6.10.7 SUBSCRIBING DECT PHONE DATASETS

After adding a DECT phone dataset to the OMM, the DECT phone must be subscribed. The OMM must first be enabled to allow subscriptions from DECT phones. Subscribing DECT phone datasets is possible in the **Overview** panel and in the **Device** panel. To start subscription, press one of the following commands in the **DECT phones** menu:

- **Subscription**: Start DECT phone subscription with configured IPEI. For more information on this see section 5.7.3.1.
- **Wildcard subscription**: Start DECT phone wildcard subscription (without configured IPEI). In the **Wildcard subscription** dialog, which is now opened, enter the **Timeout** for this subscription method. Press the **Start** button. For more information on this see section 5.7.3.2.

6.10.8 DELETING DECT PHONE DATASETS

Deleting DECT phone datasets is only possible in **configuration mode**. You can delete the fixed DECT phone dataset (in case of fixed relation) or only the DECT phone user data resp. the DECT phone device data (in case of dynamic relation).

To delete one or more existing DECT phone datasets proceed as follows:

1 Select the appropriate DECT phone dataset(s) in the DECT phone table by activating the corresponding checkbox(es).

2 In the task bar on the right of the **DECT phones** panel click on the **Delete** command.

– In the **Overview** submenu the whole DECT phone dataset will be deleted.

– In the **Users** submenu only the DECT phone user data will be deleted.

– In the **Devices** submenu only the DECT phone device data will be deleted.

The **Delete [xxx]** dialog opens showing a confirmation prompt.

3 Confirm the displayed prompt with **OK**.

6.10.9 SELECTING COLUMNS

You can adapt the parameters shown in the DECT phone table to your needs:

1 Click **Select columns** under the Task list on the right-hand side of the **DECT Phones** window.

The **Select columns** dialog opens.

2 Select the columns that shall be shown by activating the appropriate checkboxes.

3 Click the **OK** button.

4 The DECT phone table will be adapted accordingly.

6.10.10 FILTERING DECT PHONE TABLE

You can filter the list of DECT phone datasets shown in the DECT phone table by using a filter.

1 Click **Filter** under the Task list on the right-hand side of the **DECT Phones** window.

The **Filter** dialog opens.

2 Enter the search string that serves as filter criterion. You can enter digits and characters. The search is case sensitive.

3 Click on the **Filter** button.

The **Filter** dialog is closed and the DECT phone table will be adapted accordingly.

4 To reset the filter, click on the **Filter** command in the task bar on the right of the **DECT phones** panel.

5 In the **Filter** dialog click on the **Reset** button.

6.10.11 CHANGING THE RELATION TYPE

You can change a user data-device relation data set from “fixed” to “dynamic” and vice versa. This means the login/logout feature can be enabled or disabled for a DECT phone. The user data device relation can only be changed by the admin user.

To change the relation type of a DECT phone:

1 Select the appropriate DECT phone dataset(s) in the DECT phone table by activating the corresponding checkbox(es).

2 Click **Change rel. type** under the Task list on the right-hand side of the **DECT Phones** window.

Rules to change the relation from “fixed” to “dynamic”

- The DECT phone must be subscribed.
- A user login/logout PIN is configured in the user data set.
- Depending on the DECT phone user login type (“LoginID”), in the **DECT** tab of the **System settings** menu, the **Login ID** option must be set in the **DECT phone user login type** field.

IMPORTANT : If there is no specific PIN configured then “0000” is automatically set.

Rules to change the relation from “dynamic” to “fixed”

- The user relation type must be “Dynamic” (not “Unbound”).
- The user data set is not retrieved from an external user data server / the user data set is provisioned locally in the OMM database.

6.10.12 ENABLING / DISABLING DECT PHONE EVENT LOG

You can store a DECT phone event log file in **Monitor Mode**. Do the following:

1 To enable/disable the DECT phone event log, click **Log events** under the Task list on the right-hand side of the **DECT Phones** window:

✓ - DECT phone event log is enabled.

✗ - DECT phone event log is disabled.

2 Repeat step 1 to disable/enable the DECT phone event log.

The DECT phone event log will be stored in a file called “pp_event.log“. This file can be found in the user’s home directory:

- On a Linux system it is located under ‘~/.oamp’,
- On a windows system under ‘c:/Users/<user>/MyDocuments/.Oamp’.

6.10.13 USER MONITORING

User monitoring menu available in monitoring mode only a list of the DECT Phone users who are configured for user monitoring.

The following parameters are displayed for each DECT Phone user:

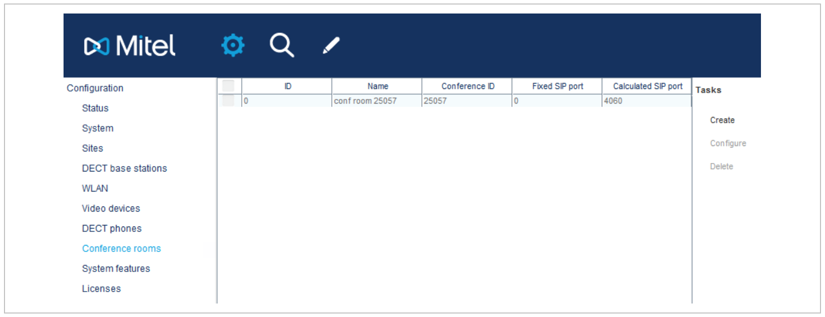
- User ID
- Name
- Number
- Related device ID
- Mode: User monitoring mode (active or passive)
- Combined User Status (CUS)
- Handset Assignment Status (HAS) (Dynamic User logged on)
- Handset Subscription Status (HSS) (DECT subscribed)
- Handset registration status (HRS) (DECT attached)
- Handset activity status (HCS) (Handset active within time period)
- SIP user registration status (SRS) (SIP user registered)
- Silent charging status (SCS) (Silent charging + Charger)
- Call diversion status (CDS) (immediate call diversion enabled)
- Handset battery status (HBS) (Battery power above limit, warn only)
- Software status (SWS) (minimal required software version, warn only)

Monitoring parameter can have these values:

- ✓ - Available
- ⚠ - Warning
- ✗ - Unavailable
- ✗ - Escalated

6.11 "CONFERENCE ROOMS" MENU

On this menu page you managed individual conference rooms for the Integrated Conference Server (ICS). For details on how to configure the conferencing feature refer to section 7.21 .



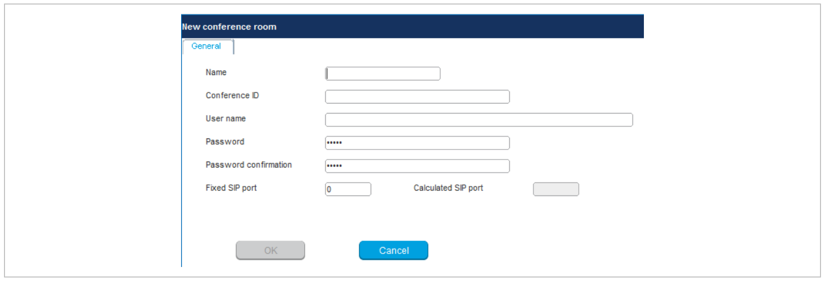
ID	Name	Conference ID	Fixed SIP port	Calculated SIP port
0	conf room 25057	25057	0	4060

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create conference room		6.11.1
Configure: Configure selected conference room		6.11.2
	Show details: Show details about a selected conference room	6.11.4
Delete: Delete selected conference room		6.11.3

6.11.1 CREATING CONFERENCE ROOMS

In **Configuration Mode** you can create new conference rooms. Conference rooms will be registered on the configured SIP registrar, thus you must enter the SIP account data to be used.



Name:
Conference ID:
User name:
Password: •••••
Password confirmation: •••••
Fixed SIP port: 0
Calculated SIP port:

1 Click **Create** in the **Tasks** menu of the **Conference rooms** page.

2 In the **General** tab, enter the conference room parameters.

- **Name**: Enter the SIP display name for the SIP account to be used.
- **Conference ID**: Enter the SIP user id.

- **User name**: Enter the SIP authentication name.
- **Password, Password confirmation**: Enter the password that is required by the SIP server.
- **Fixed SIP port**: Enter the port used explicitly for SIP signaling. If set to 0, an automatically calculated port is used for this conference room. The default is 0. See section 3.17 for more information on this feature.

3 Click **OK**.

6.11.2 CONFIGURING CONFERENCE ROOMS

In **Configuration Mode** you can configure an existing conference room.

1 Select the appropriate conference room entry in the conference rooms table.

2 Click **Configure**.
The **General** tab is displayed showing the current conference room configuration.

3 Change the conference room parameters as required.

4 Click **OK**.

6.11.3 DELETING CONFERENCE ROOMS

In **Configuration Mode**, you can delete conference rooms.

1 Select one or more conference rooms entries in the conference rooms table.

2 Click **Delete**.
A confirmation dialog appears.

3 Click **OK** to confirm.

6.11.4 VIEWING CONFERENCE ROOM DETAILS

In **Monitor Mode**, you can view the details of a conference room.

1 Select the appropriate conference room entry in the conference room table.

2 Click **Show details**.
The **General** tab is displayed showing the conference room configuration.

3 Click **Cancel** to close the tab.

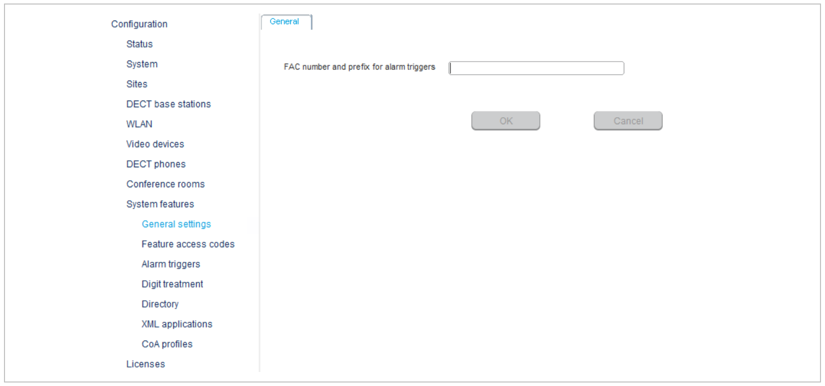
6.12 “ALARM TRIGGERS” MENU “SYSTEM FEATURES” MENU

The **System features** menu provides the following entries:

Configuration mode	Monitor mode	See section
General settings	General settings	6.12.1
Feature access codes	Feature access codes	6.12.2
Alarm triggers	Alarm triggers	6.12.3
Digit treatment	Digit treatment	6.12.4
Directory	Directory	6.12.5.1
XML applications	XML applications	6.12.7
CoA profiles	CoA profiles	6.12.8

6.12.1 “GENERAL SETTINGS” MENU

The **General settings** menu allows to configure/view the FAC number prefix used for feature access codes and alarm triggers.

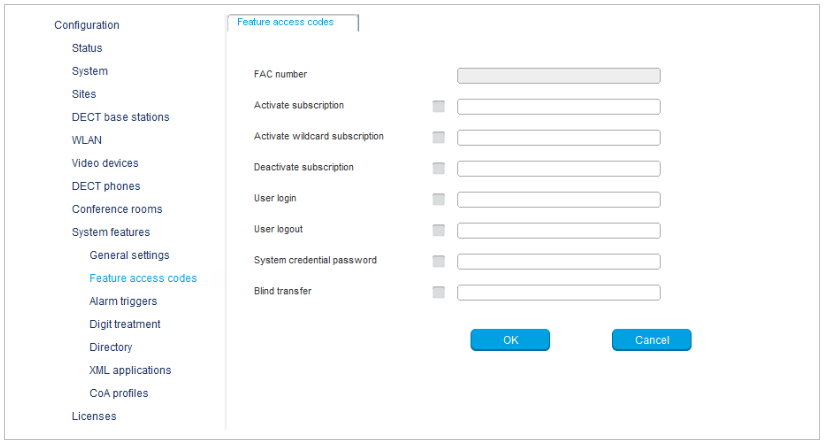


1 **FAC number and prefix for alarm triggers**: Enter a unique FAC number.

2 Press the **OK** button.

6.12.2 “FEATURE ACCESS CODES” MENU

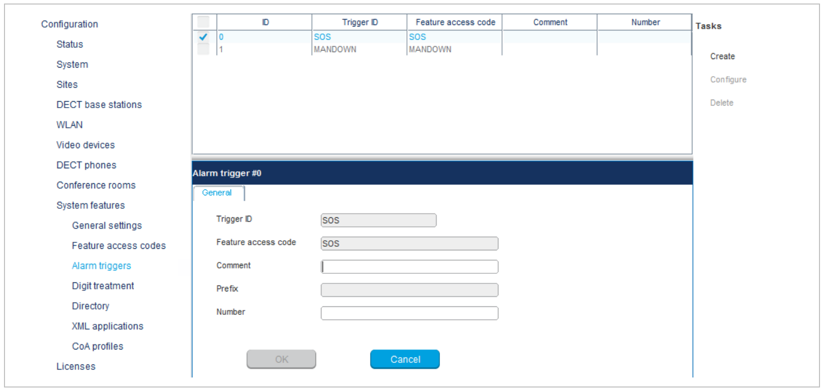
The **Feature access codes** menu is used to configure/view the feature access codes parameters.



The **FAC number** which introduces the feature access code (see also section 6.12.1) is displayed. For a description of the parameters which can be set in this menu see section 5.9.4.

6.12.3 "ALARM TRIGGERS" MENU

The **Alarm triggers** menu allows configuration and display of numerous alarm trigger datasets. There are two predefined alarm triggers ("SOS" and "MANDOWN") which cannot be deleted.



	ID	Trigger ID	Feature access code	Comment	Number
✓	0	SOS	SOS		
	1	MANDOWN	MANDOWN		

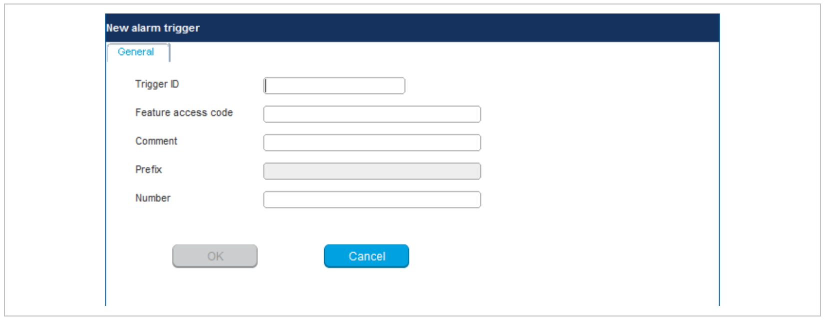
Trigger ID: SOS
Feature access code: SOS
Comment:
Prefix:
Number:

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create alarm trigger		6.12.3.1
Configure: Configure a selected alarm trigger		6.12.3.2
	Show details: Show parameters of a selected alarm trigger	6.12.3.4
Delete: Delete selected alarm triggers		6.12.3.3

6.12.3.1 Creating "Alarm triggers"

In **Configuration Mode** you can create new alarm triggers.



