic can be classified by the system into various service classes. A network that isconfigured for QoS, is thus in a position to priorities certain data ahead of other.SIP TOSFrom the list, select the class of the SIP signalling packets.IAX TOSFrom the list, select the class of the IAX signalling and voice data
packets.RTP TOSFrom the list, select the class of the RIP voice data packets.Video TOSFrom the list, select the class of video data.Video bitrateSelect the maximum video bitrate for a single video call. The
maximum bandwidth selectable is 2048 kbps.

SNMP	
SNMP	Activate the SNMP service if to integrate the DPx DPx in a network monitoring system.
SNMP version	Select the SNMP version to be supported.
SNMP user	The SNMP client must log in to the DPx with a user name or a community.
SNMP password	A password is required for SNMPv3.

A phone call cannot be connected without a correct network configuration. Check if the DNS and NTP servers that have been entered can be accessed and are functioning. Telephony is not possible via SIP service providers (ITSPs) without a functioning DNS. Kindly contact funktel support in the event of problems. If the IP address of the system has been changed, log in to the system under the new IP after a restart.

To save the information, click on **Save** on the lower bar. An instruction follows, that the system must be restarted.

7.4. Numbers

The numbering plan used can be administered under the Numbers menu.



7.4.1. Extensions

Extensions can be managed under **Extensions**.

the second	Nr	Name	e Given name	Description	Protocol	SIP transport	Voicemailbox	Conference room	UC licen
	8075200	200	D11		SIP	UDP	-		
	8075201	201	FC4		SIP	UDP			
	8075202	202	FC4		SIP	UDP	2	2 2	
0	8075203	203	D11		SIP	UDP			

The extensions that have already been set up are listed. These are opened for editing by means of a double-click on the respective entry.

Click on **New** to set up a new extension.

7.4.1.1 Standard

Given name	[D11]	Name	200	1
Nr	8075200	Description		
Data:				
E-mail		Language	German	~
Voicemailbox	· •	Voicemailbox authentification	Without login	~
Caller ID presentation		External number	[
Range	International 🗸	Internal ringtone	Bellcore-dr3	~
DTMF-mode	Auto 🗸	Protocol	SIP	~
Line nr				
Password:				
Password				
TAPI Password		- v		
SIP/IAX2 password	•••••	· •		

When the New extension screen is open the first tab is Standard

Active	Mark the checkbox, if this extension is to be active.
Given name	Enter the first names of the subscriber.
Name	Enter the surname of the subscriber.
Nr	Enter the internal number of the extension.
Description	Enter a description for this extension if necessary.
Data	
E-mail	Enter the E-mail address of the subscriber. The e-mail address is used for notification e-mails such as information regarding missed calls. The entry of the e-mail address still does not lead to automatic notification. In addition, this must be configured in the options of the extension
Language	Select the default language that is to be used by the DPx for this extension for notification texts. The language configured at this point can be overwritten by other configurations if required.
Voice mailbox	After clicking on the button, it is possible to create or edit a new mailbox. The selection list enables an existing voice mailbox to be assigned to this extension. All the existing voice mailboxes in the list are shown. In the same manner, a single mailbox can be assigned to multiple extensions.

Voicemailbox authentication This option sets the login parameters for the specific voice mailbox.

	• Without login: No check when accessing mailbox, if the request is made from this extension.
	• PIN only: Only the PIN is requested if the voice mailbox is
	accessed from this extension.
Caller IP presentation	Mark this checkbox if the number of the subscriber is to be displayed
External number	Enter the number that is to be transferred to the receiving device in
	the event of the number identification function being activated. The format must be national or international (e.g. 0049 431 123456 or 0431 123456).
Range	Specify the outbound call rights for this subscriber.
	• Internal: Subscriber may only call internally
	• Local: Subscriber may only call internally and in the local area code.
	• National: Subscriber may call in own country (country code).
	 International: Subscriber has no restrictions and may call worldwide.
Internal ringtone	Select a ringtone by which internal calls will be signaled (support by terminal required).
DTMF-mode	Select from the list the manner in which DTMF tones are to be relayed in SIP. If you select "Inband" then G.711 must be selected as the audio codec, as otherwise DTMF will not be possible. The
	standard setting is Auto.
Protocol	Extension can be external numbers, SIP or IAX2 terminals or a Fax2Mail service. If "External" is selected, then fixed-line numbers can be stored under Extension Number These must in turn be in national or international format. The external number is routed according to the routing configuration.
Line nr	Input field for the number when "External" is set in the Protocol field (see above). For further information, see INFO at the end of this section.
Passwords	
Password	The password is a freely selectable character string (at least 6 and a maximum of 24 characters), by which access to the DPx user web interface is secured. If it is also used for the unblocking of the telephone, only digits are permissible.
TAPI Password	The TAPI password is a freely-definable string that contains at least 6 and a maximum of 24 characters. It is used to connect a TAPI client to the DPx. The TAPI interface can only be accessed if a valid TAPI connector license is available.
SIP/IAX2 Password	The SIP password is the password that is used by the terminal to log in to the DPx. This password is used for authorization in the web interface or in the configuration of the terminal.
SJW; Reviewed: SPOC 6/14/2017	Solution & Interoperability Test Lab Application Notes34 of 71©2017 Avaya Inc. All Rights Reserved.FtelDPx_CM7_SM7

Protocol	If Fax2Mail is selected as the protocol, it is possible to receive faxes on this extension number and to relay them by e-mail. The faxes are sent to the e-mail addresses stored in the E-mail field as a PDF attachment. Multiple numbers can be set up with the Fax2Mail function. A maximum of two faxes can be received simultaneously. The receipt of faxes is only possible via the T.38 or with the aid of the G.711 audio codec. Other codecs do not support receiving.
Extension No.	The default value is "no entry" and should always be left blank during setup. This option makes it possible to influence the connection channel. If, for example, an SIP user is set up with the number 1234, then the connection channel is SIP/1234. If the string 9876 is entered under the connection number, then its connection channel is SIP/9876. If a string is entered under the connection number, it is no longer possible for an SIP terminal to register on this account. This enables one, amongst other things, to define two numbers (virtual extensions) that use the same terminal (connection channel). It does, however, seize the call forwarding setting of the number called in each case, even though the same terminal is used. In addition it is possible to define users, in which - for example - the protocol is set to external and any external number (without exchange code) is entered as the connection number. The call forwarding settings also come into action in this case. If the external subscriber is engaged, then the call can be diverted accordingly. This subscriber can also be a member of a team. If the Fax2Mail function is selected under Protocol, no entry may be made in the port number field.

7.4.1.2 **Options**

Click on the **Options** tab.

