SIP-DECT Multi-OMM Manager

Mitel

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

SIP-DECT Multi-OMM Manager
Administration Guide
Release 8.0 - July 2018

Chapter 1

Multi-OMM Manager Overview

Multi-OMM Manager functionality

The Multi-OMM-Manager (MOM) is a server application that provides centralized provisioning and user/device data synchronization across multiple SIP-DECT sites within a SIP-DECT system.

In previous SIP-DECT releases, administrators could deploy one OMM with DECT base stations installed at different sites, however, such deployments provided no redundancy or local survivability for a site in the event of a connection failure to the OMM. Alternatively, administrators could deploy an OMM and DECT base stations at each site, to ensure local survivability, but each system had to be maintained separately.

With SIP-DECT 7.0 and later, you can create a multi-site SIP-DECT system with local survivability and centralized management capabilities. You deploy OMMs and DECT base stations as a stand-alone system at each site, but manage the entire SIP-DECT system through the MOM interface.
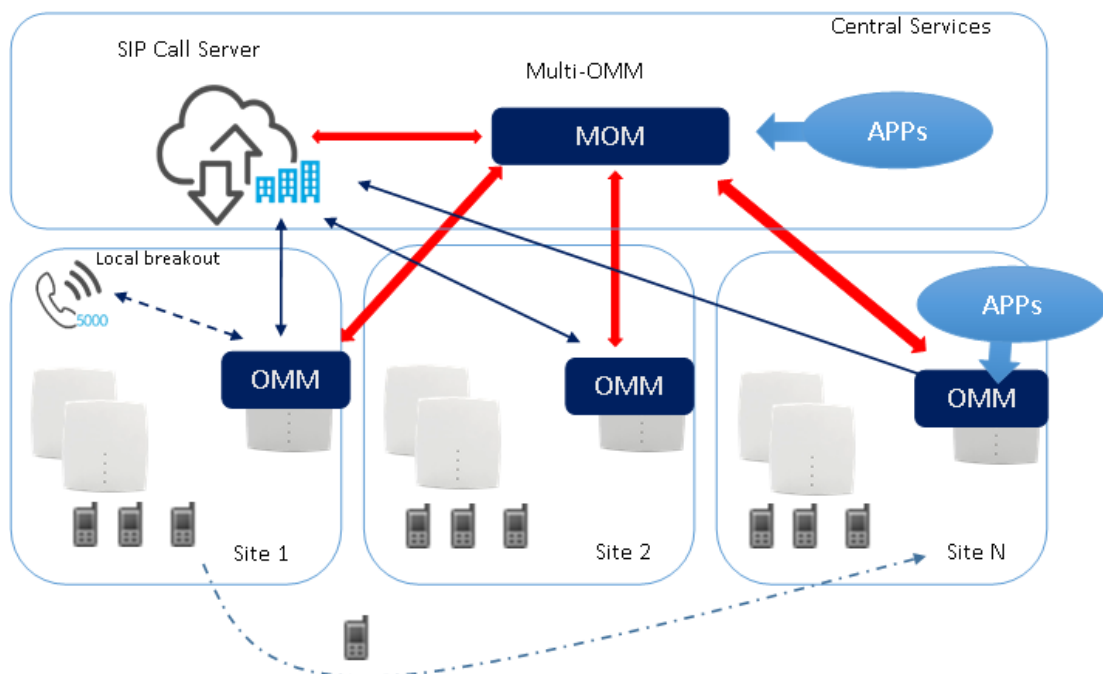
The MOM maintains a connection to each OMM in the system and manages all user and device operations, including roaming between sites. In addition, the MOM provides messaging and alerting support across all sites in the system, and provides an interface through which applications attached to the OMMs at different sites can communicate.

> **Note:** If the connection to an OMM is disconnected, the MOM tries to re-establish the connection every minute.

The MOM also supports simplified OMM provisioning. You can create provisioning files with OMM-specific settings and deploy them to individual OMMs from the MOM interface.

Centralized user and DECT phone management

The MOM solution supports centralized management for up to 500 sites / 50000 users.

Every time the MOM connects to an OMM, all of the OMM's user and device information is imported into the MOM. As a result, the MOM has knowledge of every user and DECT phone device in the system.

See the following sections for more information:

*   "User and device dataset configuration" on page 3

*   "DECT phone subscription" on page 3

*   "Roaming between sites" on page 3

User and device dataset configuration

You can perform user and device configuration on a local OMM or the MOM. Configuration changes are synchronized when the MOM connects to the OMM, based on the latest time stamp.