1 Click **Create**. In the **General** tab enter the alarm trigger parameters.

2 **Trigger ID**: Enter the AlarmTrigger ID that the OMM sends to identify the alarm scenario and the source that triggers the alarm.

3 **Feature access code**: Enter the feature access code that the user dials to initiate the alarm.

4 **Comment**: Enter a comment for the new trigger.

5 **Prefix**: This field displays the **FAC number** which introduces the feature access code (see also section 6.12.1).

6 **Number**: Enter the number to be called if the user triggers the alarm by dialing the feature access code. If no number is specified, the call is released.

7 Press the **OK** button.

6.12.3.2 Configuring "Alarm triggers"

In **Configuration Mode** you can configure an existing alarm trigger.

1 In the alarm trigger table click on the appropriate trigger entry.

2 Click **Configure**.

The **General** tab is displayed showing the current trigger configuration.

3 Change the trigger parameters.

4 Press the **OK** button.

6.12.3.3 Deleting “Alarm triggers”

In **Configuration mode** you can delete alarm triggers. The predefined alarm triggers (‘SOS and ’Man down‘) cannot be deleted.

1 In the alarm trigger table click on one or more trigger entries.

2 Click **Delete**.

3 Confirm the displayed prompt with **OK**.

6.12.3.4 View “Alarm trigger” Details

In **Monitor Mode** you can view the details of an alarm trigger.

1 In the alarm trigger table click on the appropriate trigger entry.

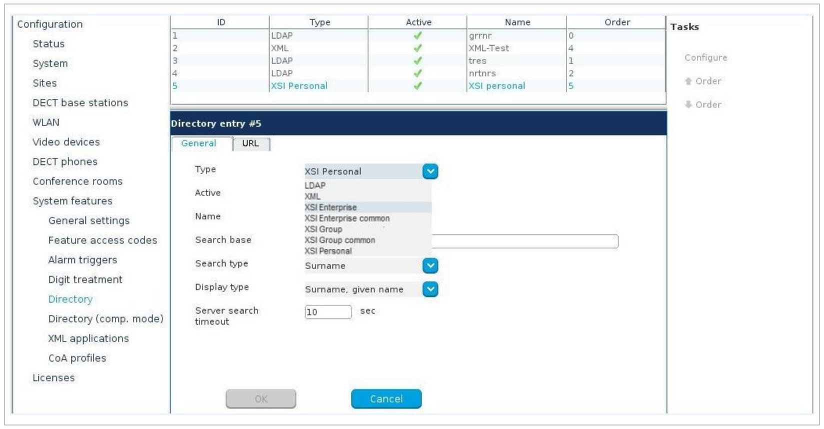
2 Click **Show details**.

The **General** tab is displayed showing the trigger configuration.

3 Click **Cancel** to close the tab.

6.12.4 “DIGIT TREATMENT” MENU

The **Digit treatment** menu allows you to configure the number manipulation that is provided by the digit treatment feature for LDAP corporate directories.



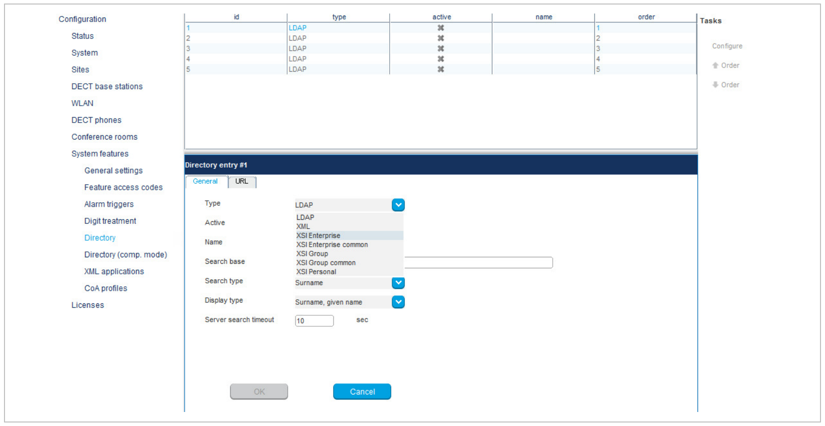
ID	Type	Active	Name	Order
1	LDAP	✓	grrnr	0
2	XML	✓	XML-Test	4
3	LDAP	✓	tres	1
4	LDAP	✓	nrtnrs	2
5	XSI Personal	✓	XSI personal	5

Type: XSI Personal
Active
Name
Search base
Search type: Surname
Display type: Surname, given name
Server search timeout: 10 sec

For a description of tasks and parameters available in this menu, refer to section 5.9.1.

6.12.5 “DIRECTORY” MENU

The **Directory** menu allows configuration of LDAP, XML or XSI -based corporate directory services.



id	type	active	name	order
1	LDAP	✖		1
2	LDAP	✖		2
3	LDAP	✖		3
4	LDAP	✖		4
5	LDAP	✖		5

Type: LDAP
Active
Name
Search base
Search type: Surname
Display type: Surname, given name
Server search timeout: 10 sec

The tasks which can be performed are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new directory entry in detail panel		6.12.5.1
Configure: Configure selected directory entry in detail panel		6.12.5.2
	Show details: Show selected directory entry in detail panel	6.12.5.3
Delete: Delete selected directory entry/entries		6.12.5.4

6.12.5.1 Creating New Directory Entries

Adding directory entries is only possible in **configuration mode**. You can configure up to five directory entries. To add a new entry, do the following:

1 In the **Tasks** panel, click **Create**.

The **New directory entry** panel opens and provides various tabs where the directory data must be entered.

2 Configure the directory entry (see parameter descriptions below).

3 Click **OK** to save your changes.

You can specify values for the following parameters in the **New directory entry** panel:

General tab

The following table describes the parameters on the General tab and to which directory type they apply.

Parameter	Description	LDAP	XML	XSI
Type	Interface type supported by the directory server. Possible values: • LDAP • XML • XSI Enterprise • XSI Enterprise common • XSI Group • XSI Group common • XSI Personal	✓	✓	✓
Active	Enables or disables the directory entry on the DECT phone.	✓	✓	✓
Name	Name to be displayed for the directory (Latin-1 character set is supported). **Note**: If there is only one directory entry configured, this value is ignored when the user searches for a number in the telephone's central directory. SIP-DECT 6.0 and later supports the "SIPProxy" placeholder for a directory entry name, in place of the current primary, secondary or tertiary SIP server address.	✓	✓	✓
Search base	Location in the LDAP directory from which the search begins (e.g., "ou=people, o=my com"). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: • "<TEL>" (for the user's telephone number) • "<DESC1>" (for the user's "Description 1" attribute) • "<DESC2>" (for the user's "Description 2" attribute) • "SIPProxy" (for the current primary, secondary or tertiary SIP server address); supported for release 6.1 and later	✓		
Search type	Attribute on which searches are performed (**Surname** or **Given name**).	✓		✓
Display type	Display mode for search results (**Surname, First Name** or **Given name Surname**).	✓		✓
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).	✓		

URL tab

The following table describes the parameters on the **URL** tab and to which directory type they apply.

Parameter	Description	LDAP	XML	XSI
Protocol	Transfer protocol used to communicate with the XML or XSI directory server (**http** or **https**).		✓	✓
Port	Server port number. Specify a value, or enable the **Use default port** flag. For LDAP, the default is 389. SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268. For XML or XSI, the default is 80 for HTTP, and 443 for HTTPS.	✓	✓	✓
Server	IP address or FQDN of the directory server.	✓	✓	✓
User name	Name of the account for directory server access, if required.	✓	✓	
Password	Password for directory server access, if required. Confirm the password in the next field. **Note**: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.	✓	✓	
Path (and parameters)	URL (with parameters, if required) to the XML directory on the XML directory server.		✓	
Use common certificate configuration	Enables or disables use of the system's certificates (loaded for provisioning purposes) for HTTPS directory access.		✓	✓

6.12.5.2 Changing a Directory Entry

Changing directory entry is only possible in configuration mode. To change the configuration of an existing directory entry, do the following:

1 Select the appropriate directory entry in the table.

2 Click **Configure** in the **Tasks** panel.

3 Change the directory entry parameters as required (see parameter descriptions in section 6.12.5.1).

4 Click **OK**.

6.12.5.3 Viewing Directory Entry Details

You can view the configuration of a directory in **Monitor Mode**. Do the following:

1 Select the appropriate directory entry in the table.

2 In the **Tasks** bar click **Show details**.

The directory entry data is displayed in the detail panel.

3 Click **Cancel** to close the directory entry detail panel.

6.12.5.4 Deleting Directory Entries

Deleting directory entries is only possible in **Configuration Mode**. To delete one or more existing entries, do the following:

1 Select the appropriate entry/entries in the directory entry table by activating the corresponding checkbox(es).

2 In the **Tasks** pane, click **Delete**.

A confirmation dialog opens.

3 Click **OK** to confirm.

6.12.6 EASY MIGRATION FROM CORPORATE DIRECTORY (COMP. MODE) TO NEW CORPORATE DIRECTORY STRUCTURE

If there is a corporate directory (comp. mode) entry and a new corporate directory structure entry with identical settings, then the corporate directory (comp. mode) entry gets automatically removed.

Use case: Migration from old to new structure with provisioning files w/o manual configuration and to avoid double entries.

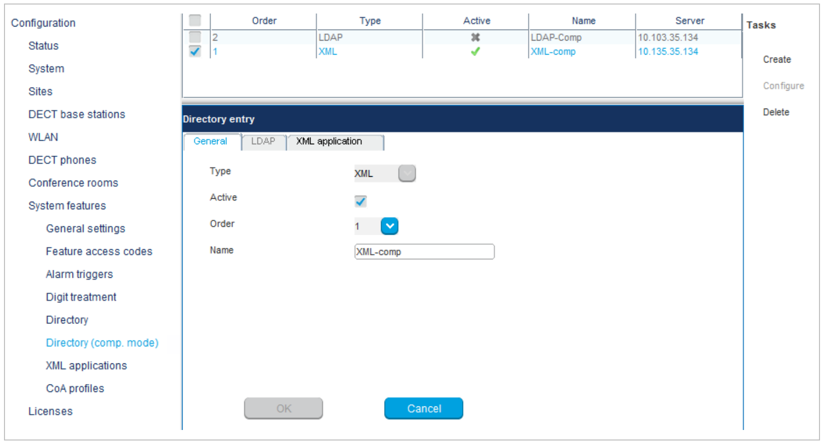
The following parameters is considered for comparison:

- **Directory type (LDAP, XML)**
- **Name**
- **Server**
- **Path**

6.12.7 “DIRECTORY (COMP. MODE)” MENU

With the introduction of XSI directory support in SIP-DECT 6.2, the underlying database model for directory support in SIP-DECT has changed. To support backwards compatibility, the Directory (comp) page provides directory configuration and maintenance for existing SIP-DECT systems with LDAP or XML directory support.

The **Directory (comp. mode)** menu allows configuration of LDAP or XML corporate directory services.



	Order	Type	Active	Name	Server
□	2	LDAP	✗	LDAP-Comp	10.103.35.134
☑	1	XML	✓	XML-comp	10.135.35.134

Type: XML
Active: ☑
Order: 1
Name: XML-comp

6.12.7.1 Creating New Directory Entries

Adding directory entries is only possible in **configuration mode**. You can configure up to five directory entries. To add a new entry, do the following:

4 In the **Tasks** panel, click **Create**.

The **New directory entry** panel opens and provides various tabs where the directory data must be entered.

5 Configure the directory entry (see parameter descriptions below).

6 Click **OK** to save your changes.

You can specify values for the following parameters in the **New directory entry** panel:

General tab

The following table describes the parameters on the **General** tab.

Parameter	Description
Type	Interface type supported by the directory server. Possible values: LDAP or XML.
Active	Enables or disables the directory entry on the DECT phone.
Order	Specifies where you want the directory to appear in the list.
Name	Name to be displayed for the directory (Latin-1 character set is supported). **Note**: If there is only one directory entry configured, this value is ignored when the user searches for a number in the telephone’s central directory. SIP-DECT 6.0 and later supports the “SIPProxy” placeholder for a directory entry name, in place of the current primary, secondary or tertiary SIP server address.

LDAP tab

The following table describes the parameters on the **LDAP** tab (only available when LDAP is selected as the directory type).

Parameter	Description
Search base	Location in the LDAP directory from which the search begins (e.g., ”ou=people, o=my com”). The configuration is valid for all DECT phones that support the LDAP directory feature. To make search requests unique for different users, the search base configuration can include placeholders that are replaced by user-specific values when submitting the LDAP request to a server. The following placeholders are defined: • “<TEL>” (for the user’s telephone number) • “<DESC1>” (for the user’s “Description 1” attribute) • “<DESC2>” (for the user’s “Description 2” attribute) • “SIPProxy” (for the current primary, secondary or tertiary SIP server address); supported for release 6.1 and later
Search type	Attribute on which searches are performed (**Surname** or **Given name**).
Display type	Display mode for search results (**Surname, First Name** or **Given name Surname**).
Server	IP address or FQDN of the directory server.
Port	Server port number. The default is 389. SSL (default port 689) is not supported. Windows Active Directory Server uses port 3268.
User name	Name of the account for directory server access, if required.
Password	Password for directory server access, if required. Confirm in the next field. **Note**: If no user/password is specified, an anonymous bind takes place. SIP-DECT supports LDAP simple bind.
Server search timeout	Interval (in seconds) during which the OMM waits for search results from the LDAP server (1 – 10 seconds).

XML application tab

The following table describes the parameters on the **XML application** tab (only available when XML is selected as the directory type).

Parameter	Description
Protocol	Transfer protocol used to communicate with the XML directory server (**HTTP** or **HTTPS**).

Parameter	Description
Port	Server port number. Default is 80 for HTTP, and 443 for HTTPS.
Server	IP address or FQDN of the directory server.
User name	Name of the account for directory server access, if required.
Password	Password for directory server access, if required. Confirm the password in the next field.
Path (and parameters)	URL (with parameters, if required) to the XML directory on the XML directory server.

6.12.7.2 Changing a Directory Entry

Changing directory entry is only possible in configuration mode. To change the configuration of an existing directory entry, do the following:

1 Select the appropriate directory entry in the table.

2 Click **Configure** in the **Tasks** panel.

3 Change the directory entry parameters as required (see parameter descriptions above).

4 Click **OK** to save your changes.

6.12.7.3 Viewing Directory Entry Details

You can view the configuration of a directory in **Monitor Mode**. Do the following:

1 Select the appropriate directory entry in the table.

2 In the **Tasks** bar click **Show details**.

The directory entry data is displayed in the detail panel.

3 Click **Cancel** to close the directory entry detail panel.

6.12.7.4 Deleting Directory Entries

Deleting directory entries is only possible in **Configuration Mode**. To delete one or more existing entries, do the following:

1 Select the appropriate entry/entries in the directory entry table by activating the corresponding checkbox(es).

2 In the **Tasks** bar click **Delete**.

A confirmation dialog opens.