Options:			
Extension behind NAT Gateway		Phone lock	
Call number on forwarding		BLF	
Secondary ringer	1	Wartefeldagent	Main 🗸
UC license	-	•	
Busy on busy		Phonebook	
Transfer with #		Activate email	
Login main ringer	1		
Conference room	-	•	
Qualify	on	•	
Call-limit	3	•	
SIP Transport	UDP	•	
Codecs:			
1. Codec	G.711a 🔹	2. Codec	G.711u 🗸
3. Codec	G.726	4. Codec	GSM 🗸

Options

Ext. behind NAT Gateway	Mark the checkbox, to switch on synchronous RTP. This is useful and necessary in the case of many terminals that are connected
	behind a NAT gateway. By default this value is "off" and should only be activated in special cases (firewall without SIP inspection).
Phone lock	If the phone lock is activated, only emergency calls can be made.
	The phone lock can be disabled on the telephone by dialing a code and entering the PIN.
Call number on forwarding	When a permanent ACD is activated, the own number is signaled instead of that of the original caller.
BLF	If the checkbox is selected, it is possible (in the case of suitable terminals) to signal the current status of the terminal on a busy lamp field. If required, this function must also be activated for specific TAPI functions and when the terminal is used for the BMS
	Contact Centre.

Secondary ringer	If the checkbox is selected, it is possible to register up to two additional SIP terminals with specific accounts for this number. These can be reached at the same number. The additional automatic SIP usernames have the syntax za <extension number=""> and zb<extension all<br="" for="" is="" number.="" password="" same="" the="">accounts.</extension></extension>
Wartefeldagent	Specify which terminal is to be used in the waiting fields. Only SIP and DPx UC terminals are permissible.
UC license	Assign a DPx UC license to the extension, if this DPx UC is to be used.
Busy on Busy	If the checkbox is selected, the callers receive the busy tone when subscribers are busy. This function is helpful when the secondary extension is used simultaneously. It is not supported for external extensions.
Phonebook	If this checkbox is marked, then this extension is listed in the internal phone book - for example in the DPx User book or in the DPx phone book for SIP terminals.
Transfer with #	During a call the option exists of transferring the call by pressing the \Box key and then dialing the destination number.
Activate email	Notifications regarding missed calls are sent to the e-mail address stored in the E-mail Address field if this checkbox is marked.
Login main ringer	The main extension can, as an option, be deactivated when the secondary extension is activated. Activation and deactivation is also possible by calling the primary extension on the on the extension's own number.
Conference room	This extension can be assigned to a personal conference room. The subscriber can then manage this conference room in DPx User and DPx Live Conference.
Qualify	If this feature is switched on, a regular check of the connection runtime to the server takes place every 90sec. (Keep alive). If a terminal can no longer be reached, no further calls are assigned to this device automatically, so that there is no time consuming wait for an answer from the device when a call is put through. Activate this feature, if DPx is operated behind a NAT firewall. Not all terminals are able to process these notifications correctly, meaning that this function may have to be deactivated.
Call-limit	By means of this setting it can be determined how many simultaneous conversations may be conducted via this extension. If one call is selected, it is no longer possible to transfer calls.
SIP Transport	The DPx supports UDP, TCP as well as TLS as protocol for SIP. UDP is selected as the default. The activation of TLS also activates the encryption of audio data by means of SRTP.

Solution & Interoperability Test Lab Application Notes ©2017 Avaya Inc. All Rights Reserved. Codecs

1....4. Codec

Select the codec to be used for voice coding. The pre-set corresponds to the current setting.

DPx supports the G.711a, G.711u, G.722, G.726, GSM and Opus codecs for the extensions. Additionally, the H.261, H.263, H.263p, H.264 and VP8 video codecs can be used. Transcoding does not take place between various video codecs

7.4.1.3 Call forwarding

Call forwarding is the final tab for a new extension.

Range	International	~	
Unconditional	8230001		
No answer	8230001	Timeout	10
Busy			
Auto		IP	
On external cal	ls:		
Range	International	~	
Unconditional	8230001		
No answer	8230001	Timeout	10
Busy			
Automatic		IP	
Automatic			<u>.</u>

In the event of internal calls / In the event of external calls

Range	Specify what rights the extensions should have to set up call forwarding (internal, local, national, international).
Unconditional	Activate the checkbox and enter a number if to set up a permanent call forwarding setting. If a permanent call forwarding set is
	activated, then call forwarding no longer functions in the event of no answer and busy.
No answer	Activate the checkbox and enter a number if to set up a permanent call forwarding setting in the event of No answer .
Timeout	Enter the time (in seconds), after which automatic call forwarding takes place in the event of No answer .
Busy	Activate the checkbox and enter a number if to set up call forwarding When Busy .

SJW; Reviewed:	Solution & Interoperability Test Lab Application Notes	38 of 71
SPOC 6/14/2017	©2017 Avaya Inc. All Rights Reserved.	FtelDPx_CM7_SM7

Auto	If the checkbox is marked, the system checks when a call is made to this extension whether a PC or other device is available at the specified IP address. If no device is detected, the call is diverted to the destination phone. This is of particular interest with regard to soft phones (e.g. in a call centre). Calls are only connected if the PC is ready to operate. In this way a check can also be made as to whether a workstation (phone) is in fact busy and it enables an automatic diversion to a defined number, if the workstation is
	switched off. This type of Automatic Call Forward has the highest
	priority and is evaluated aread of an others.
IP	Enter an IP-address for automatic Automatic Call Forward.

To save the information, click on **Save** on the lower bar.

7.4.2. Mappings

The allocation of numbers (mapping) is edited in this menu. In doing so, the external public numbers are assigned to the internal numbers.

	Edit n	nappings					
6	Filter off	~					
	Active	Name	Description	From Nr	To type	To Nr	Time control
	0	200		8075200	Extension	8075200	
		201		8075201	Extension	8075201	-
		202		8075202	Extension	8075202	14 I
		203		8075203	Extension	8075203	-
		Huntgroup 1		8075204	Team	8075204	-
	New	Delete Drint	1				
	<u>Id</u> em	Print	J				

The allocation that has been entered is listed. These are opened for editing by double-clicking on the respective entry.

A new entry can be created by clicking on New

The mapping tool is a convenient way and means of allocating telephone numbers. Inbound call (external) can be assigned to an internal number. A number can also be inbound at a SIP provider. By means of this function a number of a SIP provider can be assigned to an internal number. In this way, multiple SIP gateways can also be assigned directly to the respective subscribers. In addition to the subscribers, an entire team can be dialed.

Even when no mapping has been added, a series of specified mappings is listed. All subscribers who have already been set up in the user area, are assigned on a 1:1 basis automatically. A subscriber with extension 258 is assigned automatically by the system in such a way that an external call on the international number will also reach extension 258. This standard mapping facilitates setting up and can be changed at any time.

SJW; Reviewed:	Solution & Interoperability Test Lab Application Notes	39 of 71
SPOC 6/14/2017	©2017 Avaya Inc. All Rights Reserved.	FtelDPx_CM7_SM7

7.4.2.1 Standard

Standard Y Active Data: 200 Description Name 8075200 From Nr To type Extension ~ To Nr 8075200 Time control × Cancel Acc<u>e</u>pt Save

When a new Mapping is selected the **Standard** tab is shown.

Active	Mark the checkbox, if the entry is to be active.
Data	
Name	Enter a name for the entry, e.g. the location
Description	Enter a description if necessary.
From Nr	If required, enter a particular number, which is to be assigned to a particular destination. As rule, a number is stored here in the international format without the 00 prefix. Numbers can only be
	processed correctly in this format. The * symbol is permitted at the end of a From Nr and indicates that any digits may follow the preceding number.
To type	Select the type of destination (extension, conference room, mailbox)
To Nr	Enter the number of the destination. By clicking on the To-No., a selection list with possible destination number is opened. A destination can be assigned directly by a double-click within the selection list.
Time control	If time control is configured, it can be assigned to each mapping entry. Within time control, specific destinations can be assigned for various time frames. If an inbound call takes place outside of the defined time frame, the standard destination takes the call new destinations can be controlled centrally by time control.