The MOM displays all device and user records for the entire SIP-DECT system (and identifies the OMM to which they are locally registered). Each OMM only displays local user and device datasets.

For example, if you create a user dataset in the OMM, the information is immediately moved to the MOM database (if the connection to the MOM is active). The information only appears on the local OMM when the user/phone pair becomes active.

DECT phone subscription

The Access Rights Identity of the MOM system is the SARI (common identity), in contrast to the PARI (system local identity), which is individual for every OMM. A DECT phone, which is subscribed to the SARI that enables to roam among the OMMs; whereas a DECT phone, which is subscribed to the PARI that operates only within the local OMM.

The MOM handles device subscription for all OMMs. When the MOM is connected to the OMM; the local **Auto-create on Subscription** option is disabled, and cannot be enabled on the OMM.

Since the MOM sets the SARI on the OMM when a connection is established, all DECT phones at the OMM's site subscribe to the SARI.

> **Note:** DECT phone configuration includes an option to **Subscribe to PARI only**. Any devices with this option enabled do not subscribe to the SARI, and therefore cannot roam between sites. This option is disabled by default.

You can set the subscription mode (that is, by configured IPEIs or wildcard subscription) and enable Auto-create on Subscription of unbound device datasets on subscription from the MOM interface only.

Roaming between sites

The MOM allows users/devices to roam between different SIP-DECT sites and ensures that each OMM has the necessary user/device data records to initiate SIP registration when a user changes location.

When a user roams to another site, the DECT phone connects to a base station at the new site, which triggers a location registration with the local OMM. The new OMM notifies the MOM of the device's new location, and the MOM transfers the user/device record from the old OMM to the new OMM. The new OMM initiates a SIP registration on the configured SIP server, while the old OMM unregisters the DECT phone from its configured SIP server.

Permanent users

Most roaming scenarios require an active connection between the MOM and the OMM. Each OMM only has knowledge of users and devices registered to its local system, and relies on the MOM to obtain new user/device records for users who roam to its site.

By enabling the "Permanent" flag, you can always configure the user record, which is available in every OMM. All users with the "Permanent" flag are enabled and their bound devices are imported to all OMMs in the system and remain in the OMM database, regardless of their current location. If the OMM's connection to the MOM is down, and the user roams to the site, the OMM has the information necessary to initiate a SIP registration to the configured SIP server on their behalf.

> **Note:** The number of permanent users permitted in the system is limited to 512. The total number of local users/devices (including permanent users) may not exceed the OMM capabilities.

Centralized system provisioning

The MOM provides a mechanism for centralized OMM provisioning, based on configuration files containing AXI commands. The MOM can also host resource files, such as software or configuration files, accessed by the OMMs.

This system data provisioning feature can be enabled or disabled per OMM.

OMM configuration files

An OMM configuration file (ipdect.cfg) contains AXI commands with specific parameters and values. The OMM uses this provisioning file to load system configuration.

With the centralized OMM provisioning feature, the MOM can generate the ipdect.cfg for each OMM. The MOM uses a configuration file template that contains AXI commands and placeholder keys for individual parameters, and uses a separate OMM configuration data file for each OMM, which contains OMM-specific values that corresponds to the placeholder keys in the configuration file template.