3 Click **OK** to confirm.

6.12.8 "XML APPLICATIONS" MENU

The SIP-DECT XML terminal interface allows external applications to provide content for the user on the Mitel 600 DECT phone display. To make the XML terminal interface applications available to the DECT phone user, the relevant hooks must be configured in the **XML applications** menu.

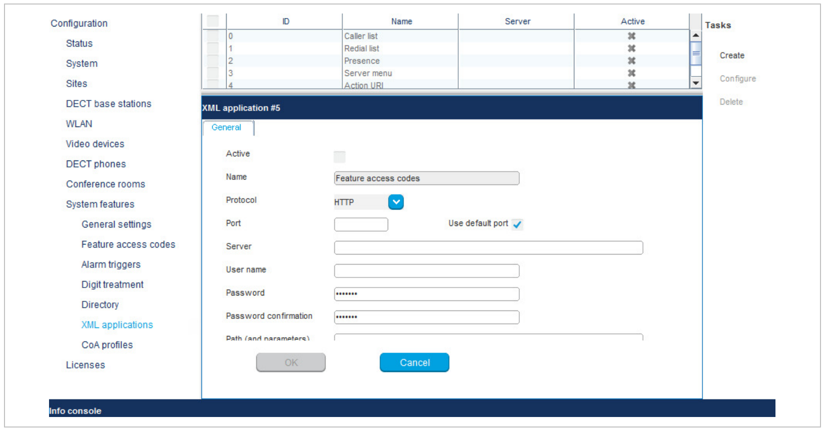
There are 15 predefined hooks and 10 hooks which can be freely defined. For a full list of the predefined hooks and their descriptions, see section 5.9.5.

These hooks can be activated or deactivated but not deleted. Up to 10 additional hooks can be created dynamically.

> **Please note:** "Caller list" and "Redial list" replace the local caller and redial lists of the Mitel 600 if activated. These XML hooks can also be used to enable the centralized call log feature (MX-ONE systems only). Additionally the list access must be set to "Automatic" or "PBX" on the DECT phone in the "Settings > List access" menu. If the list access is set to "Local", the local list is used by the DECT phone.

Note: An XML directory entry is also read-only listed in the XML applications menu. For information on configuring XML directories please see section 6.12.5.1.

An activated hook becomes available on a DECT phone (including the corresponding menu entry) after the next DECT location registration of the DECT phone. This can be forced by switching the DECT phone off and on. The same applies if a hook is deactivated.



ID	Name	Server	Active
0	Caller list		✖
1	Redial list		✖
2	Presence		✖
3	Server menu		✖
4	Action URI		✖

XML application #5

Active □

Name: Feature access codes

Protocol: HTTP

Port: Use default port ✓

Server:

User name:

Password: •••••••

Password confirmation: •••••••

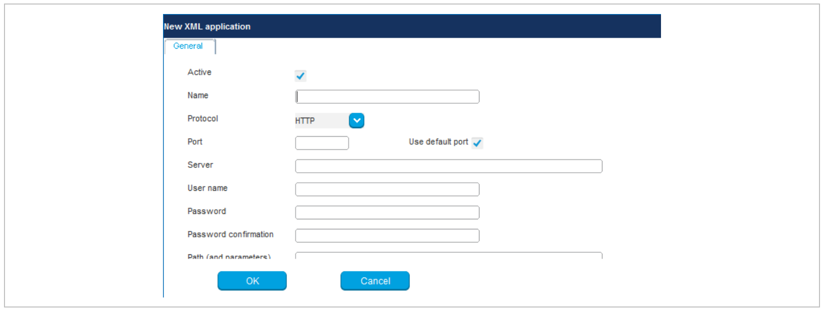
Path (and parameters):

The tasks you can perform in the **XML applications** menu are mode-dependant.

Configuration mode	Monitor mode	See section
Create: Create new XML hooks		6.12.7.1
Configure: Configure selected XML hook in detail panel		6.12.7.2
	Show details: Shows selected XML hook in detail panel	6.12.7.3
Delete: Delete selected XML hook		6.12.7.4

6.12.8.1 Creating a New XML Hook

In addition to the 15 predefined XML hooks, you can create up to 10 additional XML hooks. You can only add XML hooks in **Configuration Mode**.



New XML application

General

Active ☑

Name

Protocol HTTP

Port

Use default port ☑

Server

User name

Password

Password confirmation

Path (and parameters)

To add an XML hook, do the following:

1 In the **Tasks** bar click on **Create**.

The **New XML application** panel opens.

2 Specify values for the following XML hook parameters:

- **Active**: This setting activates or deactivates a configured XML application entry.
- **Name**: The predefined hooks have fixed predefined names. A name must be configured for the free defined hooks.
- **Protocol**: Select the protocol HTTP or HTTPS.
- **Server**: Enter the IP address or the name of the server which provides the XML content.

Note: SIP-DECT 6.0 and later supports “SIPProxy” placeholders for XML Server application URLs within SIP redundancy setups. In cases where applications are located on a SIP server, it is necessary to address XML applications by using the current primary, secondary or tertiary SIP server address. In those cases, the “SIPProxy” placeholder can be used as server input.

- **User name**: Enter the login user name if an authentication is required by the server.
- **Password, Password confirmation:** Enter the password if the authentication is required by the server.
- **Path (and parameter)**: Enter the path and query of the URI. For “Feature access codes translation”, the **Path** settings contains placeholders for the queried translation: {subsc} = Number, {ppn} = Device ID, {fac} = FAC.

3 Click **OK** to save your changes.

6.12.8.2 Modifying an XML Hook

You can only modify XML hooks in **Configuration Mode**.

To change the configuration of an existing XML hook, do the following:

1 Select the appropriate XML hook in the table.

2 In the **Tasks** bar, click **Configure**.

3 Edit the XML application parameters (described above) as necessary. You cannot change the name of a predefined XML hook.

Note: SIP-DECT 7.0 and later supports centralized call logs for systems using the MX-ONE call server. To enable this feature, you must enter ”**CSIntegration?object=history**" as the value for the **Path** parameter. This applies to both the **Caller list** and **Redial list** predefined XML hooks.

Refer the description comment in chapter 5.9.5s.

4 Click **OK**.

6.12.8.3 Viewing XML Hook Details

You can view the configuration of an XML hook in **Monitor Mode**. Do the following:

1 Select the appropriate XML hook in the table.

2 In the **Tasks** bar click on the **Show details** command.

The user account data is displayed in the user account detail panel.

3 Click **Cancel** to close the XML hook detail panel.

6.12.8.4 Deleting XML Hooks

You can only delete XML hooks in **Configuration Mode**. You cannot delete any predefined XML hooks.

To delete an XML hook, do the following:

1 Select the appropriate XML hook(s) in the table by activating the corresponding checkbox(es).

2 In the **Tasks** bar, click **Delete**.

A confirmation dialog opens.

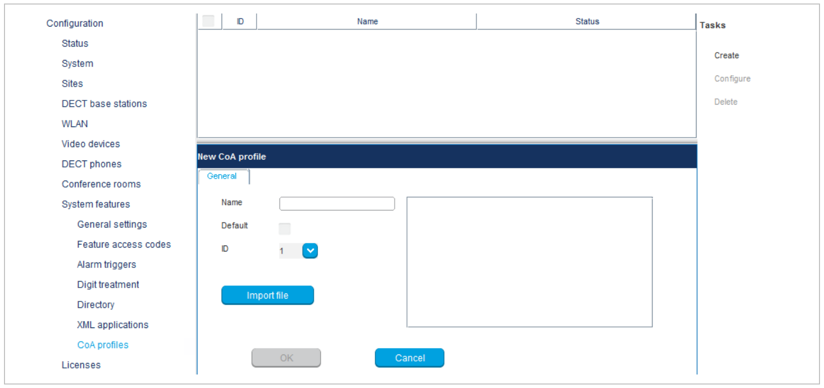
3 Click **OK** to confirm.

6.12.9 “COA PROFILES” MENU

SIP-DECT 6.0 and later supports central configuration over the air (CoA) for Mitel 602 DECT phones. The CoA profiles page lists the available CoA profiles that can be downloaded to the DECT phones.

> **Note:** The profiles generated by the user_common.cfg configuration file are also listed in this window. When managed with OMP, they can be overwritten when the user_common.cfg configuration file is reloaded. The maximum download size is 4kB.

You can import CoA profiles via the **CoA Profiles** menu. Once you have imported the profiles, you can assign them to specific DECT phone users.



Name

Default □

ID 1

To create a new CoA profile:

1 Click **Create** under the Tasks list on the right-hand side of the **CoA profiles** window.
The **New CoA profile** dialog opens.

2 Configure the settings for the CoA profile:

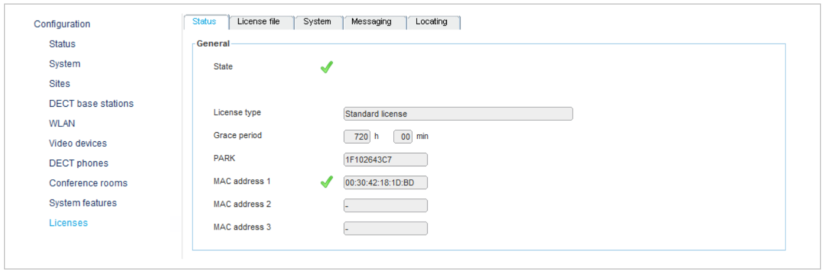
- **Name**: Specify a name for the CoA profile
- **Default**: Indicate whether this is the default CoA profile to be used
- **ID**: Select an ID for the CoA profile from the drop-down menu.

3 Click **Import file** to select the CoA file to import.

The **CoA profiles** page displays the new CoA profile in the table.

6.13 “LICENSES” MENU

The **Licenses** pageprovides an overview of licenses currently in use. In **Configuration Mode**, you can also import a license file.



State ✓

License type: Standard license

Grace period: 720 h 00 min

PARK: 1F102643C7

MAC address 1 ✓ 00:30:42:18:1D:BD

MAC address 2: -

MAC address 3: -

The license information is displayed in the following tabs:

- **Status**: Shows general license information.
- **License file**: Allows import of a license file
- **System**: Shows system license status.
- **Messaging**: Shows Integrated Messaging and Alerting Service (IMA) license status.
- **Locating**: Shows Locating license status.

“General” tab

The General tab displays general information about the current system license.

“License file” tab

The License file tab allows you to import a license file (only possible in **Configuration Mode**).

1 Click the **File** button to select the path and file name where the license file is stored.

2 Click the **Import** button.

“System” tab

The “System” tab provides OM System license information. This includes supported software version and number of licensed DECT base stations (RFPs) compared to number of connected DECT base stations.

“Messaging” tab

The “Messaging” tab provides OM Messaging and Alerting license information.

“Locating” tab

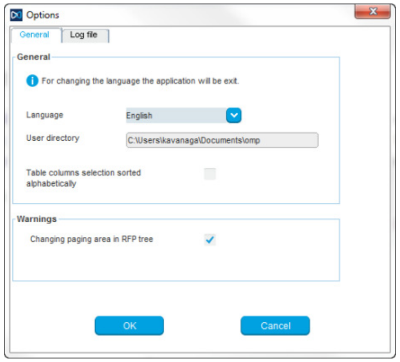
The “Locating” tab provides OM Locating license information.

6.14 “GENERAL” MENU

The **General** menu is available in all program situations. It contains following submenus:

- **Exit**: Selecting this menu entry opens the exit dialog to close the OMP.
- **Options**: Selecting this menu entry opens the **Options** dialog (see below).

“Options” - “General” tab



Options

General | Log file

General

For changing the language the application will be exit.

Language: English

User directory: C:\Users\kavanaga\Documents\omp

Table columns selection sorted alphabetically □

Warnings

Changing paging area in RFP tree ☑

OK | Cancel

Language: You can select the OMP language. After changing the language, the OMP is automatically closed and must be started again.

The field **User directory** shows the path where the following files are saved if necessary:

- System dump file “sys_dump.txt”
- Expert console log file “spy.log” when the application terminates
- Exception log file “spy_trace_<date>_pxxx” in case of a Java exception, file name extension “xxx” ranges from 000 to 999

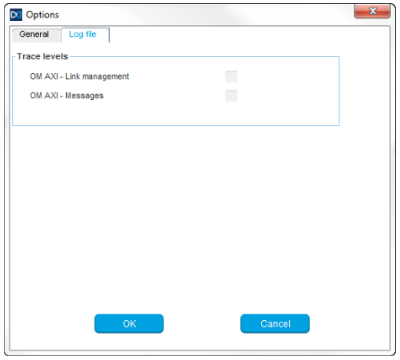
In the **Warnings** section you can activate/deactivate the display of warning messages in the OMP.

Notes on log files

The mechanism for creating the log files is the same as the PC OMM spy log mechanism, what means:

- The maximum size of the log file is 1 GB
- 1000 log files per day at maximum
- Only the 30 newest created log files are kept, older ones are removed automatically
- Log files older than 6 days are removed

“Options” - “Log file” tab



Options

General | Log file

Trace levels

OM AXI - Link management □

OM AXI - Messages □

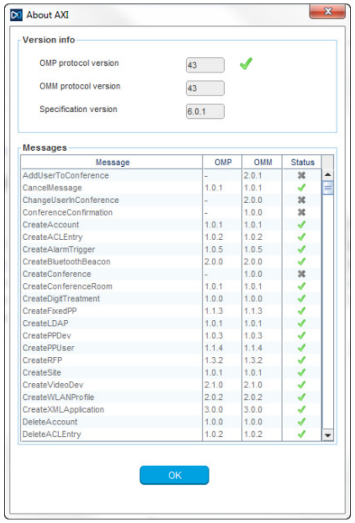
OK | Cancel

In the **Log file** tab you can enable several trace levels.

6.15 “HELP” MENU

The **Help** menu is available in all program situations. It contains following submenus:

- **Info**: Selecting this menu entry displays the End User License Agreement (EULA).
- **About AXI**: Selecting this menu entry displays the About AXI dialog. This dialog compares the protocol version numbers which are provided by the OMM with the protocol version numbers supported by the OMP. The warning icons ⚠ or ✖ show a version mismatch. A version number “-” means the protocol element is not used by OMP.



OMP protocol version 43 ✓

OMM protocol version 43

Specification version 6.0.1

Messages

Message	OMP	OMM	Status
AddUserToConference	-	2.0.1	✖
CancelMessage	1.0.1	1.0.1	✓
ChangeUserInConference	-	2.0.0	✖
ConferenceConfirmation	-	1.0.0	✖
CreateAccount	1.0.1	1.0.1	✓
CreateACLEntry	1.0.2	1.0.2	✓
CreateAlarmTrigger	1.0.5	1.0.5	✓
CreateBluetoothBeacon	2.0.0	2.0.0	✓
CreateConference	-	1.0.0	✖
CreateConferenceRoom	1.0.1	1.0.1	✓
CreateDigitTreatment	1.0.0	1.0.0	✓
CreateFixedPP	1.1.3	1.1.3	✓
CreateLDAP	1.0.1	1.0.1	✓
CreatePPDev	1.0.3	1.0.3	✓
CreatePPUser	1.1.4	1.1.4	✓
CreateRFP	1.3.2	1.3.2	✓
CreateSite	1.0.1	1.0.1	✓
CreateVideoDev	2.1.0	2.1.0	✓
CreateWLANProfile	2.0.2	2.0.2	✓
CreateXMLApplication	3.0.0	3.0.0	✓
DeleteAccount	1.0.0	1.0.0	✓
DeleteACLEntry	1.0.2	1.0.2	✓

- **About OMP**: Selecting this menu entry displays the OMP version info and copyright.