To save the information, click on **Save** on the lower bar.

7.5. Modules

In this menu you will find the settings for Callrouting and terminal management as well as all settings for special functions of the DPx.



7.5.1. VoIP provider

The providers that have already been set up are listed. These are opened for editing by means of a double-click on the respective entry.

Active	Server	Name		comment	VolP provider nar
8	myServer	sipgeneric	Test		SIP/Generic
	10.10.16.77	Session Manager			SIP/Generic

New providers can be created by clicking on **New**.

SJW; Reviewed: SPOC 6/14/2017 Solution & Interoperability Test Lab Application Notes ©2017 Avaya Inc. All Rights Reserved.

7.5.1.1 Standard

Active				
VoIP provider name	SIP/Generic 🗸	Name	Session Manager	
Number	s	Comment	[
Provider data:				
Server	10.10.16.77	Port	5060	
Username	[]	Password		
Authentication		Usernation the passi	word of your SIP account.	
Registration		Allow registration		
SIP Call Limit	0			
Codecs:		Options:		
1. Codec	G.711a 🗸	Reinvite		
2. Codec	G.711u 🗸	Qualify	No	~
3. Codec	· •	SIP NAT	No	~
4. Codec	- •	SIP Transport	TCP	~
		DTMF mode	Rfc2833	~

Active	Mark the checkbox, if this provider is to be active.
VoIP provider name	Select an entry from the list.
Name	Give a unique name to this provider. This name, in conjunction with the prefix "prov" is also used for the optional authentication of the provider to the PBX.
Number	A number assigned by the provider is stored here. In most cases the standard entry s is correct.
Comment	Enter a comment for this entry if necessary.
Provider Data	
Server	Enter the address of the server or of the media gateway.
Port	Enter the port. For SIP providers or media gateways this is usually Port 5060. Port 50601 is usually used in the case of SIP TLS being used.
Username	User name for provider login
Password	Password for provider login
Authentication	Mark the checkbox, if to request authentication of the provider in the case of inbound calls.
Registration	Registers the respective user with the VoIP service provider. This is necessary for most service providers in order that inbound calls can be connected.
CIWA Descioned	Salution & Internanchility Tract Lab Application Nature 40 a571

SJW; Reviewed:	Solution & Interoperability Test Lab Application Notes	42 of 71
SPOC 6/14/2017	©2017 Avaya Inc. All Rights Reserved.	FtelDPx_CM7_SM7

SIP Call Limit	Specify how many simultaneous calls via this VoIP provider are to be allowed. The value 0 cancels a limit.
Username in "From"	This option places the user name in the From-header in SIP protocol instead of the number.
Allow registration	This option permits a terminal - for example, a media gateway - to be registered on the DPx.
Codecs	
Codecs 1 4.	Codec selection of the voice coding in use. The pre-set corresponds to the current setting.
Options	
Reinvite	The Reinvite option makes it possible to swap speech data (RTP) directly between the terminals. In this case, the DPx serves only as an SIP signaling gateway a compatible network infrastructure is required for this option. If required, contact a specialist dealer.
Qualify	If the checkbox is marked, a regular check of the connection runtime takes place.
SIP NAT	Select "Yes" if the system is used behind a firewall when connected to SIP providers.
SIP Transport	Select from UDP, TCP or TLS as a transfer method. The correct setting can be obtained from a VoIP provider or from the documentation of the media gateway. When TLS is selected, the encryption of audio data by means of SRTP is also activated.
DTMF mode	Select here whether DTFM signals are to be transferred.

7.5.1.2 Outbound

In this screen, the various SIP headers can be adapted to the respective VoIP service providers or the respective media gateway with the aid of POSIX-compliant, regular expressions.

Active	Priority Description	Header type	Search	Replace	Caller name
0	1	From	496990739886([0-9]*)	\$2	Name
٢	2	From	49([0-9]*)	0\$2	Name
0	3	From	.+	\$1	Name
0	1	P-Asserted-Identity	496990739886([0-9]*)	\$2	
0	2	P-Asserted-Identity	49([0-9]*)	0\$2	
٢	3	P-Asserted-Identity	.+	\$1	
0	1	P-Preffered-Identity	496990739886([0-9]*)	\$2	
0	2	P-Preffered-Identity	49([0-9]*)	0\$2	
0	3	P-Preffered-Identity	.+	\$1	
0	1	Privacy	0	id	
\bigcirc	1	То	069(\d)+	\$2	
0	2	То	496990739886([0-9]*)	\$2	
\bigcirc	3	To	49([0-9]*)	0\$2	
0	4 Polizeinotruf, Euro	То	49(11[025])	\$2	
\bigcirc	5 Harmonisierte Die	To	49(116[0-9]{3})	\$2	
0	6 Auskunftsdienste	To	49(118[0-9]{2})	\$2	
0	7 Standard	То	.+	\$1	

The outbound rules that have already been set up are listed. These are opened for editing by double-clicking on the respective entry.

Before changing the rules under the Outbound tab, the newly created VoIP service provider must be stored and re-opened. Depending on the selected profile, a standard set of rules then becomes available.

Click on **New** to set up a new rule. Complete the fields carefully.

Active	1				
Data:					
Header type	From	~	Priority	3	ĺ
Description	<u> </u>				
Search	.+]	Replace	\$1	ĺ
Caller name	Name	~			

Active Data	Mark the checkbox, if this rule is to be active.
Header type	Select the SIP-Header to be set.
Priority	In the event of there being multiple rules for the same header. The header can be prioritized.
Description	Enter a description for this entry if necessary.
Search	A search for the destination or source number can be made with the aid of regular expressions, depending on the selected header type.
Replace	The source number or the destination number can be modified for the selected header type.

Some examples for regular expressions.

.+	One or more of any characters
.*	No or any characters, as desired
{3}	precisely 3 characters of the prefixed expression
{2.4}	precisely 4 characters of the prefixed expression
$\setminus d$	Digits from 0 to 9
[0,-9]	Digits from 0 to 9
[a-z]	alphabetic characters from a to z
[0,4,7]	Digits 0, 4 and 7
\+	The + sign

7.5.1.3 Inbound

In this screen, the various SIP headers can be interpreted as destination or source numbers with the aid of POSIX-compliant, regular expressions.

Active	Priority	Description	Header type	Search	Replace	Caller name	Intern
0	1		From	([0-9]{4,})	49\$1	-	8
٢	3		From	.+	\$1	Name	٢
8	4		From	\+(\d+)	\$2	10 III	8
8	5		From	00(\d+)	\$2	-	8
8	6		From	0(\d+)	49\$2		8
8	7		From	[aA]nonymous	\$1	-	8
٢	7		From	.+	Anonymous	2	8
0	1		То	\+(\d+)	\$2	Nummer	8
0	2		То	00(\d+)	\$2	Nummer	8
٢	3		To	0(\d+)	49\$2	Nummer	8
0	4		То	\d+	\$1	Nummer	8
0	4		To	\d+	\$1	Nummer	(

The inbound rules that have already been set up are listed. These are opened for editing by double-clicking on the respective entry.