When an OMM requests an ipdect.cfg file (that is, where **Provisioning** is enabled for this OMM in the MOM), the MOM generates the configuration file based on the configuration file template and the OMM-specific placeholder values provided in the OMM configuration data file.
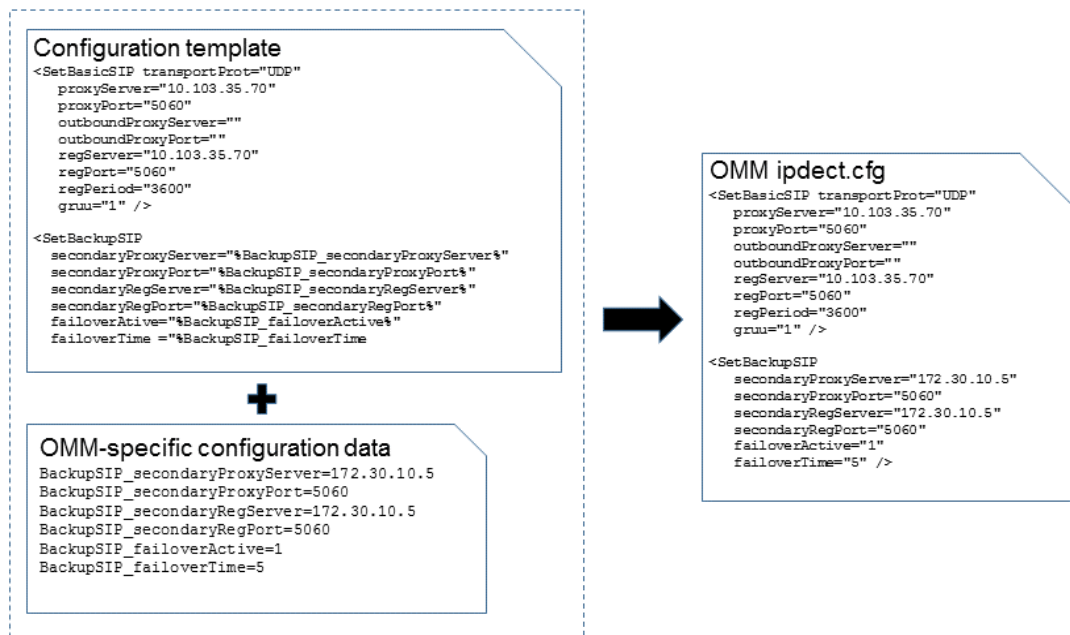
Configuration file template

The configuration file template is an OMM configuration file that contains AXI commands (in XML format) for SIP-DECT system configuration. You can customize the configuration file template to include only those commands and parameters that you want to provision for the SIP-DECT system.

You can customize the configuration file by:

- enabling an AXI command with placeholders, you can specify different values for the AXI command in individual OMM placeholder files

- configuring an AXI command with a specific parameter value (applies to all OMMs)

- addressing an AXI command to a particular OMM (identified by Cloud-ID)

Placeholders for individual OMM values

Each AXI command contains one or more parameters for the command and a placeholder for the parameter value. The placeholder starts and ends with a % character, and the string between the % characters represents a unique placeholder name.

For example, the following AXI command enables provisioning of the DECT regulatory domain and specifies a placeholder key (%DECTRegDomain_regDomain%) for the regulatory domain parameter:

```
<SetDECTRegDomain regDomain="%DECTRegDomain_regDomain%" />
```

The MOM replaces the placeholder name with a specific value from the OMM placeholder configuration data file when generating the ipdect.cfg file for a particular OMM. If no placeholder/value pair exists in the OMM configuration data file, the placeholder is not replaced.

Same value applied to all OMMs

If you specify a parameter value in the configuration template file (instead of a placeholder), that value is applied to all OMMs in the system with provisioning enabled.

For example, the following AXI command enables provisioning of the DECT regulatory domain and specifies the EMEA regulatory domain:

```
<SetDECTRegDomain regDomain="EMEA" />
```

The MOM includes the parameter and its value in every OMM-specific ipdect.cfg file that it generates.

Enabling an AXI command for a specific system

If you want to apply an AXI command to a specific OMM, you can add the cloud-Id attribute to the AXI command and specify the SIP-DECT system cloud-ID as the value.

For example, the following AXI command enables provisioning of the DECT regulatory domain and specifies the EMEA regulatory domain, but only for the OMM identified by 001F1028D67A:

```
<SetDECTRegDomain cloudId="001F1028D67A" regDomain="EMEA" />
```

The MOM includes the command and parameter into every ipdect.cfg file generated for the OMMs. Each OMM executes only commands without Cloud-ID or with a Cloud-ID identical to the Cloud-ID owned by this specific OMM.

OMM placeholders file

If you use placeholders in the configuration template, you must create OMM-specific values for the placeholders. The MOM uses the configuration template and the placeholder file to generate an OMM-specific ipdect.cfg file that contains the appropriate AXI commands and parameter values.

You can define your own placeholder names, but the placeholder name in the OMM file must match the placeholder name used in the configuration file template.

> **Note:** Placeholder names are case-sensitive.

For example, the following AXI command in the configuration template enables provisioning of the DECT regulatory domain and specifies a placeholder key (%DECTRegDomain_regDomain%) for the regulatory domain parameter:

```
<SetDECTRegDomain regDomain="%DECTRegDomain_regDomain%" />
```

In the OMM placeholder file, you specify the placeholder value (without the % characters) used in the template and the value you want to set for the OMM:

```
DECTRegDomain_regDomain=EMEA
```

Enabling/Disabling an AXI command for a group of systems

If an AXI command has to be applied only for a group of OMMs, two special placeholders to comment-out an AXI command can be introduced.