7 CONFIGURATION AND ADMINISTRATION

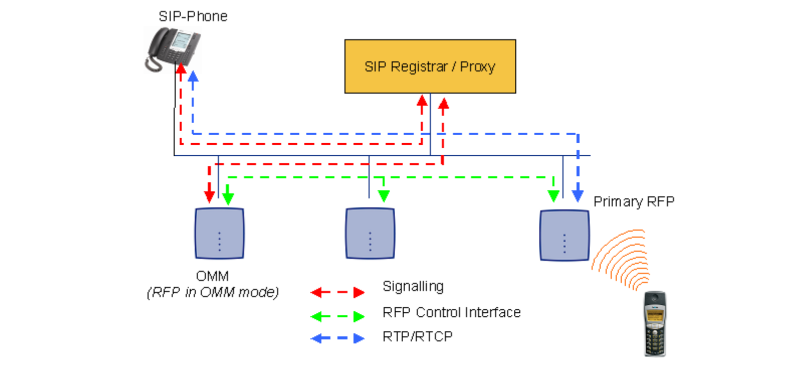
This section provides detailed information on various configuration and administration aspects of the SIP-DECT solution.

7.1 IP SIGNALING AND MEDIA STREAM

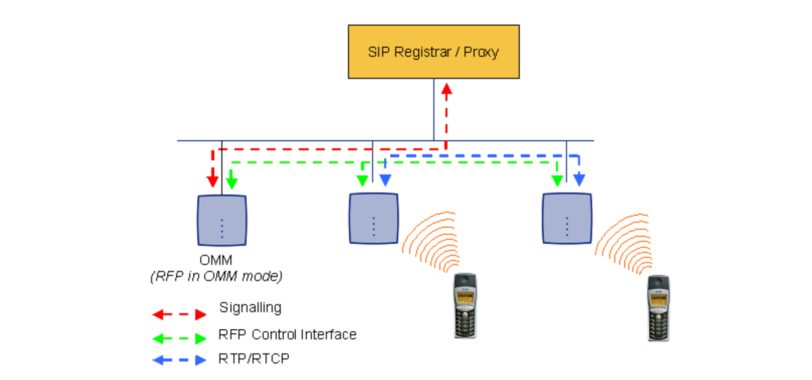
To establish a call between an IP Phone and a DECT phone (e.g. Mitel 600), the following IP streams must be established:

- A signaling channel to and from the SIP phone.
- A signaling channel to and from the OMM.
- A control interface between the OMM and the RFP that has a connection to the DECT phone (known as the primary RFP).
- A Real Time Protocol (RTP) / Real Time Control Protocol (RTCP) connection between the SIP phone and the primary RFP.

The following figure illustrates this scenario.

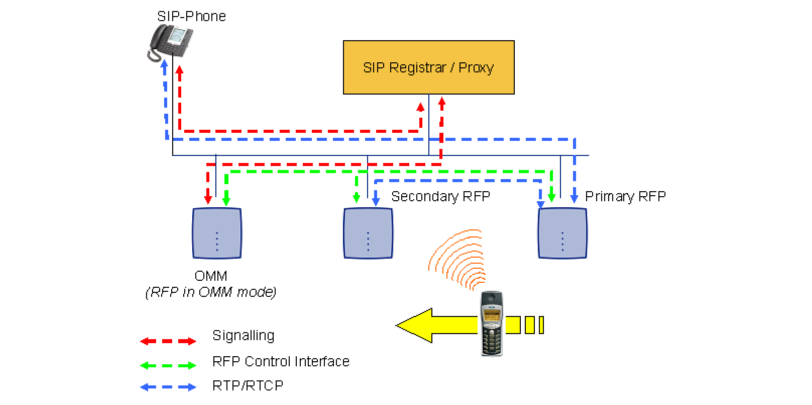


To establish a call between two DECT phones, the same IP streams must be established like in the scenario before, except the IP phone is not involved. The following figure illustrates this scenario.

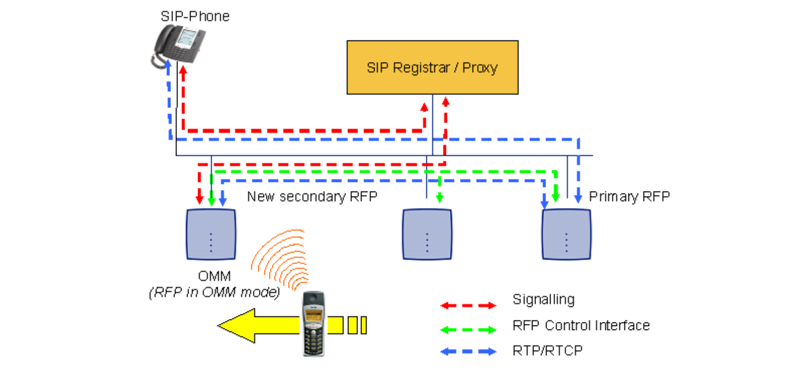


A call from one DECT phone to another that resides on the same RFP will loop back within the RFP if no media gateway is involved. So the call will not pass through to the Local Area Network (LAN). Although the voice packets will not impact LAN traffic, signal packets will.

If the DECT phone user is moving, the DECT phone detects that another RFP has a better signal strength and, therefore, it starts the handover process. The media stream from the IP phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the secondary RFP, as shown in the following figure.



As the DECT phone user moves into the next RFP zone of coverage, the DECT phone detects that the RFP has a better signal strength. Again the media stream from the SIP phone cannot move to the secondary RFP, so the primary RFP uses the LAN to direct the voice to the new secondary RFP.

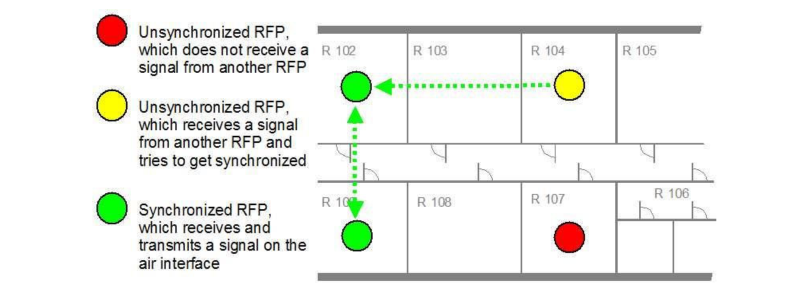


7.2 DECT BASE STATION SYNCHRONIZATION

To guarantee a seamless handover if a caller moves from one DECT base station zone of coverage to another DECT base station zone of coverage, an accurate synchronization of the DECT base stations is necessary.

The DECT base stations are synchronized over the air interface. The first DECT base station to complete startup transmits a signal on the air for the other DECT base stations to synchronize from. If a DECT base station gets in sync, it transmits a signal on the air and becomes the sync source for the next DECT base station. Only DECT base stations that can receive a synchronization signal become synchronized.

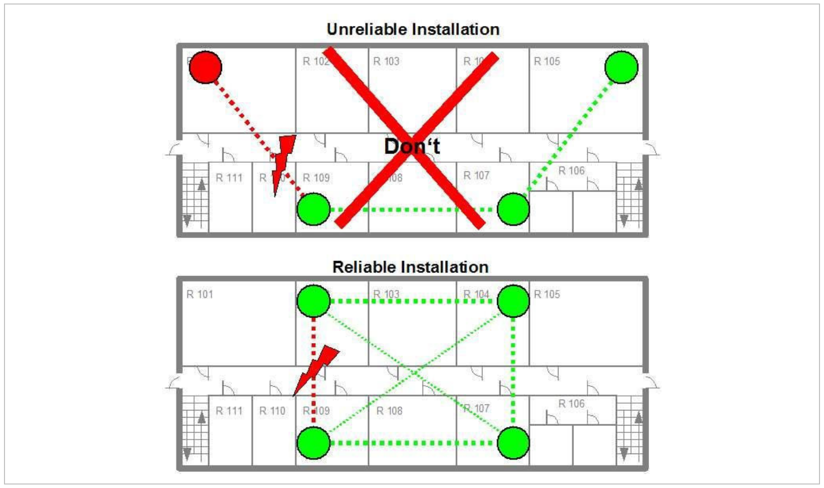
For the DECT base station to sync to another DECT base station, the signal strength cannot drop below -70 dBm. You must consider this requirement during the site survey.


Unsynchronized RFP, which does not receive a signal from another RFP
Unsynchronized RFP, which receives a signal from another RFP and tries to get synchronized
Synchronized RFP, which receives and transmits a signal on the air interface
R 102
R 103
R 104
R 105
R 106
R 107
R 108
R 109

As long as a DECT base station is not in sync, no calls can be established using this DECT base station.

If a DECT base station loses the synchronization, the DECT base station does not accept new calls ("busy bit"). There is a delay of maximum 3 minutes until the active calls on this DECT base station are finished. Then it tries to get synchronized again.

A SIP-DECT installation is more reliable if a DECT base station can receive the signal from more than only one DECT base station because the other signals are also used for synchronization.



The sync-over-air solution is very reliable because all existing redundant paths are used for synchronization. Thus, hardware tolerances have only very little influence. No DECT base station has a key position. Only unfavorable setups without redundant synchronization paths can cause problems.

Sometimes DECT base stations do not need to be synchronized (e.g. if they are in different buildings). These DECT base stations can be put into different clusters. DECT base stations in different clusters are not synchronized with each other. Different clusters start up at the same time independently.

7.2.1 INITIAL SYNCHRONIZATION PROCEDURE

To avoid synchronization problems and to speed up the synchronization on system startup, an initial synchronization procedure is used. For every cluster the following synchronization stages are defined.

- Synchronization stage 0
  - If at least one preferred DECT base station was configured, the synchronization process waits up to 30 seconds for an incoming startup message of such a preferred DECT base station. Receiving a message will finishing stage 0 and the synchronization process jumps to stage 1.
  - If no message is received within 30 seconds, this stage will be terminated and the next stage begins.
  - If no preferred DECT base station was configured, this stage is ignored.
- Synchronization stage 1
  - If a preferred DECT base station was determined in stage 0, this one becomes the synchronization source for the subsequent DECT base stations. Otherwise the first DECT base station that sends a startup message becomes the synchronization source for the subsequent DECT base stations.
  - In this stage, only DECT base stations reporting an RSSI value better than -65 dBm are permitted to perform synchronization.
  - If a DECT base station has completede its synchronization, this DECT base station will be also a synchronization source for other upcoming DECT base stations.
  - The initial timeout for this stage is 30 seconds. Whenever a DECT base station has finished its synchronization in this stage a new stage timeout value is calculated.
  - If no DECT base station comes up within the timeout time or if all the upcoming DECT base stations do not fit the RSSI threshold, this stage will be terminated and the next stage begins.
- Synchronization stage 2
  - The behavior of this stage is identical to stage 1, but an RSSI threshold value of -70 dBm is significant.
- Synchronization stage 3
  - The behavior of this stage is identical to stage 1, but an RSSI threshold value of -75 dBm is significant.
- Synchronization finished
  - No more RSSI threshold value is significant. All DECT base stations that failed the stage conditions above are now permitted to perform synchronization.

The last level “synchronization finished” will be achieved either all registered DECT base stations of this cluster are synchronized or the timer of stage 3 expires.

7.2.2 CHECKING THE SYNCHRONIZATION OF A NETWORK

For every cluster a periodically check of the synchronization of the network is done. If the network is split into at least two subnets, all the RFPs of the lesser subnet(s) will be resynchronized. While doing initial synchronization procedure this check is deactivated. You can check the DECT base station synchronization from the **Sync view** menu of the OM Management Portal (OMP), see section 6.7.6.

7.3 DECT BASE STATION CHANNEL CAPACITY

The DECT base station has 12 available time slots on air; eight can have associated DSP/media resources for media streams. All DECT time slots are used for control signaling, software download over air, messaging and bearer handover independent of associated DSP/media resources.

If all eight media stream channels are used, the DECT base station announces a “busy bit”. In that case, the DECT phones determine whether another DECT base station has an appropriate signal strength. If so, the DECT phone performs a handover to that DECT base station. Once the handover is complete, the DECT base station lowers its “busy bit”.

Whenever the busy state is announced a log entry is made to the system logs. If the announcement of busy raises in a specific area, an additional DECT base station should be installed to double the number of media streams available for calls.

Notes on Hi-Q connections

Each Hi-Q connection uses twice the capacity of conventional narrowband on the DECT air interface. Due to this fact, four Hi-Q connections (instead of eight) can be established via one DECT base station.

It is not possible to have DECT XQ audio combined with Hi-Q audio within the same connection.

7.4 NETWORK INFRASTRUCTURE PREREQUISITES

To establish and maintain an SIP-DECT installation, a network infrastructure is assumed, which comprises at least the following components:

- DECT base stations
- DECT phones
- IP PBX/media server (e.g. Asterisk)
- TFTP server

Depending on the operational modes the following services should be provided:

- DHCP
- TFTP
- SNTP
- DNS
- LDAP
- Syslog daemon

Notes on network infrastructure prerequisites

- In NA outdoor RFPs may only be installed with the antennas shipped with the units. No other antennas or cabling are permitted. In EMEA the outdoor RFPs are shipped without antennas and you may use the units with one of the optional antennas (separate order no.).
- A TFTP server is no longer required for boot of an RFP 35/36/37 IP or RFP 43 WLAN.
- TFTP, FTP(S), HTTP(S), SFTP are supported for RFP 35/36/37 IP or RFP 43 WLAN software update.

7.5 SIP-DECT STARTUP

This section contains detailed information on the startup (booting) process of the SIP-DECT solution.

For booting an RFP 32/34 or RFP 42 WLAN, there must be at least one TFTP server on the attached network to load the OMM/RFP application software.

RFP 35/36/37 IP or RFP 43 WLAN uses the internal flash to start the boot image. A fileserver is only needed for software update over the network.

The essential network settings can be alternatively:

- Communicated by a DHCP server at startup time.
- Configured on the RFP with the OM Configurator tool (see section 7.6). The settings made by the OM Configurator will be saved permanently in the internal flash memory of each OMM/RFP.

7.5.1 TFTP AND DHCP SERVER REQUIREMENTS

TFTP server requirements

The DECT base station obtains the boot image file from a TFTP server. The requirement list for the used TFTP server is defined as follows:

- The support of RFC 1350 /1/ is mandatory.
- To accelerate the download of a boot image file for older 2nd generation DECT base stations, it is possible to increase the packet size of the transmitted TFTP packets from 512 bytes per packet to 1468 bytes per packet. To use this optional feature, the TFTP server must support RFC 2347 /3/ and RFC 2348 /4/.
- To reduce the overall download time of the older 2nd generation DECT base stations in a system, it is possible to use TFTP multicast download. To use this optional feature, the TFTP server must support RFC 2090 /2/ and RFC 2349 /5/.