Before changing the rules under the Inbound tab, the newly created VoIP provider must be stored and re-opened. Depending on the selected profile, a standard set of rules then becomes available. Click on **New** to set up a new rule.

Defaul <u>t</u>				
Active				
Data:				
Header type	From	~	Priority	3
Description				
Search	.+		Replace	\$1
Caller name	Name	~	Intern	
Use mapping				
Cancel	Acc <u>ept</u>			

Active Data	Mark the checkbox, if this rule is to be active.
Header type	Select the SIP header to be analyzed.
Priority	In the event of there being multiple rules for the same header. The
-	header can be prioritized.
Description	Enter a description for this entry if necessary.
Search	A search for the destination or source number can be made with
	the aid of regular expressions, depending on the selected header
	type.
Replace	The source number or the destination number can be modified for
	the selected header type.
Caller name	Specify if the caller name is to be taken from the corresponding
	SIP header (Name), or replaced by the number of the caller
	(Number) or not placed at all.
Intern	If the DPx is operated as a sub-system it is then possible to mask
	inbound calls via this VoIP service provider as internal calls. These
	calls are then not made via the mapping but rather directly via the
	internal routing to the number dialed.

Likewise, calls masked as internal are not captured by time control. Masking only takes place if the stored expression in the search field matches the header for which the search is being made.

To save the information, click on **Save** on the lower bar.

7.5.2. VoIP provider group

You can manage the provider groups in this menu. The provider groups combine one or many VoIP providers into a single virtual VoIP service provider. The VoIP service provider groups form the basis for callrouting.



The providers that have already been set up are listed. These are opened for editing by means of a double-click on the respective entry.

New providers can be created by clicking on New.

7.5.2.1 Standard

Standard \	/oIP provider
Active	1
Data:	
Name	AvayaTest
Description	[
Cancel	Accent Save
Cancer	

Active	Mark the checkbox, if this provider is to be active.
Data	
Name	Give a unique name to this provider group. This name serves as a reference in call routing.
Description	Enter a description for this entry if necessary.

7.5.2.2 VoIP provider

Select	VolP provider name	Name
1	SIP/Generic	Session Manager

By marking the **Select** checkbox, select which VoIP providers should belong to the provider group.

To save the information, click on **Save** on the lower bar.

7.5.3. Callrouting

You can manage call routing in this menu. Call routing defines the path of an outgoing call.

 Active	Priority	Name	Description	Source number	Destination number	VoIP provider group	VolP provider group	VoIP provider group	Routing type
0	1	Default Routing	Default Routing	[0-9]*	[0-9]*	AvayaTest	-		External
0	1	Intern Avaya		[0-9]*	8[23][357]\d*	AvayaTest	-		Internal

The call routings that have already been set up are listed. These are opened for editing by doubleclicking on the respective entry.

A new call routing can be created by clicking on New.

7.5.3.1 Default

	Default			
	Active	1		
	Data:			
	Name	Intern Avaya	Description	
	Priority	1	Routing type	Internal 🗸
	From:			
	Source number	[[0-9]*		
	Emergency calls		Destination number	8[23][357]\d*
	IP address		Netmask	
	Start weekday	* •	End weekday	* •
	Start time	00:00	End time	23:59
	to:			
	VoIP provider group	AvayaTest 🗸		
	Source Number	(\$1)	Destination Number	(\$1)
	1. Fallback:			
	VoIP provider group	- •		
	Source Number	(\$1)	Destination Number	(\$1)
	2. Fallback:			
	VoIP provider group	- v		
	Source Number	(\$1)	Destination Number	(\$1)
	C <u>a</u> ncel Ad	cc <u>ept</u>		
ctive ata		Mark the checkbo	ox, if this routing	g rule is to be active.
ame		Give a unique nar	ne to this routin	ng rule.
escript	ion	Enter a descriptio	n for this entry	if necessary.
riority		Enter the priority	of this routing 1	rule. In the event that multiple
		rules satisfy the sa	ame conditions,	then the rule with the highest
outing	type	If the DPx is oper	the lowest prio	rity number, is selected.
outing	type	number or ranges	of numbers can	be directed to the primary D
		via an SIP trunk.	In this case the	routing type is to be set as
		Internal. The Exte	ernal setting mu	st be selected for normal rout
		to a media gatewa	ay or a VoIP pro	ovider.

From	
Source number	 The source of a routing is always an internal number of an extension. Groups of extensions can be summarized with the aid of regular printouts to POSIX. Example 1([0-9]*): All internal extensions, whose numbers begin with 1. Bracketing in round brackets is important, if one wishes to use this part of the number to change the number at a later stage.
Emergency calls	Mark the checkbox, if this routing rule is to apply to all emergency numbers defined in the emergency number list. In doing so, the configuration in the destination number field is not taken into consideration.
Destination number	International numbers in the E.164 format can be stored as destinations. The routing rule is then valid for the destination numbers stored here.
IP Address	Enter an IP address if this routing is to be valid only for terminals from a particular IP network. Otherwise this field remains empty.
Netmask	Enter the corresponding network screen.
Weekday from/to	Select the range of weekdays.
Time from/to To	Specify the time range for which this rule is to be valid.
VoIP provider group	Select the VoIP service provider group via which the calls are to be routed.
Source Number	To change the source number, the relevant modifications can be stored here.
	(\$1) denotes the entire number from the above-mentioned source number entry. If no changes are made, then the CLIP number stored for the relevant extension is taken over, or else the internal number The individual bracketed areas of the above-mentioned source number are numbered in turn and are available with (\$2), (\$3), Example: The extension has number 123 and is to be changed to number 98713. To do so, enter 987(\$1). The result of
	the source number must always be a number in the E.164 format in order to guarantee correct routing.
Destination Number	The destination number can be modified in a manner analogous to that of the source number. The standard input is (\$1)
Fallback 1. and 2.	
VoIP provider group	If the specified VoIP service provider group cannot be reached for technical reasons, then a fallback can be defined for routing via an alternative VoIP provider group.
Source Number	The source number can be modified.
Destination Number	The destination number can be modified.

To save the information, click on [Save] on the lower bar.

8. Configure Funktel f.airnet DECT

8.1. Configure a DECT Controller

The DECT Controller is accessible via its factory default IP address 192.168.2.1. To access the controller Web Based Management(WBM) you have to configure an IP address in the network 92.168.2.0/255.255.255.0, e.g. 192.168.2.101 on the maintenance PC. If the IP address 192.168.2.1 is already used in your network, directly connect the maintenance PC and the DECT Controller via Ethernet. This may be accomplished by using a direct Ethernet cable or via a separate Ethernet switch where only the maintenance PC and the DECT Controller are connected.

Test via ping, if the DECT Controller is replying to the ping requests (ping 192.168.2.1). If not, check all cabling, switch settings, (e.g. VLAN configuration). Ensure that the configured local IP of the maintenance PC address is up (e.g. ping 192.168.2.101).

Start the Web browser at the maintenance PC.