For example, the AXI command "**SetDECTRegDomain**" is not allowed for "SIP-DECT with Cloud-ID" systems. To comment-out such request, the placeholder "**%BeginComment%**" and "**%EndComment%**" can be introduced in the template file:

```
%BeginComment%
  <SetDECTRegDomain regDomain="EMEA">
%EndComment%
```

In the OMM placeholder file of the "SIP-DECT with Cloud-ID" systems, specify the start and stop values for the XML comment block:

```
BeginComment=<!--
EndComment=-->
```

In the OMM placeholder file of all other systems, specify the empty start and stop values.

```
BeginComment=
EndComment=
```

For detailed information which AXI commands are supported, please see "SIP-DECT with Cloud-ID - System Manual".

Configuration URL

When the **Provisioning** feature is enabled for the OMM, the MOM sets the ConfigURL and provisioning system credentials (username and password) on the OMM every time the MOM connects to the MOM, overwriting any local modifications.

The ConfigURL for the provisioning files points to the MOM interface, and the provisioning credentials used are the OMM credentials configured in the MOM.

> **Note:** By default, the MOM enables only limited SSL certificate validation on the OMM, You can change the settings on the Certificates tab in the OMMs panel.

In addition, the MOM enables daily automatic reload of the configuration and firmware files for the OMM, and sets the time of day for configuration file reload. The time of day is a value between 00:00 and 00:50 (format: hh:mm) to reduce simultaneous requests for configuration files to the MOM from multiple OMMs.

When the **Provisioning** feature is disabled for an OMM, the ConfigURL setting is also disabled on the OMM.

OMM resource files

The MOM can also host resource files, such as software or configuration files, for system OMMs.

The MOM can host common resource files that are available to all OMMs in the system, including:

- customer_image.png (branding logo)
- OMP.jar (OMP application)
- user_common.cfg (for example, COA profiles)
- iprfp3G.dnld (DECT base station software)

You can store the files on the MOM server in the **/opt/SIP-DECT-MOM/web/resources** directory and require no credentials for access.

The MOM can also host OMM-specific resource files, including:

- ima.cfg (Integrated Messaging and Alerting configuration file)
- OMM backup files (e.g., automatic database backup), written to the MOM by the OMM

The files can be stored in the **/opt/SIP-DECT-MOM/web/omm_files/Cloud-ID-<cloud-id>** directory on the MOM server, which is login protected and requires OMM credentials for access.

You must create the OMM-specific directory on the MOM server and make the files available there if you want to use the MOM to host resource files for the OMM.

> **Note:** For automatic database backup, each OMM on the MOM site requires a specific configuration.

Predefined placeholders

The MOM provides a set of specialized placeholders that are not replaced by OMM-specific values in the ipdect.cfg file. These placeholders are used in AXI commands to reference the MOM interface for the path to resource files and OMM credentials for access to OMM-specific folders on the MOM server.

You do not specify OMM-specific values for these placeholders. The MOM automatically replaces the placeholders with the appropriate values when generating the ipdect.cfg file.

Placeholder name	Description
%MOM_IP_ADDR%	IP address of the MOM interface
%MOM_WEB_HTTPS_PORT%	Port of the MOM interface
%MDB_OMM_cloud_id%	OMM Cloud-ID
%MDB_OMM_username%	User name of the account used to access the OMM
%MDB_OMM_password%	Password for the account used to access the OMM

URL for common resource files

You can provision the MOM as the source for OMM resource files. For example, the following AXI command specifies the resources directory on the MOM server as the source for the customer logo file (when the special branding feature is enabled):

```
<SetSpecialBranding plainText="1">
   <url enable="true"
       protocol="HTTPS"
       host="%MOM_IP_ADDR%"
       port="%MOM_WEB_HTTPS_PORT%"
       path="resources"
       useCommonCerts="true"/>
</SetSpecialBranding>
```

The generated ipdect.cfg file sets the URL for the custom branding image to the resources folder on the MOM server.