To use the TFTP multicast option, the attached network must support multicast too. Furthermore a support of IGMP, RFC 2236 /6/ is required.

Note: If many DECT base stations loading the boot image simultaneously, the network load could increase significant. To balance the network load or for backup reasons, it is possible to configure more than one TFTP server in a network.

DHCP server requirements

A DHCP server needs to support RFC 2131 /9/. The TFTP and DHCP server need not to reside on the same host.

7.5.2 BOOTING STEPS

Booting is performed in two steps:

1 Starting the boot process.

2 Starting the application.

Booter startup

On startup each DECT base station tries to determine its own IP address and other settings of the IP interface from the configuration settings in the internal flash memory. If no settings are available or these settings are disabled, the DECT base station tries to determine these settings via DHCP. Depending on the DECT base station type, the DECT base station software is to be loaded:

- A 3rd generation DECT base station gets the application image from internal flash memory.
- An older 2nd generation DECT base station only has a small standalone application built into the flash. This software realizes the so-called net boot process. The RFP gets the application image file from the TFTP server.

Application startup

After starting the application image, the RFP software checks the local network settings in its internal flash memory. If no settings are available or if they are disabled, the RFP software starts a DHCP client to determine the IP address of the OMM and other application startup settings.

The RFP software acquires the OMM IP address:

- within the local network settings, if active

- through DHCP request
- DECT base station configuration file (see 7.7.7)

If the IP address of the actual RFP device matches one of the acquired OMM IP addresses, the DECT base station software continues in OMM mode. Otherwise, the DECT base station runs as normal DECT base station without OMM mode.

Note: Only 3rd generation DECT base stations are able to run in OMM mode while older 2nd generation DECT base stations cannot function as OMM.

7.5.3 BOOTER STARTUP

The SIP-DECT DECT base station software includes a booter with the following features:

- VLAN can be configured via the OM Configurator without a static IP configuration. This means that the first DHCP request will be done by using VLAN.
- To balance the network load with older 2nd generation RFP devices, up to three TFTP servers can be configured. This can be done using the OM Configurator (local setting) or using the DHCP option 150. Before starting the download, the TFTP server will be selected randomly by the booter. **But**, if the option "Preferred TFTP server" was set by the OM Configurator, the option "TFTP server address" will specify the TFTP server to use. No randomly selection will be done in this case.
- Older 2nd generation RFPs only: to reduce the number of TFTP packets sent by the TFTP server, the packet size can be increased. This will be done by using a TFTP option (see 7.5.1 "TFTP server requirements").
- Older 2nd generation RFPs only: Multicast TFTP download is possible if the TFTP server and the connected network support this.
- To indicate the actual state of the booter, the LEDs of the RFP will be used (see 7.5.5).

7.5.3.1 DHCP Client

Within the initial boot process the DHCP client supports the following parameters:

• IP address	mandatory
• Net mask	mandatory
• Gateway	mandatory
• Boot file name	mandatory for older RFPs
• TFTP server	mandatory for older RFPs
• Public option 224: "OpenMobility" / "OpenMobilitySIP-DECT"	mandatory
• VLAN-ID	optional
• TFTP server list	optional

7.5.3.1.1 DHCP Request

The DHCP client sends the vendor class identifier (code 60) "OpenMobility3G" (3rd generation RFPs) or "OpenMobility" (older 2nd generation RFPs) and requests the following options in the parameter request list (code 55):

- Subnet mask option (code 1)
- Router option (code 3)
- VLAN ID option (code 132)
- TFTP server list (code 150)
- Public option 224 (code 224) *(string "OpenMobility" or "OpenMobilitySIP-DECT")*
- Public option 225 (code 225) *(*VLAN ID, not relevant for SIP-DECT)
- Public option 226 (code 226) *(not relevant* for SIP-DECT)

7.5.3.1.2 DHCP Offer

The DHCP client selects the DHCP server according to the following rules:

- The **public option 224** (**code 224**) has a value equal to the string "OpenMobility",

or

- The **public option 224** (**code 224**) has a value equal to the string "OpenMobilitySIP-DECT".

If none of the two rules above match, the DHCP offer is ignored.

Information retrieved from the DHCP offer:

- The IP address to use is taken from the **yiaddr** field in the DHCP message.
- The IP net mask is taken from the **subnet mask option (code 1)**.
- The default gateway is taken from the **router option (code 3)**.
- The TFTP server IP address is taken from the **siaddr** field in the DHCP message and additionally DHCP option 150, if available.
- The boot image filename is taken from the **file** field in the DHCP message, if this field is empty, the default filename is used.

7.5.3.1.3 Retries

If the DHCP client does not get an appropriate DHCP offer, a new DHCP request is send after 1 second. After 3 DHCP requests are sent the DHCP client will sleep for 60 seconds. During this time the booter accepts a local configuration with the OM Configurator.

This cycle repeats every 3 minutes until either **all** the required DHCP options are provided or the system is manually configured using the OM Configurator tool.

7.5.3.2 TFTP Client

The TFTP client will download the application image from the TFTP server. Both TFTP server and the name of the application image are supplied via the DHCP client. The application image is checksum protected.

Downloading the application image via TFTP is mandatory for older 2nd generation RFPs only. 3rd generation RFPs will load the application image from the internal flash, and (if configured) also download the application image via TFTP for update.

7.5.3.3 Booter Update

With older second generation RFPs, each application software image comes with the latest released booter software. The application software will update the booter automatically. With third generation RFPs, the booter will only be updated if you update the software.

If you downgrade the RFP's application software image to an older release, the booter does not downgrade automatically. In addition, if you want to use the OM Configurator tool (see 7.7), the OM Configurator version must match the booter software version.

7.5.4 APPLICATION STARTUP

After successfully starting the application software, the DECT base station checks the local network settings in its internal flash. If no settings are available or if they are disabled, it starts a DHCP client to determine the IP address of the OMM and other application startup settings.

7.5.4.1 DHCP Client

The DHCP client is capable of receiving broadcast and unicast DHCP replies. Therefore the flags field is `0x0000`. The DHCP request contains the well-known magic cookie `(0x63825363)` and the end option `(0xFF)`.

Parameters

The following parameters are supported within this step:

Option / Field	Meaning	Mandatory
yiaddr	IP address of the IP-RFP	yes
siaddr	Parameter named “Boot Server Host Name” with value as the IP address of the TFTP server	no (3G RFPs) yes (older 2G RFPs)
file	Parameter named “Bootfile Name” with value of the path (optional) and name of the application image. For example “iprfp3G.dnld “ (3rd generation RFPs) or “iprfp2G.tftp” (older 2nd generation RFPs).	no (3G RFPs) yes (older 2G RFPs)
option 1	Subnet mask	no
option 3	Default Gateway	no
option 6	Domain Name Server	no
option 15	Domain Name	no
option 42	IP address of a NTP server	no
option 43	Vendor-specific options (see table below)	yes

Option / Field	Meaning	Mandatory
option 66	Provisioning URL for the OMM (ConfigURL). URL of an external server that provides configuration files for the Base Station(s) hosting the OMM. **Note**: In SIP-DECT 2.1 - 6.1, this option was used for the RFP Config file server. If you want to specify a URL for the RFP Config file server, use option 233 instead.	no
option 132	VlanId	no
option 150	TftpServerIpList	no
option 224	Parameter named magic_str must be set to value "OpenMobility" or "OpenMobilitySIP-DECT".	yes
option 226	Enabling 802.1X feature (set to 1).	no
option 233	URL that specifies the protocol, server and path to access the DECT base station configuration files (see section 7.9). For SIP-DECT 6.1 or earlier, this option takes priority over option 66 when set.	no
option 234	Provisioning URL for the OMM (ConfigURL). URL of an external server that provides configuration files for the Base Station(s) hosting the OMM.	no
option 236	This mode value determines which instance (OMM, RFP) shall use the given Provisioning URL (Option 43-2, 66 or 234). Valid values are: 1. The RFP shall use the given Provisioning URL. 2. The OMM and RFP shall use the given Provisioning URL. Else: The OMM shall use the given Provisioning URL.	no

Vendor specific options

The Vendor Specific Options consist of:

Vendor Specific Option	Meaning	Length	Mandatory
option 10	ommip1: Used to select the IP-RFP that hosts the Open Mobility Manager (OMM).	4	yes
option 14	syslogip: IP address of a Syslog Daemon	4	no
option 15	syslogport: Port of a Syslog Daemon	2	no
option 17 (SIP-DECT 5.0 and older)	Country: Used to select the country in which the OMM resides. This enables country specific tones (busy tone, dial tone, …).	2	no
option 18 (SIP-DECT 5.0 and older)	ntpservname: Name of a NTP Server	x	no

option 19	ommip2: Used to select a secondary IP-RFP that hosts the standby Open Mobility Manager (OMM). This option must be included if the OMM Standby feature is used (see section 7.15).	4	no
option 43 sub-option 1 (SIP-DECT 6.2 and later)	URL that specifies the protocol, server and path to access the DECT base station configuration files (see section 7.9).		no
option 43 sub-option 2	Provisioning URL for the OMM (ConfigURL). URL of an external server that provides configuration files for the Base Station(s) hosting the OMM.		no
option 43 sub-option 226	Enable 802.1x feature (set to 1).	1	no

Example

An example of the minimal contents for the Option 43 parameter value would be:

0a 04 C0 A8 00 01 where “C0 A8 00 01” represents “192.168.0.1” for the OMM IP.

The option 43 contains a string of codes in hex the format is “option number” “length” “value” in this example
0a = option 10 (ommip1)
04 = following value is 4 blocks long
C0 A8 00 01 = 192.168.0.1

If there is more than one option, add the next option at the end of the previous one. Depending of the DHCP server you must end the option 43 with FF.

Country specific tones (SIP-DECT 5.0 and older ONLY)

Tones for the following countries are supported:

Country code	Country		Country code	Country
1	Germany		15	Hungary
2	Great Britain		16	Poland
3	Switzerland		17	Belarus
4	Spain		18	Estonia
6	Italy		19	Latvia
7	Russia		20	Lithuania
8	Belgium		21	Ukraine
9	Netherlands		22	Norway
10	Czechoslovakia		24	Sweden
11	Austria		25	Taiwan
12	Denmark		100	North America
13	Slovakia		101	France
14	Finland		102	Australia

7.5.4.2 Configuration using DHCP

The DHCP client of the RFP family requests several parameters that are used to configure the RFP. The DHCP client vendor class identifier (option 60) is different for the different RFP generations:

- 3rd generation RFPs (RFP 35/36/37 IP / RFP 43 WLAN) use “OpenMobility3G”.
- Older 2nd generation RFPs (RFP 32/34 / RFP 42 WLAN use) “OpenMobility”.

BOOTP/DHCP Option	Meaning	Type	Remarks
siaddr	IP address of the TFTP server	4 octets	Optional for 3G RFPs for SW update; Mandatory for older 2G RFPs because of the NETBOOT process;
File	Path to the boot image server by the TFTP server	N octets	Optional for 3G RFPs for SW update; Mandatory for older 2G RFPs because of the NETBOOT process
150	TFTP server list	N * 4 octets	Only used by the NETBOOT process of older 2G RFPs
224	Magic String	“OpenMobility” or “OpenMobilitySIP-DECT”	The client uses this option to select the server, mandatory

* The magic string “OpenMobilitySIP-DECT” instead of “OpenMobility” (as defined in SIP-DECT 2.x) makes sure that a SIP-DECT software is loaded into the RFP 35/36/37 IP/ RFP 43 WLAN even an different, non-SIP-DECT SW is previously installed and running.

7.5.4.3 Selecting the Right DHCP Server

The DHCP client requests its own IP address using code 50. The DHCP client will select the DHCP server that offers the currently used IP address. Additionally the mandatory options must be offered otherwise the DHCP offer is ignored by the DHCP client.

If no matching reply was received, the DHCP client resends the request 2 times after 1 second. Then the DHCP client will wait for 1 minute before resending 3 requests again.

If the DHCP client cannot accept a DHCP offer within 30 minutes, the RFP is rebooted.

7.5.5 RFP LEDS

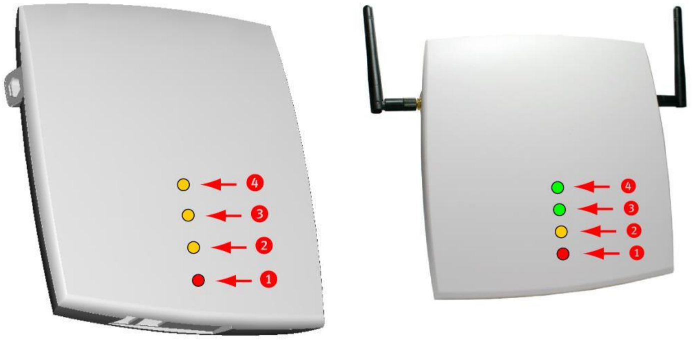
7.5.5.1 3rd Generation RFPs

- RFP 35 IP
- RFP 36 IP
- RFP 37 IP
- RFP 43 WLAN

7.5.5.1.1 LED States

RFP 32/34 IP
RFP 32/34 NA
RFP 35/36 IP

RFP 42 WLAN
RFP 43 WLAN



LED 1 Info / Booter; LED 2 System;
LED 3 DECT; LED 4 (unused)

LED 1 Info / Booter; LED 2 System
LED 3 DECT; LED 4 WLAN

7.5.5.1.2 Booter LED Status

RFP 35/36 IP, RFP 43 WLAN

The RFP 35/36 IP and RFP 43 WLAN booter uses LED1 for signaling its activity. After power up, the LED 1 (INFO) is red. The successful start of the boot image is signaled by the LED 1 turning orange.

RFP 32/34 IP, RFP 32/34 NA, RFP 42 WLAN

The following table illustrates the different meaning of the LEDs while the booter is active.

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
Booter	🟥 cont.		⬛	⬛	⬛	⬛	⬛	⬛	Power connected
	🟥 cont.		🟨 cont.		🟨 cont.		🟨 cont.		Wait for OMM Configurator Input
	🟥 1s	⬛ 1s	⬛	⬛	⬛	⬛	⬛	⬛	DHCP
	🟥 1,9s	⬛ 0,1s	🟨 cont.		🟨 cont.		🟨 cont.		DHCP failed, wait for OMM Configurator Input
	🟥 0,25s	⬛ 0,25s	⬛	⬛	⬛	⬛	⬛	⬛	TFTP download after DHCP
	🟥 0,25s	⬛ 0,25s	🟨 cont.		⬛	⬛	⬛	⬛	TFTP download after local configuration
	🟥 0,25s	⬛ 0,25s	⬛	⬛	🟨 cont.		⬛	⬛	TFTP download after DHCP Multicast
	🟥 0,25s	⬛ 0,25s	🟨 cont.		🟨 cont.		⬛	⬛	TFTP download after local configuration and multicast
	🟥 3,9s	⬛ 0,1s	🟨 cont.		🟨 cont.		🟨 cont.		TFTP failed, wait for OMM Configurator Input
Now, the kernel / application is running: LED1 will never be RED									

7.5.5.1.3 Application LED Status

The following tables illustrate the different meaning of the LEDs while the application is starting or active.