Access the WBM at the following URL: http://192.168.2.1

Log in to the WBM with appropriate credentials:

Press the **Login** button (not shown). The configuration page for the IP-DECT System Server appears.

Administration by Report 198 High Columns Course Hear Durt Debusins Dates Lart			
Administration into memory are recordenized order over over over over secondary second star			
Administration			
Configuration			
		linense	
		Load License	
		Configuration:	
		Restore Config	
		Beckup Config	
Program Info			
	Artist Column		
Manuface Produces by LIFE 1.2	Active System.	Construction	
version system 1: vs.Lz		System update	
		Reboot Board	
Version System 2: V5.1.2			
		Shutdown Board	
		Factory Setting	
		EULA/Info	
			ApplicType=IWU UserType=DoIPAdmin Active System=1 Hardware=2
		(Logout Help Info Cancel Apply

8.2. Configuration of VoIP (Infrastructure) Network

Since configuration of the IP VoIP (Infrastructure) Network settings requires a reboot of the DECT Controller, these settings are configured initially.

To allow direct IP communication between the DECT Controller and the PBX both devices have to be located in the same IP network. Therefore it is necessary to adapt the IP address of the DECT Controller to the network of the VoIP (Infrastructure). You need at least one unused IP address of the Infrastructure network, which has to be configured at the DECT Controller. Select the **configuration page Network** (not shown).

Change the configuration in the bottom frame to the designated values of the DECT Controller (not shown).



Change the following values as needed:

IP address

Configure the IP address at which the DECT Controller should be available inside the VoIP (Infrastructure) Network.

This configuration example uses ip address 192.168.100.1.

Network mask

Enter the corresponding netmask for the IP address as configured above. (Default for Class C networks: 255.255.255.0). This configuration example uses the network mask 255.255.255.0.

Routing Configuration

If routing to another network is necessary (e.g. access from Maintenance PC to IP VoIP (Infrastructure) network) or if infrastructure components (e.g. PBX, NTP servers) are located behind other routers, routing may be configured using a **Default Gateway** or by a specific network route (**Network destination**).

The usage of a **Default gateway** is the recommended routing method.

Using the method **Network destination**, the values for **Network destination**, **Network mask** and **Gateway** have to be configured. At the Maintenance PC a corresponding route has to be configured. This configuration example uses the Default Gateway IP address 192.168.100.83.

Time Server IP

The time settings have to be set according a NTP (or SNTP) time server. After activating the NTP Server, it may take some minutes upon activation of the NTP service. This is due to the nature of time synchronization between NTP server and NTP client.

The Server has a built-in hardware clock. However, usage of an accurate time by using NTP is suggested. This configuration example uses the NTP Server ip address 192.168.201.94. Set the Time zone to an appropriate zone (e.g. " (GMT +01:00) Amsterdam, Berlin, Rome,

Stockholm, Vienna").

Switch to configuration page **Network** → **Local Servers.**

Add an NTP server entry by clicking on Add Server

Enable the new entry, configure the ip address of the NTP Server in filed **IpAddr**, select **NTP** as Type. All other filed in this row may be left unchanged.

Administrati	on Iwu	Network SI	P Media Gateways	Group	User	Dect	Debugging	Status	System				 Ī
Network/S	erver												
[_												
Local Serve	ers												
Index	Enabled	Name	lpAddr	Туре		User				Password	Poll Timer		
1	V	default	10.10.16.1	NTP							0		
			10. The second										
Add	Server	Delete Server	Edit Server	Show Serve	erConfig								

Important: Ensure that the *ip configuration* is configured *correctly*. Otherwise - after rebooting the DECT Controller - it may not be accessible without resetting it to its factory defaults (which have a fixed IP setting of 192.168.1.1 or 192.168.2.1).

8.3. Configuration of DECT Network

Since configuration of the DECT Network settings requires a reboot of the DECT Controller, the settings are configured before the DECT Controller hardware is attached to the designated network segment.

Select configuration page Media Gateways → Dect Network.

Administr	ation Iwu Netw	ork SIP Media	Group Group Group	up User Dect	Debuggi	ng Statu	s System
Media Ga	teways-Dect Netwo	rk 🛛					
Dect	Dect Network License						
Index	Name	Dect Serverip	Dect Netmask	Dect Listen Port	VPN en	VLAN Id	MGW a
1	MgwLocal	192.168.22.1	255.255.255.0	10500		0	

Change the configuration of entry **MgwLocal** in the table to the designated values of the DECT Controller.

Dect ServerIp

This field contains the IP address of the server (the DECT Controller) in the DECT network. It is used for communication between all DECT base stations and the DECT Controller. This configuration example uses the Server IP address 192.168.10.1.

Dect Netmask

In this field the corresponding network mask which is assigned to the Server Ip address is configured. (The default value for a Class-C network is 255.255.255.0). This configuration example uses the network mask 255.255.255.0.

Select configuration page Media Gateways → Dect.

Administr	ation Iwu Network	SIP	Media Ga	teways	Group User Dect Debugging	Status	System			
Media Ga	teways-Dect									
Dect	Dect Network License									
Index	Name	ARI exc	FPS	PLI	Segments/RPNs/LAL	System	Default	Page R		
1	MgwLocal	1024f0b	c	29	1 - 255 RPNs/Loc.Area - LAL=31	0000		6		

ARI excl FPS, FPS

In the field **ARI excl FPS** and **FPS** the System ARI (DECT ID) which has to be unique at each DECT system is configured. The System Ari is provided by the license dongle. Supported System Ari classes are Class B Ari.

Hint: All handset registrations are bound to a specific System ARI. If the System ARI is changed, all handsets lose their registration at the DECT Controller. To achieve system functionality, the handsets have to be registered again at the DECT Controller.

ARI excl FPS = 101b2ff

FPS = 7

This configuration example uses the System ARI 101b2ff7.

System Pin

The **PIN** is a 8-digit number and it is needed for the registration of handsets. It is preconfigured with "00000000" and may be configured system wide here. Change the system pin to another decimal value if required. This configuration example uses the System Pin **1234**. Apply the changes by clicking the **Apply** button(not shown) at the bottom section.

Apply!	Configuration saved!

As stated above, for the changes to become active, the DECT Controller has to be rebooted.

Important: After rebooting, the DECT Controller will not be accessible by its the IP address 192.168.2.1 anymore. Instead it is accessible by the IP address of the IP VoIP (Infrastructure) Network (configured at the step above). If you have attached the DECT Controller directly via an Ethernet cable you have to attach the DECT Controller physically to the designated network segment **after rebooting** it.

Select the configuration page Administration(not shown).

Initiate the reboot by clicking on the **left button** which is labeled [Active (x)]. The "x" is a placeholder for the active partition number, in this example x=2.



Start the reboot process by clicking on button **Active (2)**, if the current active partition is System 2 (as this example used - see output of **Active System:**). If the active system of your DECT Controller is 1, then click the **left button** which is labeled **Active (1)**.

Wait about 2 minutes for the DECT Controller to come up again.

Access the WBM (Web based management) by the IP address you have configured before for the IP VoIP (Infrastructure) Network.

8.4. Configuration of Users at the PBX

It is assumed that the VoIP users at the PBX are already configured. Configuration of Users at the DECT Controller.