URL for OMM-specific resource files

You can provision the MOM as the source for OMM-specific resource files. For example, the following AXI command enables the Integrated Messaging and Alerting (IMA) service and specifies the OMM-specific folder on the MOM server as the source for the ima.cfg file:

```
<SetIMA enable="1">
   <url enable="1" plainText="true"
       protocol="HTTPS"
       host="%MOM_IP_ADDR%"
       port="%MOM_WEB_HTTPS_PORT%"
```

```
       path="/omm_files/Cloud-ID-%MDB_OMM_cloud_id%/ima.cfg"
       username="%MDB_OMM_username%"
       password="%MDB_OMM_password%"
       useCommonCerts="1"/>
</SetIMA>
```

> **Note:** For this scenario, you must create the OMM folder on the MOM server, and copy the ima.cfg file to the directory.

URL for OMM file storage

You can also provision the OMM to write to the protected folder on the MOM (for example, to store a system dump or automatic database backup). For example, the following AXI command specifies the OMM-specific backup directory on the MOM server as the destination for remote OMM database backups:

```
<SetAutoDBBackup plainText="true">
   <url enable="1"
       protocol="HTTPS"
       host="%MOM_IP_ADDR%"
       port="%MOM_WEB_HTTPS_PORT%"
       path="/omm_files/Cloud-ID-%MDB_OMM_cloud_id%/Backup"
       username="%MDB_OMM_username%"
       password="%MDB_OMM_password%"
       useCommonCerts="1"/>
</SetAutoDBBackup>
```

The generated ipdect.cfg file sets the OMM's auto backup URL to use the OMM-protected folder on the MOM server to store backup files.

MAXI interface for applications and provisioning

The MOM provides an interface (MAXI), based on the AXI protocol, that allows applications to communicate with the MOM. In addition to enabling MOM provisioning, the interface enables system wide messaging and a data channel that allows remote AXI applications to communicate.

The maximum number of concurrent MAXI connections to the MOM is 8.

> **Note:** The MAXI protocol is based on the AXI protocol, but not all AXI commands are supported. Detailed AXI / MAXI specifications are available to registered partners through the Mitel MSA program.

System Wide DECT messaging

The MOM supports DECT messaging between DECT phone users no matter where they are located in the system. OMMs can transmit DECT messages to other OMMs via the MOM.

Application data channel

Through the MAXI, the MOM provides a data channel for local OMM applications to communicate with each other through a central application connected to the MOM. This functionality means that applications do not need to maintain multiple connections to various sites.

MOM interface

You can access the MOM interface from a web browser (e.g., https://<server-IP-address>/).

> **Note:** At the first time the browser will notify that an untrusted certificate is used. Configure the browser to always trust the MOM certificate.
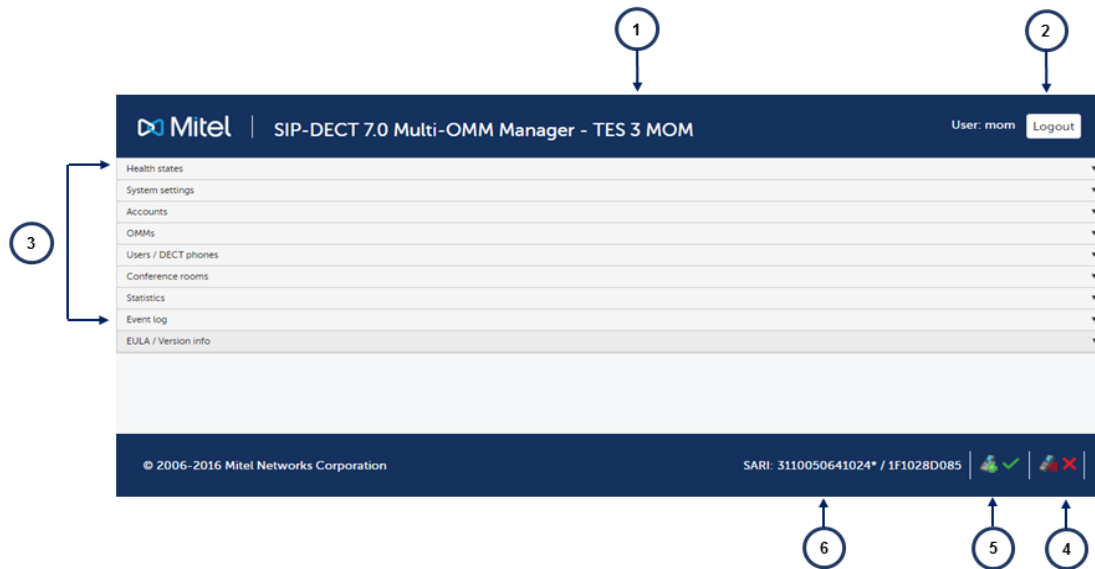
1	System name
2	Login area
3	Configuration panes
4	DECT phone subscription status: enabled (Subscription | Wildcard) | disabled (Off)
5	Auto-create status (enabled / disabled)
6	DECT identifier for the system

Configuration panes

The MOM interface includes multiple panes that contain different information about the SIP-DECT system.