RFP 35/36 IP, RFP 43 WLAN

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
Kernel	🟨 cont.		⬛	⬛	⬛	⬛	⬛	⬛	kernel boot phase (inflator, …)
RFPM	🟨 1s	⬛ 1s							DHCP phase
	🟨 1,85s	⬛ 0,5s							DHCP failure (idle loop)
	🟨 0,5s	⬛ 0,5s							obtaining external configuration
	🟨 0,85s	⬛ 0,15s							external configuration failure
	🟩 cont.								Ready
	🟩 1,85s	🟨 0,15s							Up & running + RFP houses OMM

	LED1 (INFO)		LED2 (OMM / SYSTEM)		LED3 (DECT)		LED4 (WLAN)		
RFP general			1s	1s					OMM connect phase
			1,85s	0,15s					OMM connection failure (idle loop)
			cont.						Up & running (OMM connected)
			1,85s	0,15s					Up & running + OMM warning
			1,85s	0,15s					Up & running + OMM failure
RFP DECT					cont.				DECT not configured on this RFP
					1,85s	0,15s			DECT inactive (not synced yet)
					cont				DECT 'on air'
					1,85s	0,15s			DECT + call active
					1,85s	0,15s			DECT + call active +busy bit
RFP WLAN							cont.		WLAN not configured on this RFP
							1,85s	0,15s	WLAN inactive yet
							cont.		WLAN 'on air'
							1,85s	0,15s	WLAN + assoc. clients
							cont.		WLAN failure (e.g. 10 Mbit/s uplink)
Reboot request	cont.		cont.		cont.		cont.		RFP will reboot

7.5.5.2 4th Generation RFPs

- RFP 44
- RFP 45
- RFP 47 and RFP 47 DRC (Indoor and Outdoor Unit)
- RFP 48

See the section 1.2.1.1 RFP 4G DECT Base Station family for more information.

7.5.5.2.1 LED States

The following tables show the LED status of an RFP according to the different states.

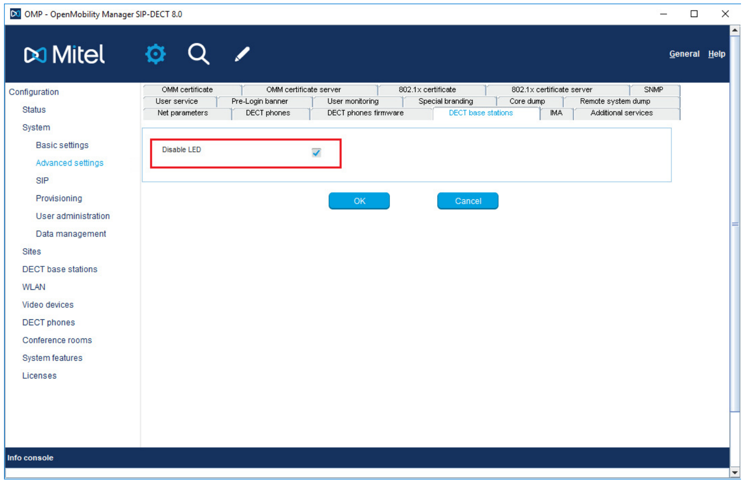
A red respectively orange colored field in the table means that the LED glows permanently in red or orange. A split field with e.g. the specification 1s/1s means that the LED is flashing with a frequency of one second LED red on and one second LED off. Grey means that the LED is off.

The new RFP family is equipped with one colored LED, which shows the individual states of the 4th generation RFP.

LED color/rhythm		Description
continuous		Booter phase
continuous		Kernel boot phase
1s	1s	Configuration phase
1,9s	0,1s	DHCP failure (idle loop)
continuous		System up and Running (with or without OMM)
1s	1s	OMM connection phase
continuous		OMM connected
1s	1s	DECT inactive (not synced yet)
continuous		DECT “on air”
continuous		WLAN “on air”
1s	1s	DECT inactive (not synced yet) + WLAN “on air”
continuous		DECT + WLAN “on air”
0,1 sec	0,1 sec	Button pressed: 0 sec < t < 3 sec = no action
0,1 sec	0,1 sec	Button pressed: 3 sec < t < 8 sec = Activate Cloud-Id
0,1 sec	0,1 sec	Button pressed: 8 sec < t < 10 sec = no action
0,1 sec	0,1 sec	Button pressed: 10 sec < t < 15 sec = Factory Reset
0,1 sec	0,1 sec	Button pressed: 15 sec < t < oo = no action

7.5.5.2.2 Turning Off the RFP 4G LED

Under the **DECT base stations** tab, select the check box to disable the LED for the active DECT and WLAN states.



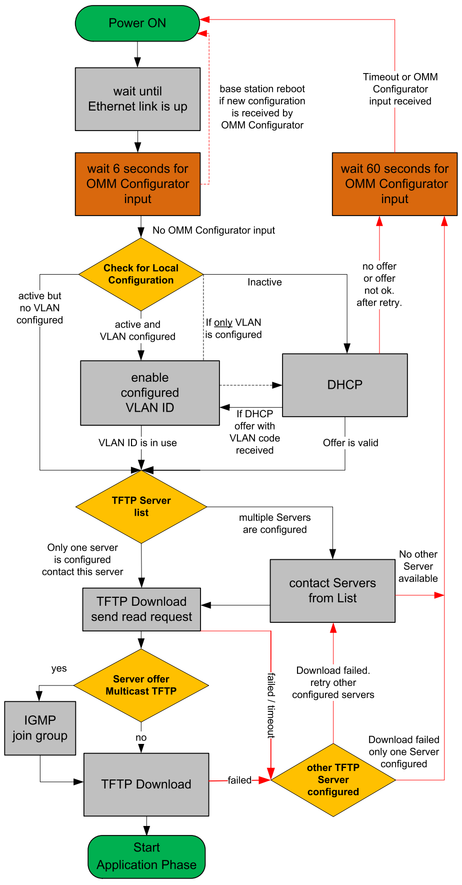
Disable LED ☑

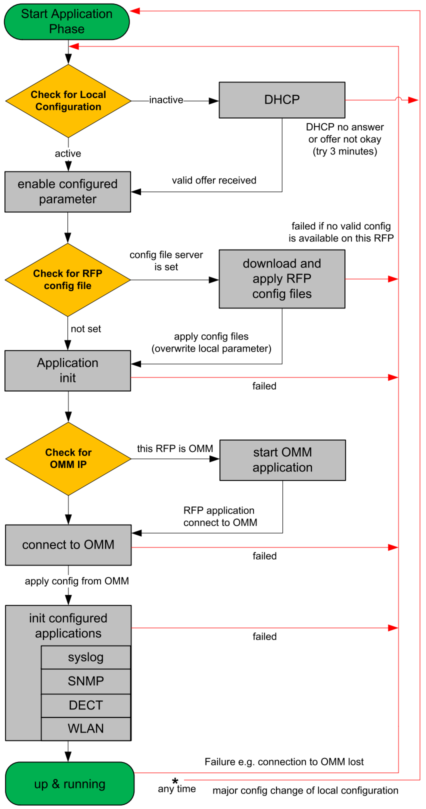
7.5.6 RFP 3G WITH SIP-DECT 7.X VERSUS RFP 4G WITH SIP-DECT 8.0

RFP 3G with SIP-DECT 7.x	RFP 4G with SIP-DECT 8.0
Cloud-ID Stick to appoint OMM RFP	Configuration button to appoint OMM RFP
Cloud-ID Stick to provide SDC SW	One SW for SIP-DECT and SDC Configuration button to switch to SDC
Cloud-ID Stick to provide Cloud-ID, PARK, DECT regulatory domain	Cloud-ID key is entered through OMM's Web service
Cloud-ID Stick to store backups beside other backup alternatives	Not applicable; other backup alternatives still available
Cloud-ID Stick to reset the RFP to factory defaults	Configuration button to initiate a reset to factory defaults
OMM provides SDC or SIP-DECT SW to connected RFPs to switch operational modes	Just one SW for both, SIP-DECT and SDC; OMM provides operational mode (**SDC or SIP-DECT)** to connected RFPs (SW update provided from OMM RFP still maintained)
SW update through USB stick beside other SW update options	Not applicable; other SW update options still available
Enables you to subscribe a DECT phone after applying the Cloud-ID SW and Cloud-ID from stick even w/o IP configuration	Enables you to subscribe a DECT phone after switching to SDC mode through configuration button and applying the Cloud-ID key through the OMM's Web service; an IP configuration through DHCP is required to apply the Cloud-ID key
Static IP configuration through DECT phone after applying the Cloud-ID SW and Cloud-ID from stick	Static IP configuration through DECT phone after switching to SDC mode through configuration button and applying the Cloud-ID key through the OMM's Web service
Enables you to subscribe DECT phone to determine the IP address assigned to the RFP/OMM	Use the Web browser script to access/find my SIP-DECT base station

7.6 STATE GRAPH OF THE START-UP PHASES

The following figure illustrates the start-up phase for older 2nd generation RFPs. 3rd generation RFPs use a similar start-up sequence, but they start with the application phase (see below).


Power ON
wait until Ethernet link is up
base station reboot if new configuration is received by OMM Configurator
Timeout or OMM Configurator input received
wait 6 seconds for OMM Configurator input
wait 60 seconds for OMM Configurator input
No OMM Configurator input
Check for Local Configuration
Inactive
no offer or offer not ok. after retry.
active but no VLAN configured
active and VLAN configured
If only VLAN is configured
enable configured VLAN ID
DHCP
If DHCP offer with VLAN code received
VLAN ID is in use
Offer is valid
TFTP Server list
multiple Servers are configured
Only one server is configured contact this server
contact Servers from List
No other Server available
TFTP Download send read request
failed / timeout
Download failed. retry other configured servers
yes
Server offer Multicast TFTP
IGMP join group
no
TFTP Download
failed
other TFTP Server configured
Download failed only one Server configured
Start Application Phase

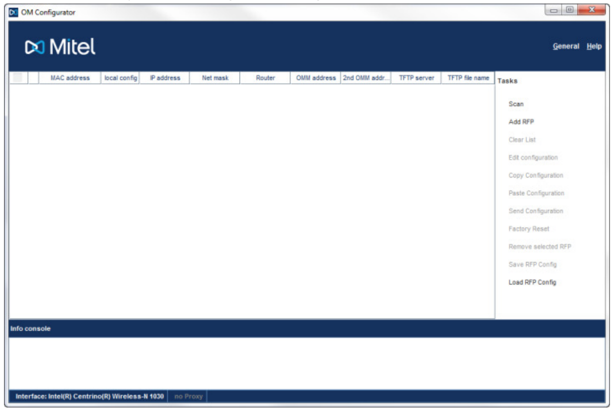

Start Application Phase
Check for Local Configuration
inactive
DHCP
DHCP no answer or offer not okay (try 3 minutes)
active
valid offer received
enable configured parameter
failed if no valid config is available on this RFP
config file server is set
Check for RFP config file
download and apply RFP config files
not set
apply config files (overwrite local parameter)
Application init
failed
Check for OMM IP
this RFP is OMM
start OMM application
RFP application connect to OMM
connect to OMM
failed
apply config from OMM
init configured applications
failed
syslog
SNMP
DECT
WLAN
Failure e.g. connection to OMM lost
up & running
*
any time
major config change of local configuration

7.7 LOCAL DECT BASE STATION CONFIGURATION (OM CONFIGURATOR)

As an alternative to DHCP configuration, you can use the OM Configurator tool to statically configure the DECT base stations individually. RFP settings configured through the OM Configurator tool are saved permanently in the internal flash memory of the RFP. The OM Configurator version must match the installed SIP-DECT software version to be used for the local configuration of RFPs.

> **Please note:** The OM Configurator requires the Java Runtime Environment version 1.7 or higher.
>
> **Please note:** An initial configuration of the RFPs 35/36/37 IP / RFP 43 WLAN via the OM Configurator tool requires a login and password. The default login and password is “omm” and “omm”. No login is required for the initial configuration of the previous RFP family (RFPs 32/34 / RFP 42 WLAN. If the RFP is configured by the OMM later on, the OMM also sets the configuration password. You must enter the OMM’s full access user and password in the OM Configurator tool then.

At start-up of the OM Configurator displays a table with configuration data for all RFPs. The task bar on the right side shows permitted actions. The Info console in the lower part of the window shows information and errors as they occur during OM Configurator operation



Interface: Intel(R) Centrino(R) Wireless-N 1030

7.7.1 SELECTING THE NETWORK INTERFACE

You can select the network interface of the computer used by the OM Configurator via the **General -> Options** menu. The selected interface is shown on the status line of the program.

7.7.2 ADDING DECT BASE STATIONS FOR CONFIGURATION

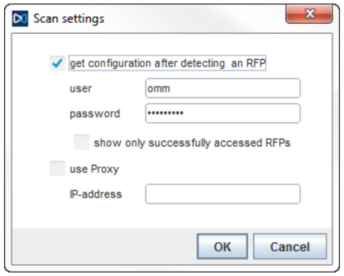
Before you can configure an RFP, you must add the RFP to the OM Configurator database. You can add an RFP record by:

- scanning for RFPs that are already attached to the network
- entering the MAC address of the RFP
- loading a configuration file that contains RFP MAC addresses and configuration parameters

> **Please note:** Adding an RFP to the OM Configurator database does not modify the RFP configuration. Configuration data must be transmitted explicitly to the RFP(s) through the **Send Configuration** option.

7.7.3 SCANNING FOR DECT BASE STATIONS

The OM Configurator tool can scan for RFPs on the LAN segment.



☑ get configuration after detecting an RFP

user omm

password •••••••••

□ show only successfully accessed RFPs

□ use Proxy

IP-address

- If **get configuration after detecting an RFP** is enabled, the OM Configurator attempts to fetch the local configuration settings from all RFPs that are detected during the scan. The program uses the **user/password** combination if an access without login data fails.
- If **show only successfully accessed RFPs** is enabled, the OM Configurator adds only RFPs that provide configuration information to its database, and displays those RFPs in the OM Configurator table.
- The **use Proxy** parameter allows access to RFPs that are located in network segments other than the segment that hosts the OM Configurator. The **IP-address** field must contain the address of a RFP located in the network segment to be scanned. This RFP works as proxy and must be up and running.

You initiate the scan process by clicking **OK** button. The OM Configurator adds the results to the table.

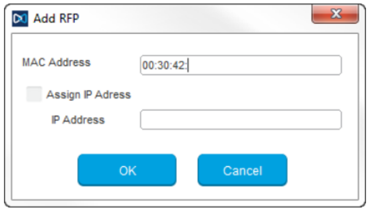
In rare cases, it is possible that a RFP is expected to appear in the table after the scan operation but does not. If this occurs, repeat the scan operation.