8.5. Gateway and Group

Access the WBM of the DECT Controller via the web browser at the maintenance PC. Example: http://192.168.100.10

Log in to the WBM with the appropriate credentials.

Switch to configuration page "SIP \rightarrow General".

Add a new gateway entry by clicking on the button Add Gateway(not shown).

Administra	ation Iwu	Network	SIP Media	Gateways Group U	Jser Dect Del	bugging Status	System				
5IP-Gene	ral										
General	SIP Settings										
Index	Display	Enabled	Name	Gateway Type	ListenPortRe	SIP Server Id	Resolv	Use OBP	Outbound Proxy	Netmask	
		[TTTA]	A	Defer	6060	40 40 46 7	(and	[and]	0000	255 255 255 0	

Change the following values:

Gateway Type

The Gateway Type is set to "Default".

SIP Server Id and Netmask

Change the preconfigured **SIP Server Id** from 0.0.0.0 to the IP address of the used **PBX** as well as the corresponding **Netmask**. This configuration example uses the IP address 192.168.100.50 and the network mask 255.255.255.0.

Switch to configuration page tab Group

Groups are the connecting link between Gateways and VoIP Users. A User is assigned to a Group and a Group is assigned to a Gateway.

Add a new group by clicking on the button Add Group.

Administrat	tion Iwu	Network SIP	Media Gateways	Group	ser De	ect D	Debugging	Status Sy	tem
Group									
Enabled	Update	Name	Gateways	Intern	C CV	V (C	VM (Vo	VM Number	/0
	5	default	[001] default	3					

Name

Change the preconfigured name of the Group (e.g. to the name of the corresponding PBX). This name is only used for the internal configuration of the DECT Controller Software. This configuration example uses the default Group name "default".

Gateways

Select the gateway from the dropdown field which you have configured in the last step.

InternCallLength

With this setting the maximum number of digits of the calling Party number for internal calls is configured. Calls with a larger number of digits are signaled as external calls at the handset. The default value is "3".

Note: Alternatively it is possible to register several users at once using the Bulk Registration *Mode (see "Multi-Register (Bulk Registering) of Handsets"). Since this method is out of scope of a quick start, the manual method is used here.*

Switch to configuration page User, sub page User (User \rightarrow User).

• Set up one or several **Users** according the user configuration at the **PBX** for the connection with the DECT Controller. Please take care of the consistency of the entries between the PBX and the DECT Controller.

Add a new user by clicking on the button Add User.

Note: To add a new user entry (even during running system services) it is necessary to select an existing user (otherwise an error message will appear) and then click on button [Add User]. A new entry with default values is inserted above the selected user entry..

Administra	ation Iwu	Network	SIP Media Ga	teways Group L	Jser Dect Deb	ugging Status	System
User-User							
User	/oip Dect						
Index	Enabled	Msn	DisplayName	Comment	Language	Groups	
2		8075200	D11 8075200	default	Deutsch	[001] default	
1	1	8075201	FC4 8075201	default	Deutsch	[001] default	
3		8075202	FC4 8075202	default	Deutsch	[001] default	
4		8075203	D11 8075203	default	Deutsch	[001] default	

Change the contents of the following fields:

MSN (necessary)

The MSN has to correlate with the Call number of the User at the PBX. This configuration example uses MSN 8075200, 8075201, 8075202 and 8075203.

DisplayName (necessary)

This information is shown at the idle display of the corresponding handset. This configuration example uses MSN D11 8075200, FC4 8075201, FC4 8075202 and D11 8075203.

Comment (optional)

Enter any desired text for administration purposes e.g. "Sales", "Marketing" and "Support". This configuration example uses the values "default".

Language

The language used for display messages of the handset can is selected here. This configuration example uses language "Deutsch". The supported languages are shown in the picture.

											_
Administra	ition Iwu	Network	SIP	Media Gatewa	ays Group	User	Dect	Debu	ugging	Status	System
User-User											
User V	oip Dect										
Index	Enabled	Msn	Display	Name	Comment		Language		Gr	oups	
2		8075200	D11 80	75200	default		Deutsch	×	× [0]	01] default	
1		8075201	FC4 80	75201	default		Deutsch		[0]	01] default	
3		8075202	FC4 80	75202	default		English		[0]	01] default	
4		8075203	D11 80	75203	default		Nederland	5	[00	01] default	
							Francais				
							Italiano				
							Espanol				
							Danish				
							Cesky				
							Suomi				
							Turkce				
							Polski				

Groups

Choose a Group (and with that a Gateway) from the dropdown box to which the user is associated to. This configuration example uses the default Group name "default". Switch to configuration page User, sub page Voip (User \rightarrow Voip).

Administra	tion Iwu	Network	SIP Med	dia Gateways	Group	User	Dect	Debugging	Status	System	
User-Voip											
User Vo	oip Dect										
Index	Enabled	Msn	DisplayName	Con	nment		UserNan	ie	AuthName	e	Password
2	V	8075200	D11 8075200	defa	ault		8075200		8075200		*****
1	V	8075201	FC4 8075201	defa	ault)	8075201		8075201		23222
3		8075202	FC4 8075202	defa	ault		8075202		8075202		*****
4	V	8075203	D11 8075203	defa	ault		8075203		8075203		*****

Change the contents of the following fields:

UserName (necessary)

Configure the Name or Number for the registration of the User at the PBX. This configuration example uses the UserName 8075200, 8075201, 8075202 and 8075203.

AuthName (optional)

Configure the AuthName which is used for the authentication at the PBX (together with "Password"). This configuration example uses the AuthName 8075200, 8075201, 8075202 and 8075203.

Password

Optional, but necessary if an **AuthName** is configured. The password which is used for the authentication at the PBX (together with **AuthName**). This configuration example uses the Passwords 0000 but shown as ****.

Note: The entries in the password field are visible only at time of adding or overwriting a password. After applying the changes, the password fields are masked out and not visible anymore.

Apply the changes by clicking the Apply button(not shown) at the bottom section.



Confirm the message box by clicking on **OK**.

To append further users to the configuration, repeat the steps above.

8.6. Configure DECT-FB4 IP Base Stations to the System

Attach at least two DECT-FB4 IP base stations to a PoE port of the network switch of the DECT network. If you use a standard port of the network switch without PoE, use a separate power supply.

Inside this configuration example the first DECT-FB4 IP base station is configured as the synchronization master for over-air synchronization. The second DECT-FB4 IP base station and all further base stations are configured as synchronization slave.

Wait about 2 minutes until the LED states at the DECT-FB4 IP base stations change to permanently red.

DECT About

At the WBM of the DECT Controller switch to configuration page **Dect-About**(not sohwn).

• To scan the newly attached second DECT-FB4 IP click on the button **Scan**(not shown).



The newly attached DECT FB4 IP should be found automatically and a record will be appended for it in the table of DECT devices.