- **Health states**: displays a summary of license and OMM connection state

- **System settings**: contains system wide settings

- **Accounts**: contains a list of accounts created for MOM access

- **OMMs**: contains a list of all OMMs in the SIP-DECT system

- **Users/DECT phones**: contains a list of all user and device datasets in the system

- **Conference rooms**: contains a list of all conference rooms configured for the system

- **Statistics**: displays counters of statistics related to MOM operations

- **Event log**: displays events related to MOM operations

- **EULA / Version info**: displays the End User License Agreement and the version of the MOM software currently installed

The operations you can perform depends on which pane is open. See "Multi-OMM Manager Installation and Configuration" on page 13 for detailed configuration procedures for each pane.

Customizing the data display

The MOM displays information about system entities (e.g., OMMs, user/device records, conference rooms) in tables. By clicking on any column header you can:

• sort table data in ascending or descending order, based on the field in the header. The order of the tables (MOM Web-GUI) has 3 states:

   • Ascending

   • Descending

   • None (data record changes do not change the sorting order, new records are appended to the end of the table)

• filter table data by selecting the **Filter** option, setting specific filter criteria (filters are not persistent)

• show or hide columns (only for tables without tabs)

Note: The MOM web service use a web framework based on JavaScript; the interface is automatically updated via active web socket connections. Do not use F5 or page-forward/page-back browser functions to refresh the interface, as it will close the current session.

Chapter 2

Multi-OMM Manager Installation and Configuration

Getting started with the Multi-OMM Manager

Review the system requirements described below before installing the Multi-OMM Manager (MOM) application.The SIP-DECT system, to which the MOM is getting connected is done with basic setup configuration (including license, PARK, DECT base stations).

For detailed instructions, see the following sections:

- "System requirements" on page 14

- "Installing the MOM software" on page 14

- "Logging in and setting the system name" on page 15

- "Importing the MOM license file" on page 16

System requirements

The MOM is installed on a dedicated Linux server or on VMware environments. The following are the minimum requirements for hosting the MOM application:

- Platform: Virtualized (VMware ESX) or physical server

- CentOS 6 or RHEL 6 Linux (x64) operating system

- 80 GB Hard Disk

- 8 GB RAM

- 4 x 2.5GHz CPU

- 1 GE network interface

    Note: Additional Linux packages may be required for MOM installation. See SIP-DECT Knowledge Base article *OMM Linux Server Installation* for more information.

In addition, configure any firewalls to allow incoming connections on the following ports:

- MAXI (SSL): 12624/TCP

- HTTPs: 443/TCP

- HTTP: 80/TCP (optional, to redirect to HTTPs)

All connected SIP-DECT systems must be running SIP-DECT release 7.0 or higher. The OMMs and the MOM must be running the same software version to synchronize properly.

   Note: NTP must be configured on the MOM server.

Installing the MOM software

You can install the MOM software using the RPM Package Manager (RPM) utility.

To install the MOM software, do the following:

1. Log in as root, or use the `su` command to change to the root user on the server; on which you want to install the MOM software.

2. Download the MOM package (SIP-DECT-MOM-<version>.i686.rpm).

3. Enter the following command at the prompt:

    ```
    rpm -i SIP-DECT-MOM-<version>.i686.rpm
    ```

4. When installation is complete, enter the following command to start the MOM service:

    ```
    /etc/init.d/sip-dect-mom start
    ```

Once you have installed the MOM software on the Linux server, you can log in to the MOM application for initial configuration.

For information about how to remove the MOM software or upgrade to a new version, see "MOM system maintenance" on page 34.

Logging in and setting the system name

You must have a valid user account to log in to the MOM. You can use the system default account for the first login.

To log in to the MOM interface, do the following:

1. Open a browser and enter the URL for the MOM interface (**https://<server-IP-address>**).

    > **Note:** A Certificate warning will be shown as the certificate used cannot be validated. You must add an exception to establish the connection.