7.7.4 ADDING DECT BASE STATIONS MANUALLY

You can add an RFP to the OMM Configurator database manually.

When you click the **Add RFP** option in the task bar, the OM Configurator displays the “Add RFP” dialog. You must specify the MAC address of the RFP in the **MAC Address** field.

Optionally, you can also specify an IP address. If an IP address is assigned, the OM Configurator automatically proposes an incremented IP address the next time the “Add RFP” function is invoked.



Add RFP

MAC Address: 00:30:42:

□ Assign IP Adress

IP Address:

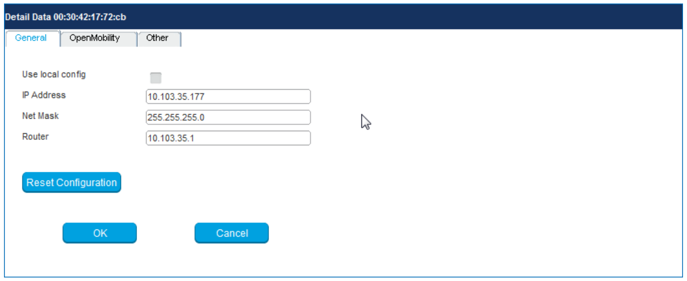
7.7.5 LOADING DECT BASE STATION DATA FROM FILE

You can import an RFP configuration file to the OM Configurator.

When you click on the **Load RFP Config** option, the OM Configurator opens a dialog window that prompts you to browse for the configuration file. All found valid RFP entries in the file are added to the OM Configurator database and displayed in the table.

7.7.6 EDITING DECT BASE STATION CONFIGURATION DATA

You can edit the configuration of a DECT base station stored in the OM Configurator database. When you double-click on a table row, the OM Configurator displays a Detail Data window below the table, with the “General” panel activated. You can also access this window by selecting one or more entries in the table and clicking the **Edit configuration** option in the task bar.



Detail Data 00:30:42:17:72:cb

Use local config □

IP Address: 10.103.35.177

Net Mask: 255.255.255.0

Router: 10.103.35.1

You can change parameters for multiple RFPs by selecting more than one RFP in the table. Parameter settings that differ between the selected RFPs are shown as “***” and retain their values if you do not make any modifications.

You cannot change the IP address value when you select more than one RFP.

If more than one parameter value is allowed (e.g. Router, DNS addresses), you must separate the values by a space.

If you click the **Reset Configuration** button, all configuration parameters are removed and local configuration in the OM Configurator is disabled. The **Send Configuration** option is also needed in this case in order to update the configuration of the RFP locally.

When you click the **OK** button, changed parameter values are committed to the database. The system performs validation checks for some parameter values. If this check fails, the system displays an error message in the Info console and the misconfigured parameter value is marked with a red frame (allowing you to correct the value). Modified RFP records are marked (▶) beside the corresponding table row.

If you press **Cancel** or select another RFP in the table, any changes are discarded.

When you press either **OK** or **Cancel**, the Detail Data panel disappears and a number of task bar options (e.g. **Send Configuration**) are re-enabled.

7.7.6.1 Other parameter panel

You can set and edit less frequently used parameters on the **Other** panel of the **Detail Data** window.

If the parameter you want to add or edit is listed in the table on the **Other** panel, click on it to display the parameter name and value in the fields on the top-right side of the panel. Click the **Change** button to commit the changed value.

If the parameter value field is empty, the parameter is cleared on the RFP when you click **Send Configuration**.

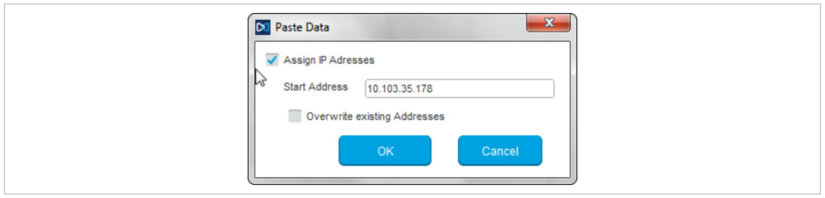
You can add a new parameter by selecting a parameter name from the drop-down list and clicking the **New** button.

7.7.6.2 Copy and Paste

You can assign parameter values from one RFP to one or more other RFPs.

To perform this operation, you must ensure that the **Detail Data** window is not active. If the **Detail Data** window is open, commit your changes or cancel to close the window.

Select an RFP in the table and click the **Copy Configuration** option in the task bar. Next, select one or more RFPs as destination RFP(s) and click the **Paste Configuration** option. The system displays the Paste Data dialog window.



Paste Data

☑ Assign IP Adresses

Start Address: 10.103.35.178

□ Overwrite existing Addresses

If the **Assign IP Addresses** option is enabled, you must provide a valid IP address in the **Start Address** field. The system may display a suggested address, based on a previous paste or Add RFP operation. The IP address is incremented by one for each RFP.

If the **Overwrite existing addresses** parameter is not enabled, an IP address is only assigned if the IP address field of the target RFP is empty.

7.7.6.3 Configuration Parameters

The following table lists the available configuration parameters for the DECT base station.

Parameter	Mandatory/Optional	Description
Use local config	Mandatory	Specifies whether the local configuration settings should be used at boot-up or not
IP Address	Mandatory	IP address of the DECT base station.
Net Mask	Mandatory	Subnet mask of the IP network
TFTP server address	Mandatory	IP address of the TFTPO server (set to 0.0.0.0 if not used)
TFTP file name	Mandatory	The boot file to be read from the TFTP server
TFTP server list	Used only by: RFP 32/34 RFP 42 WLAN Optional	List of additional TFTP servers to load the boot file
Preferred TFTP server	Used only by: RFP 32/34 RFP 42 WLAN Optional	TFTP server from which to load the boot file first
OMM address	Mandatory	IP address of the OpenMobility Manager
Router	Optional	IP address of the default gateway
DNS address	Optional	IP address of the DNS server
DNS domain	Optional	Domain name of the network
Broadcast address	Optional	Broadcast address for the network
2nd OMM address	Optional	IP address of the standby OMM
VLAN ID	Optional	VLAN identifier
Use VLAN and DHCP	Optional	Specifies whether only the local VLAN configuration settings should be used when booting or not
Syslog server address	Optional	Destination IP address for the syslog file
Syslog server port	Optional	Destination port address for the syslog file
RFP configuration file server	Optional	URL of a server with RFP configuration files (ipdect.cfg|<MAC>.cfg) alternatively or in addition to OM Configurator settings. Syntax: {ftp|ftps|http|https}://[user:password@]server/[directory/] or tftp://server/[directory/]

7.7.7 APPLYING CONFIGURATION CHANGES

To apply new or changed configuration to RFP devices, select one or more RFP entries from the table and click the **Send Configuration** option in the task bar.

Note: You must close the Detail Data window to apply configuration changes to an RFP. If the Detail Data window is open, the **Send Configuration** option is disabled.

The OM Configurator displays the **Protocol settings** dialog window.

The settings in the **Protocol settings** dialog are preset to the values used for the **Scan** operation or the last **Send Configuration** operation. If the values are correct, click **OK** to transfer the data to the RFP device.

Before sending the data, the system performs a check on mandatory parameters and the validity of some parameter values. If this check fails, an error is reported in the Info console.

The system displays a message in the Info console window indicating success or failure of the data transfer operation for each RFP.

If data is transferred successfully, the OM Configurator displays a checkmark beside the row for the corresponding RFP.

The OM Configurator attempts data transfer three times (two seconds apart) before reporting an error. Depending on the network environment and current RFP status, the data transfer may fail in rare cases. If a failure to transfer data occurs, click the **Send Configuration** option again to re-initialize the data transfer.

If the data transfer fails, the OM Configurator displays an “X” beside the row for the corresponding RFP.

7.7.8 FACTORY RESET

RFPs are protected against unauthorized configuration changes by user authentication (user and password), which are also used to configure the OMM via web service or OMP.

To reset a RFP’s configuration, select the RFP entry in the table and click the **Factory Reset** option in the task bar. This option is only enabled when a single RFP entry is selected. The option is disabled if multiple RFPs are selected.

The system displays the **Factory reset settings** dialog window. Set the correct login data (user and password) and RFP proxy address (if required). The system auto-fills the fields with the values used for previous **Scan**, **Send Configuration** or **Factory Reset** operations.

If the specified login (“omm”/”omm”) does not work and the login credentials of the last system the RFP was used with are unknown, you can reset the RFP to factory settings by sending a cookie string to the OpenMobility manufacturer support and entering the received reset key. The OM Configurator copies the cookie string to the clip board.

7.7.9 SAVING AND LOADING A DECT BASE STATION LIST

You can save the configuration of one or more RFPs to a RFP configuration file. Select the RFP entries in the table and click the **Save RFP Config** option in the task bar. (Note that if the **Detail Data** window is active, the **Save RFP Config** option is disabled.)

RFP configuration data is loaded from the file and added to the OM Configurator database via the **Load RFP config** option. You must initiate the **Send Configuration** operation after executing the **Load RFP config** operation for the configuration to take effect on the select RFPs.

> **Please note:** The data sequence has been changed from previous releases of the SIP-DECT OM Configurator. Import of files based on the old data sequence format may result in import errors or the incorrect assignment of parameter values.

7.7.10 REMOVING DECT BASE STATION ENTRIES

You can remove all RFP data records from the OM Configurator database through the **Clear List** option in the OM Configurator task.

You can remove one or more RFP records from the OM Configurator database by selecting one or more entries in the table and clicking on the **Remove selected RFP** option.

Ensure that you do not remove data records before configuration is sent to the RFP device (via the **Send Configuration** operation). Changes made to RFP configuration data but not sent to RFP device are lost on the remove operation.

You can add RFP configuration data again through the operations described above.

7.7.11 COMPATIBILITY WITH OLDER SIP-DECT RELEASES

It is not recommended to use the SIP-DECT 6.1 OM Configurator for configuration of RFPs with software from an earlier SIP-DECT release.

Configured parameters of an RFP which are unknown to actual OM Configurator are shown in the "Other parameter" panel with the name used at the protocol level. In most cases, this name will be different from the display name known from previous versions of OM Configurator.

You can edit or remove such parameters and new values will be transferred to the RFP when you execute the **Send configuration** operation.

7.8 OMM CONFIGURATION AND RESOURCE FILES

The OMM supports certain configuration files containing commands in AXI style, to support auto-configuration of small and simple installations in provider environments. It is assumed that the configuration files are automatically generated in a standardized way, to prevent configuration failures.

The following list summarizes all of the configuration and resource files related to the provisioning of a SIP-DECT system:

- ipdect.cfg / <MAC>.cfg / <PARK>.cfg

These files contain configuration parameters and are used to configure the OMM automatically. There is one common file "ipdect.cfg" for all RFPs and one file "<MAC>.cfg" for every single IP-RFP. The RFP specific <MAC>.cfg is requested if indicated in the common "ipdect.cfg" file. It is possible that all RFPs request "ipdect.cfg" and only selected RFPs request the <MAC>.cfg (for specific configuration on some RFPs).

- usr_common.cfg / <user>.cfg

These files are related to the "External User Data Provisioning" feature, whereby <user> refers to <Number/SIP user name> or <LoginID>.

<user>.cfg can also refer to user.cfg, a common file name for all users. This concept allows a provisioning server to provide user-specific settings on demand using one file name based on the specific user credentials.

- ima.cfg

This file includes the configuration for Integrated Messaging & Alerting Application, and can be loaded permanently.

- iprfp3G.dnld

This file includes the software image for RFP 35/36/37 IP / RFP 43 WLAN. This file also includes the software images for the Mitel 600 DECT phone family. RFPs can load their software image directly from the RFP OMM.

- license.xml

This file includes the license for a specific SIP-DECT system.

- customer_image.png

This resource file can include a customer logo displayed to display on the OMM Web service.

With SIP-DECT 6.0 or later, all of these files can be loaded from the same external file server, if configured (see section 7.8.1).

7.8.1 CONFIGURATION FILE URL

SIP-DECT supports provisioning through external configuration files. With SIP-DECT 6.0 or later, you can configure a URL for an external file server, from which all configuration files can be downloaded.

The configuration file server URL (ConfigURL) can be configured in the OMM (**System** -> **Provisioning** -> **Configuration file URL**), via DHCP or the Redirection and Configuration Service (RCS).

> **Note:** If the external file server requires credentials for authentication, the credentials must be configured using the DECT phone or the Web service.

The following files are automatically requested if a provisioning server is set:

- Configuration files supporting startup parameters and OM AXI code for the OMM configuration
  - ipdect.cfg
  - <mac>.cfg (note that if a standby OMM is set, two MACs are present)
  - <PARK>.cfg (PARK in MAC address format: e.g. 001F11234001)
  - User configuration files (for user login on DECT phone)
  - user_common.cfg
  - <user.cfg>
  - user.cfg
- Integrated Messaging and Alerting Service (IMA) (for alarm scenarios, email accounts, RSS feeds) - ima.cfg
- OMM license file - license.xml
- Logo for OM Web-Portal (Branding) - customer_image.png

You can also configure individual URLs for most configuration files. If present, the individual URL is used for the configured feature.

At startup, the OMM tries to retrieve the configuration file URL (ConfigURL) from the following sources, in the order listed. The OMM uses the first URL it finds to load the configuration and resource files.

The URL can be set through the following methods (in order of priority):

1 OMM database (e.g. **System** > **Provisioning** > **Configuration file URL** in either OMM Web service or OMP)
2 DHCP option 66 (SIP-DECT 6.2 or higher)
3 DHCP vendor specific option 43 – sub-option 2
4 DHCP option 234
5 Redirection and Configuration Service (RCS) – on initial setup only

Once a URL is set, it is stored in the OMM database. The URL can be overwritten at a later time e.g. during provisioning after authentication.

Note: The ConfigURL only applies to the RFP OMM, which must be running SIP-DECT 6.0 or higher.

Other DECT base stations only apply the ipdect.cfg and <mac>.cfg files without OM AXI.

7.8.1.1 Syntax

The ConfigURL has the following syntax:

```
<protocol>://<user>:<password>@<server>/<path>&<parameter>
```

- Supported protocols: ftp,ftps,tftp,sftp,http,https
- Credentials should be secured by transport protocol or digest authentication.

The ConfigURL supports additional parameters to modify the certificate validation behavior for the configuration file server:

- **cm:** <https client method > - TLS1.0, TLS1.1, TLS1.2 or AUTO (AUTO= all)
- **vc:** <validate certificates> - valid settings are: 0 or 1
  The OMM includes a list of trusted CA's (Mozilla CA certificate list)
- **ve:** <validate expires> - validation of certificate expiry: 0 or 1
- **vh:** <validate hostname> - validation of hostnames: 0 or 1
- **uc:** allow un-configured trusted certificates> - allow untrusted certs: 0 or 1
  If set to 1, validation is disables as long as no trusted certificate was imported.
- **ic:** <import certificate> - import server certificate as trusted: 0 or 1
  If ic=1 + uc=1, the trusted certificate will be imported without any validation, as long as no trusted certificate was imported previously.