Administ	ration Iwu	Network	SIP Media Gates	Nays	Group User D	ect Deby	ugging 5	tatus System					
Dect-Ab	out												
Base	Radio Sy	nc Ari	Call About Deb	and and									
index	Module	Enabled	Name	Ту	BasestationSerialNr	Version -	HwRev	Partinfo1	Partinfo2	IpAddr Module	IpAddr Server	Server	Mac Addr
1	001	V	Bslp only	Bsip	107379927	V5.1.2	14	V5.1.2 Active	nia	192.168.10.1	192.168.10.250	10500	00-1a-e8-22-35-45
2	002	1	Bsip only	Bslp	122270668	V5.1.2	15	V5.1.2 Active	n/a	192.168.10.2	192.168.10.250	10500	00-1a-e8-22-5a-c2
3	003	1	Standard Basis 0001	Fb	0000123457	V5.1.2	0	V5.1.2 Active	nia	192.168.10.3	192.168.10,250	10500	e0-b6-f5-c0-0a-c6
4	004	1	Standard Basis 0003	Fb	0000123457	V5.1.2	0	VS.1.2 Active	n/a	192.168.10.4	192.168.10.250	10500	08-38-a5-fd-20-c.b

DECT Base

At the WBM of the DECT Controller switch to configuration page **Dect-Base**. The DECT-FB4 IP base station has to be configured for usage within the IP-DECT System. Select the newly created entry for DECT-FB4 IP base station and change the contents of the following fields:

-					
Administra	tion twu	Network	SIP Media Gate	ways Group	User Dect Debugg
Dect-Base					
Base	Radio Sy	rrc Ari	Call About Del	NIQ.	
Index	Module	Enabled	Name	IpAddr Module	Mac Addr
1	001	1	Bslp only	192.168.10.1	00-1a-e8-22-35-45
2	002	1	Bslp only	192.168.10.2	00-1a-e8-22-5a-c2
3	003	1	Standard Basis 0001	192,168,10.3	e0-b6-f5-c0-0a-c6
4	004	[¥]	Standard Basis 0003	192.168.10.4	08-38-a5-10-20-c b

Enabled (necessary)

Set to Enabled for usage within the IP-DECT System.

Name (necessary)

Configure a descriptive name for the DECT base station. Change the preconfigured name of the DECT base station (e.g. to the name of the physical location it is designated for). This name is only used for the internal configuration of the base station.

IpAddrModule (necessary)

Configure an IP address for this DECT RBS inside the DECT network. Hint: The IP-DECT System-System automatically suggests a valid IP address.

DECT Sync

At the WBM of the DECT Controller switch to configuration page **Dect-Sync**.

		-		111				
Administrat	ion Iwu Network	SIP	fedia Gateways Grou	ip User De	t Debugging Status :	System		
Dect-Sync								
Base	adio Sync Ari	Call Ab	out Debug					
Index	Module Number MGW	Enabled	Name	Sync	ParkSync 1	ParkSync2	ParkSync3	StatSync Group
1	001	1	Bslp only	1588 master	n/a	n/a	n/a	1
2	002	4	Bslp only	1588 slave	[001] Bsip only	n/a	n/a	0
3	003	4	Standard Basis 0001	air	[002] Bslp only	n/a	n/a	0
4	004	V	Standard Basis 0003	air.	[003] Standard Basis 0001	n/a	n/a	0

Select the newly created entry for DECT Controller and change the contents of the following fields:

Sync (necessary)

Set Sync to air to synchronize the actual base station to another base station via air.

ParkSync1 (necessary)

Select from the dropdown to which base station the selected base station should be synchronized to. This configuration example uses Module **[001] BSIPIWU Local** as the sync master.

DECT ARI

At the WBM of the DECT Controller switch to configuration page Dect-Ari.

-							
Administra	tion Iwu	Network	SIP Media Gatev	vays Gro	up User Dect	Debugging St.	atus System
Dect-Ari							
Base	Radio Si	mc Ari	Call About Deb	40			
Index	Module	Enabled	Name	Cipher	Segment	Segmen	Rpn
1	001	1	Bslp only	1	1 - RPN 1 255	1	1/0x01
2	002	V	Bslp only	1	1 - RPN 1 255	2	2/0x02
3	003	1	Standard Basis 0001	1	1 - RPN 1 255	з	3/0x03
4	004	1	Standard Basis 0003	1	1 - RPN 1 255	4	4/0x04
1.0							

Select the newly created entry for base station and change the contents of the following fields:

Segment Relative Index

Using this dropdown box, the DECT module has to be assigned a relative Index related to the selected location segment inside the MGW. The combination of **Segment** and **Segment Relative Index** will be calculated by the WBM to the resulting RPN.

Note: The IP-DECT System-System automatically suggests a valid RPN Segment Relative Index.

Note: When using several base stations they have to be configured with a unique "Segment Relative Index" different from "0". Using the same Segment Relative Index as the DECT module number (Index) is very feasible.

DECT About

At the WBM of the DECT Controller switch to configuration page **Dect-About**.

Administr	ation 1w	Network	SIP Media Gates	Nays	Group User D	ect Deb	igging 5	tatus System					
Dect-Abo	ut												
Base	Radio S	ync Ari	Call About Deb	aug.									
index	Module	Enabled	Name	Ту	BasestationSerialNr	Version -	HwRev	Partinfo1	Partinfo2	IpAddr Module	IpAddr Server	Server	Mac Addr
1	001	V	Belp only	Bslp	107379927	V5.1.2	14	V5.1.2 Active	n/a	192.168.10.1	192.168.10.250	10500	00-1a-e8-22-35-45
2	002	1	Bslp only	Bslp	122270668	V5.1.2	15	V5.1.2 Active	n/a	192.168.10.2	192.168.10.250	10500	00-1a-e6-22-5a-c2
3	003	1	Standard Basis 0001	Fb	0000123457	V5.1.2	0	V5.1.2 Active	nia	192.168.10.3	192.168.10.250	10500	e0-b6-f5-c0-0a-c6
4	004	1	Standard Basis 0003	Fb	0000123457	V5.1.2	0	V5.1.2 Active	n/a	192.168.10.4	192.168.10.250	10500	08-38-a5-fd-20-cb

The fields **IpAddr Module** and **IpAddr Server** display the current (default) values for the selected base station.

To apply all the changes to all base stations, the base stations have to be synchronized. During the synchronization process the base station will receive its configuration values from the DECT Controller.

Apply the changes by clicking the Apply button(not shown) at the bottom section.



Confirm the message box by clicking on **OK**.

A debug window will appear.

ebug Window	6						
(Info)							
Validation	deta	ils	: Level 4				
(W - A-1 - 1							
(Module) Code Lvl:	Мо				name		
W0063(1):	2 "		BsIp	Room	2.012":	enabled, has the wrong server-ip address	
W0099(1):	2 "		BsIp	Room	2.012":	IpAddrFromModul=192.168.10.202 != IpAddrToModul=192.168.10.2	
W0100(1):	2 "		BsIp	Room	2.012":	IpAddrServerFromModul=192.168.10.120 != IpAddrServerToModul=192.168.10.1	
WOO63 occu	red	1	times				
W0099 occu	red	1	times				
W0100 occu	red	1	times				
total warn	ings:	3					
						Ok	

Confirm the Debug window by clicking on **OK**.

Start the synchronization process by clicking the **Sync** button(not shown) at the bottom section. A message box will appear.



Confirm the message box by clicking on **OK**.

The following process will transfer the new settings to all base stations. Therefore, the base stations will be rebooted automatically by the system.