You can view and change the ConfigURL via the OMM Web service (see section 5.4.2) or the OMP (see section 6.5.5.1).

7.8.2 SPECIFIC CONFIGURATION URLS

In addition to the common ConfigURL, you can configure specific URLs for individual configuration and resource files in the OMM database. As soon as a specific URL is set, the OMM uses that URL to load the appropriate configuration/resource file during startup.

Note that the user_common.cfg file is loaded from the ConfigURL and the specific URL when both URLs are set.

Configuration / Resource File	Location of Specific URL	
	OMM Web Service	**OMP**
user_common.cfg / <user>.cfg	N/A	**System** > **Data management** > **User data import** See section 6.5.7.2.
ima.cfg	**System** > **System settings** > **OM Integrated Messaging & Alerting service** See section 5.4.1.	**System** > **Advanced settings** > **IMA** See section 6.5.2.4.
iprfp3G.dnld	**System** > **System settings** > **Software update URL** See section 5.4.1.10.	**System** > **Basic settings** > **Software Update URL** See section 6.5.1.4.
Iprfp4G.dnld	**System** > **System settings** > **Software update URL** See section 5.4.1.10.	**System** > **Basic settings** > **Software Update URL** See section 6.5.1.4.
600.dnld	**System** > **System settings** > **DECT phone's firmware update** See section 5.4.1.6.	**System** > **Advanced settings** > **PP firmware** See section 6.5.2.3.
customer_image.png	N/A	**System** > **Advanced settings** > **Special Branding** See section 6.5.2.7
iprfp2G.tftp		

7.8.3 RELOAD OF CONFIGURATION AND RESOURCE FILES

The OMM automatically tries to load all configuration and resource files (ipdect.cfg, <MAC>.cfg, PARK.cfg, ima.cfg, user_common.cfg, update check for iprfp3G.dnld, etc) from the retrieved ConfigURL or specific URL (if present in the OMM database) at startup.

Note: The <user>.cfg and user.cfg files are only loaded on demand. They are not loaded automatically.

In addition, the OMM supports several mechanisms for updating the configuration by triggering a reload of the configuration and resource files:

- DHCP lease time

If the OMM is running on a RFP and DHCP is used, all configuration and resource files are reloaded when half of the DHCP lease time has elapsed.

- Daily automatic reload of configuration and firmware files

You can enable this option and specify a specific time of day to reload configuration files via the OMM Web service or the OMP (System -> Provisioning -> Daily automatic reload of configuration and firmware files).

- Manual reload via **Update** button

You can trigger a manual reload of all configuration and resource files by clicking the **Update** button in the OMM Web service (**System** ->**System settings** page) or OMP (**System** -> **System settings** -> **General** tab).

- 600 DECT phone **Administration** menu
  - When a user with a 600 DECT Phone selects the **Sync system data** option in the **Administration** menu, the OMM reloads all configuration and resource files.
  - When a user with a 600 DECT Phone selects the **Sync user data** option in the **Administration** menu, the OMM reloads the <user>.cfg file for that user.
- SIP Notify message
  - When the OMM receives a SIP Notify message with the “**check-sync**” event for a user, the OMM reloads the configuration file <user>.cfg for that user.
  - When the OMM receives a SIP Notify message with the “**prov-sync**” or ”**resync**” event for any user, the OMM reloads all configuration and resource files. The SIP Notify with ”prov-sync” or ”resync” can be also addressed to the OMM (without the user portion in the request URI).

7.8.4 AXI COMMANDS IN CONFIGURATION FILES

With SIP-DECT 6.0 or later, the OMM supports configuration files containing commands in AXI style, for OMM configuration.

The OMM attempts to load the following files from the Configuration File URL, and processes them in this order:

1 ipdect.cfg

2 <MAC>.cfg (RFP OMM only)

3 <PARK>.cfg (PARK in MAC address format: e.g. PARK: 1F11234001; MAC address format 001F11234001)

Note that the actual file name of the <MAC>.cfg depends on MAC address of the RFP where the OMM is running.

The active OMM and the standby OMM request different files, even if they belong to one system. To ensure that both OMMs can retrieve the same file independent of which one is active, each OMM requests the <PARK>.cfg. The PARK identifies a SIP-DECT system in a unique way.

None of the files are mandatory and they can be empty. The AXI commands can be all in one file or split up as needed.

Example configuration file

The following example shows how to include AXI commands in a configuration file.

```
### SIP-DECT OMM Config example - pls. be aware that some commands cannot be applied to
SIP-DECT with Cloud-ID e.g. request PARK from server, set regulatory domain etc. and some
commands depend on the actual use case/setup

### Confirm EULA

<SetEULAConfirm confirm="1" />

### Set full access account
```

```
<SetAccount plainText="1" > <account id="1" password="Sip!12" active="1" aging="none" />
</SetAccount>

### Set root account

<SetAccount plainText="1" > <account id="2" password="Sip!12" active="1" aging="none" />
</SetAccount>

### Set system name

<SetSystemName name="6.1 NB" />

### Tone scheme

<SetSysToneScheme toneScheme="DE" />

### OMP web start #####

<SetOMPURL> <url enable="1" protocol="FTP" host="ber-rd5014" path="/pub/SIP-DECT/Linux"
/></SetOMPURL>

### Enable SSH ###

<SetRemoteAccess enable="1" />

### Request a valid PARK from a Server ####

<PARKFromServer />

### Set DECT Regulatory Domain ###

<SetDECTRegDomain regDomain="EMEA" />

### Set WLAN Domain/contry ###

<SetWLANRegDomain regDomain="DE" />

### Enable Auto-create on subscription ####

<SetDevAutoCreate enable="1" />

### Set DECT AC ####

<SetDECTAuthCode ac="35239" />

### Set specific user data URL ####

<SetUserDataServer plainText="1" useCommonFileNameOnServer="1" ><url enable="1"
protocol="HTTPS" host="wwww.domain.de" path="/lpueschel/test/" username="lpueschel"
password="lpueschel" validateCerts="0" /></SetUserDataServer>

### Set SIP Proxy and Registrar ###

<SetBasicSIP transportProt="UDP" proxyServer="172.30.206.9" proxyPort="5060"
regServer="172.30.206.9" regPort="5060" regPeriod="3600" />

### use addId="" for Login at DECT DECT phone ####

<SetDECT phoneLoginVariant login="ID" />

#### Set Portrange 17000 - 32767 ####

<SetPortRangeSIP ><userUdpTcp startPort="17000" endPort="17511" /><userTls
startPort="18000" endPort="18511" /></SetPortRangeSIP>

#### Set SOS/ManDown emergency number ####

<SetAlarmTrigger><trigger id="0" triggerId="SOS" fac="SOS" comment="" num="110"
/></SetAlarmTrigger>

<SetAlarmTrigger><trigger id="1" triggerId="MANDOWN" fac="MANDOWN" comment="" num="112"
/></SetAlarmTrigger>

### Set common voice mail number ###

<SetSysVoiceboxNum voiceboxNum="6333" />
```

WARNING: **Configuration files must be automatically generated in a standardized way to avoid configuration failures. Configuration failures could cause a SIP-DECT system outage.**

Note that this configuration file approach has limitations. For example:

- Insufficient for managing data objects that are dynamically created and addressed by an index (e.g. RFPs)
- No administrator feedback for commands that cannot be processed (e.g., unknown commands, invalid parameter, conflicts which other configuration settings)

7.8.4.1 User Data in Configuration Files

Configuration files are generally insufficient for managing data objects that are dynamically created and addressed by an index. Therefore, it is necessary to configure user data also. This allows providers to manage the user data (to a limited extent) without using the <user>.cfg files.

The <user>.cfg concept supports the complete range of user-related SIP-DECT functions, including a user-specific DECT phone configuration. The user data in configuration files as described here supports only a limited set of parameters.

To allow user data in configuration files, the following rules must be applied:

1 Initialize all possible data sets with default values Number/SIP user name is automatically set to uid<X> (e.g,. uid1):

```
<CreatePPUser plainText=1 replaceData=1><user uid="1" name="" num="" addId=""
sipAuthId="" sipPw="" pin="" fixedSipPort="0" /> </CreatePPUser>

…

<CreatePPUser plainText=1 replaceData=1><user uid="512" name="" num="" addId=""
sipAuthId="" sipPw="" pin="" fixedSipPort="0" /> </CreatePPUser>
```

2 To “add” a user, set appropriate data:

```
<CreatePPUser plainText=1 replaceData=1><user uid="1" name="Account004 Mitel"
num="040226332195" addId="195" sipAuthId="040226332195" sipPw="broadnet.01" pin="195"
fixedSipPort="0" /> </CreatePPUser>
```

3 To “remove” a user, set to default data:

```
<CreatePPUser plainText=1 replaceData=1><user uid="1" name="" num="" addId=""
sipAuthId="" sipPw="" pin="" fixedSipPort="0" /></CreatePPUser>
```

This supports the use of templates such as the following:

```
<CreatePPUser plainText=1 replaceData=1><user uid="1" name="%BWNAME-1%" num="%BWLINEPORT-
1%" addId="%BWEXTENSION-1%" sipAuthId="%BWAUTHUSER-1%" sipPw="%BWAUTHPASSWORD-1%"
pin="%BWEXTENSION-1%" fixedSipPort="0" /></CreatePPUser>
```

7.8.5 USER CONFIGURATION FILES

The user configuration files (user_common.cfg and <user>.cfg) enable the “External User Data Provisioning” feature, which allows customers to import user data from a provisioning server. See the *SIP-DECT OM DECT Handset Sharing & Provisioning Installation & Administration User Guide* for a full description of that feature.

In addition <user>.cfg can also refer to user.cfg, a common file name for all users.

SIP-DECT 6.0 introduced the *UDS_CommonUserFileName* configuration attribute. When enabled, the OMM tries to fetch the same user.cfg file from the provisioning server for each user executing the login procedure, such that the login credentials of each user are used to access the provisioning server. This

means that the provisioning server executes user authentication and provides a user-specific user.cfg when the user is authorized.

The *UDS_CommonUserFileName* attribute is enabled/disabled via the user_common.cfg file.

> **Please note:** The common user file name feature is only applicable in combination with the file transfer protocols FTP, FTPS, HTTP, HTTPS or SFTP, which may require user/password credentials. Changing this attribute might cause login/logout problems for the users, because of changed authentication. It is up to the administrator to force user logouts (delete users) optionally. In any case, the administrator must publish new authentication data to users for their logins and logouts. This value is stored in the OMM database. So, the setting is stored over system restart and has no default value when not explicitly set in the user_common.cfg file.

Note that the *OM_UniqueId=NUMBER/UID* variable in the user_common.cfg file is no longer supported.

The following table summarizes the combinations of provisioning server access and type of user validation supported:

Provisioning Server access	Requested files	User validation	Supported DECT phones
• User data import URL • User data import credentials • No certificate validation	• <number | SIP user name>.cfg • <loginID>.cfg	OMM authenticates user against PIN from .cfg files	• GAP • Mitel 142d • Mitel 600
• User data import URL • User data import credentials • System Provisioning Certificate validation	• <number | SIP user name>.cfg • <loginID>.cfg	OMM authenticates user against PIN from .cfg files	• GAP • Mitel 142d • Mitel 600

• System Provisioning URL • System Provisioning credentials • System Provisioning Certificate validation	• <number | SIP user name>.cfg • <loginID>.cfg	OMM authenticates user against PIN from .cfg files	• GAP • Mitel 142d • Mitel 600
• User data import URL • User credentials (UDS_CommonUserFIleName=YES) • No certificate validation	• user.cfg	Provisioning server authenticates user at file request with user credentials	• Mitel 600
• User data import URL • User credentials (UDS_CommonUserFIleName=YES) • System Provisioning Certificate validation	• user.cfg	Provisioning server authenticates user at file request with user credentials	• Mitel 600
• System provisioning URL • User credentials • (UDS_CommonUserFIleName=YES) • System Provisioning Certificate validation	• user.cfg	Provisioning server authenticates user at file request with user credentials	• Mitel 600

7.8.6 DIGEST AUTHENTICATION AND CERTIFICATE VALIDATION

The OMM supports system credentials for provisioning to retrieve configuration and resource files from a server that requires user/password authentication.

System credentials are used to retrieve files from the external provisioning server defined by the configuration file URL, for protocols supporting authentication or servers requesting authentication. For HTTP/HTTPS, basic and digest authentication are supported.

You can set the system credentials via:

- OMM Web service **System** -> **Provisioning** -> **System credentials** page (see section 5.4.2.2)
- OMP **System** -> **Provisioning** -> **System credentials** tab (see section 6.5.5.4)
- Mitel 600 DECT phone user interface (through Feature Access Code or the Administration menu)

System credentials are also inherited if sources other than the configuration file URL are configured for specific configuration or resource files, without credentials. The system credentials are used only if requested by the file server.

7.8.6.1 System credentials via Mitel 600 DECT Phone user interface

A Mitel 600 DECT phone user can set, change or delete system credentials from the Mitel 600 DECT phone via:

- a configured feature access code (FAC)
- the **Administration** menu on the user interface

Note: The user must log in to OMM before being allowed to change valid credentials. If credentials are not set or are invalid (indicated by a health state), the OMM login is omitted.

Setting the credentials via feature access codes requires configuration of a FAC number through the **System Features** -> **Feature Access Codes** menu of the OMM web service (see section 5.9.4) or the OMP (see section 6.12.2).

When the user dials the configured feature access code, the user can select between the "Create/Change" and "Delete" options. The Administration menu additionally offers a health indication (ok or not ok). Depending on the health state, the user may be forced to login to the OMM first.

7.8.7 DECT BASE STATION SOFTWARE IMAGE FROM RFP OMM

To simplify the upgrade process for existing SIP-DECT installations in provider environments, SIP-DECT 6.0 and later provides support for a feature that allows the RFP 35/36/37 IP / RFP 43 WLAN to load their software image directly from the connected OMM.

If the RFP 35/36/37 IP / RFP 43 WLAN has no valid URL from which to load the software, they attempt to load the software from the connected OMM. If the OMM is running on a RFP, the RFP OMM delivers the software to the connected RFPs.

A new software image for the RFP OMM can be provided as a iprfp3G.dnld file on an external file server. The software update URL can be configured via the OMM Web service (see section 5.4.1.10) or OMP (see section 6.5.1.4).

7.8.8 REDIRECTION AND CONFIGURATION SERVICE (RCS)

The Redirection and Configuration Service (RCS) simplifies SIP DECT installation and management. When the MAC address or the PARK of a SIP-DECT OMM is entered in the RCS server, a SIP-DECT OMM is routed to its assigned server for configuration upon initial start-up.

If the OMM does not find a ConfigURL during initial setup, the OMM contacts the RCS to request a ConfigURL, using its RFP MAC address. If the RFP MAC Address is configured in the RCS, the RCS provides a ConfigURL that points to an external provisioning server. The OMM attempts to load all configuration and resource files from the ConfigURL received from RCS.