Wait about 2 minutes until the base station is started completely (LED states should be green/red)

To verify the configured values of the previous steps, click on the **SCAN** button(not shown).

Scan!	scanning modules
	Cancel

At the WBM of the DECT Controller switch to configuration page **Dect-About**(not shown). Verify, if the values **IpAddr Module** and **IpAddr Server** contain the correct values which have been configured before (IpAddrModule \rightarrow IpAddr Module, Server Ip \rightarrow IpAddr Server).

8.7. Start System Services and Register Handsets

8.7.1. Start System Services

Switch to configuration page System.

To start the functionality of the DECT Controller, first start the system services.

Start the services by clicking the **System Start** button(not shown) at the bottom section. Starting the services requires some time.

Check if the system services are running by clicking at the **Refresh** button(not shown) several times.

Administra	ation Iwu Netwo	rk SIP I	Media Gateways	Group User	Dect Debugging	g Status	System
System							
Enabled	Applic Name	Status	License	Up since	Service		
V	capisrv.exe	Stopped	OK	23.02.2017 13:12	V		
	iwu.exe	Stopped	OK	23.02.2017 13:13			
	EtpRouter.exe	Stopped	OK	23.02.2017 13:13			

If the system services are started correctly (all states displayed as **Running**, the LED state at the DECT base station should change from flashing yellow to flashing green.

If a time server is configured correctly and can be contacted, the field "Up since" should display actual local time values, otherwise time will start at "01.01.1970 00:00".

8.7.2. Register Handsets

Note: Alternatively it is possible to register several users at once using the Bulk Registration *Mode. Since this method is out of scope of a quick start, the manual method is used here.*

User-DECT

Switch to configuration page User-Dect.

- Prepare one handset for the registration process.
- Attention: Do not confirm the following procedure at the Handset right now! Start the Registration procedure via the menu at the Handset.
 If the handset requires a PARK, leave the PARK field empty and confirm with OK.
 If the handset requires an Access Code, enter the DECT Controller system PIN which has been pre-configured to 0000 at configuration page DECT as Access Code.
 Attention: Do not confirm this entry yet!
- Select the corresponding user in the WBM to which the handset has to be assigned to.

Administr	ation	1 uwi	Network SIP	Media Gateway	ys Group User	Dect Debuggi	ing Status Sys
User-Dec	t						
User	Volp	Dect					
Index # I	Ena	Man	DisplayName	Comment	HandsetType	Ipul	UAK
1	1	8075200	FC4 8075200	default	DolP	0000000000	
2	1	8075201	FC4 8075201	default	DolP	0000000000	
3	1	8075202	FC11 8075202	default	DolP	0000000000	
4		8075203	D11 8075203	default	DolP	0176049498	

• Activate the Registration procedure at the WBM by clicking Register(not shown) at the bottom section of page User-Dect.

Handset	register!
į	Please register handset!
	Cancel

- Now confirm the already entered PIN at the Handset (normally with soft button "OK").
- The WBM displays the successful Registration of the Handset.

Handset	register!
Ų	Handset registered!

The IPUI of the registered handset is displayed in hexadecimal notation in the user entry.

Administrati	ministration Iwu Network SIP Media Gateways Group Uber Dect Debugging Status System													
User-Dect														
Lowr. Volp Dect														
Index . Ent	Man	DisplayName	Comment	HandsetType	Ipul	UAK								
1 😥	8075200	FC4 8075200	default	DolP	0176008285									
2 🛛	8075201	FC4 8075201	default	DolP	0176018262									
3 12	8075202	FC11 8075202	default	DolP	0011E24DC5									
4 😥	8075203	D11 8075203	default	DolP	0176049498									

After registering several users, telephony functionality should be available. You should be able to establish calls between the handsets.

9. Verification Steps

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

9.1. Communication Manager SIP Trunk status

Use the status trunk n where n is the SIP trunk number. Make sure that all trunks are showing as **in-service/idle**. Make a Call into the Communication Manager and make sure that the call can be answered.

status trunk 11												
TRUNK (GROUP STATUS											
Service State	Mtce Connected Ports Busy											
<pre>in-service/idle in-service/idle in-service/idle in-service/idle</pre>	no no no											
<pre>in-service/idle in-service/idle in-service/idle</pre>	no no no											
in-service/idle in-service/idle in-service/idle	no no no											
	TRUNK (Service State in-service/idle in-service/idle in-service/idle in-service/idle in-service/idle in-service/idle in-service/idle in-service/idle in-service/idle											

9.2. Session Manager Entity Status

From the System Manager Dashboard select Session Manager \rightarrow SIP Entity Monitoring. Make sure that the Funktel Entity shows **UP** under **Conn. Status** and **Link Status**.

Home Session Manager * Session Manager *															
Session Manager Home / Elements / Session Manager / System Status / SIP Entity Monitoring															
Dashboard															
Session Manager	ssion Manager Session Manager Entity Link Connection Status														
Administration															
Communication	Inis page displays detailed connection status for all entity links from a Session Manager.														
Profile Editor	All Entity Links for Session Manager: SM71676 Status Details for the selected Session Manager:														
► Network															
Configuration															
 Device and Location 	Summary View 17 Items Refresh Filter: En														
Configuration															
 Application 															
Configuration							Conn								
▼ System Status		SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Status	Reason Code	Link Status						
SIP Entity	0	SBCE60	10.10.16.60	5060	TCP	FALSE	UP	200 Keepalive	UP						
Monitoring	0	AMS1616	10.10.16.16	5060	TCP	FALSE	UP	200 OK	UP						
Managed	0	PGSBC	10.10.16.151	5060	TCP	FALSE	UP	200 OK	UP						
Bandwidth Usage	0	AAEP1620	10.10.16.20	5060	TCP	FALSE	UP	200 OK	UP						
Security Module	0	Funktel	10.10.16.7	5060	TCP	FALSE	UP	200 OK	UP						
Status	0	<u>CM1623</u>	10.10.16.23	5060	тср	FALSE	UP	200 OK	UP						

SJW; Reviewed: SPOC 6/14/2017

Solution & Interoperability Test Lab Application Notes ©2017 Avaya Inc. All Rights Reserved. 69 of 71 FtelDPx_CM7_SM7

10. Conclusion

These Application Notes describe the configuration steps required for Funktel DPx and DECT Handsets to successfully interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager via a SIP Trunk. Please refer to **Section 2.2** for test results and observations.

11. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at <u>http://support.avaya.com</u> where the following documents can be obtained.

- [1] Administering Avaya Aura® Communication Manager, Document ID 03-300509
- [2] Avaya Aura® Communication Manager Feature Description and Implementation, Document ID 555-245-205
- [3] Administering Avaya Aura® Session Manager, Release 7.0, Issue 1 August 2015
- [4] Administering Avaya Aura® System Manager, Release 7.0, Issue 1, August, 2015

Product Documentation for Funktel Products can be obtained from Funktel.

- [1] DECT IP Controller Administration Manual, Document ID 5010790011
- [2] DPx DevConnect Setup guide
- [3] Bedienungsanltg. FC4/FC4Ex(HS), Document ID 5000807201
- [4] Bedienungsanleitung D11/FC11, Document ID 5000807226

©2017 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM 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 <u>devconnect@avaya.com</u>.