2. Enter the user name and password in the log in fields
    The first time you log in to the MOM application, use the system default account (user name "mom", password "mom").
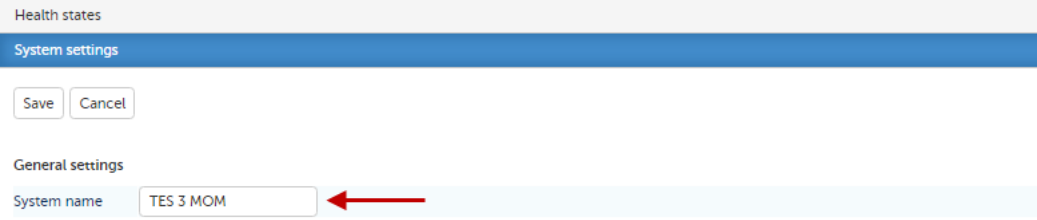

3. Click **Login**.

    At first login (or when there is a software version change), the system prompts you to accept the End User License Agreement (EULA).

4. Review the EULA and click **Accept** above the EULA panel.

5. Change the default password for the MOM system account.

    At first login only opens the Accounts pane with the default account automatically, after you have accepted the EULA.

    a. Specify a new password for the account. The password must meet the following criteria:
        *   must not be more than five characters long
        *   must not contain characters from at least three of the following groups:
        -   lower case
        -   upper case
        -   digits or other characters
        *   must contain 50% or more of the same character ('World11111' or 'W1o1r1l1d1')
        *   must contain one of the following items (either upper or lower case and forward or backward):
        -   account name
        -   host name (IP address)

15

- old password
- some adjoining keystrokes (for example, 'qwert')

    b. Click **Update** to apply your changes.

6. Specify a system name for the MOM.

    a. Click on **System settings** to open the system settings pane.

    b. Under **General settings**, specify a name for the system in the **System name** field.

    c. Click **Save** to apply your changes.

Importing the MOM license file

The MOM license file contains the license, the Secondary Access Rights Identifier (SARI), the licensed version, the customer name, the country of installation and an installation ID. Any subsequent license imports are validated against this installation ID.
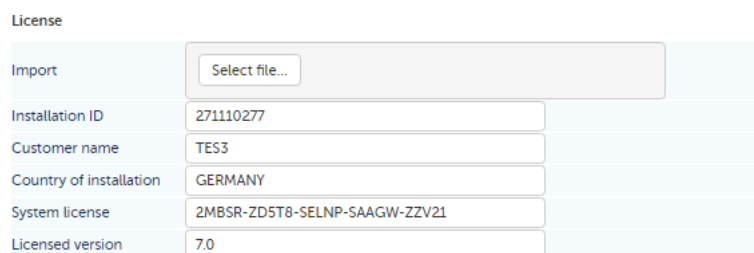
The MOM license applies to the entire SIP-DECT system (i.e., the license is not site-specific, as with the OMM license).

To import the MOM license file, do the following:

1. Click on **System settings** to open the system settings pane.

2. Scroll to the **License** section.

3. In the **Import** field, click on **Select file**.

4. Browse to the location of the MOM license file and click **Open**.

   The system imports the license file into the MOM application.

5. Verify that the following fields (under **License**) are populated:

- **Installation ID**
- **Customer name**
- **Country of installation**
- **System license**
- **Licensed version**

6. Verify that the **SARI** field is populated (under **DECT settings**).

DECT settings

SARI	1F1028D085 ←
Auto-create	☐
Subscription	Off ▼

Centralized OMM management

You can manage OMM provisioning from the MOM interface. You can customize the configuration template and create OMM-specific provisioning files by specifying placeholder values for individual OMMs.

It is important to ensure that OMM configuration includes a common feature set for all OMMs, so that users do not experience different system behaviors when roaming between sites. In particular, consider the following features for consistency in OMM configuration:

- Enhanced DECT security (enabled or disabled)

- availability of corporate directory access

- availability (and order) of XML applications

- user login type (by number or ID)

- configuration of supplementary services (local call forwarding, dial editor, branding, etc)

- Configuration over Air (CoA) profiles (content, order, availability); should be identical across OMMs

- Feature access codes

  Note: If the User Data import is used, all OMMs must be able to access the same data.

For detailed instructions, see the following sections:

- "Adding OMM records to the MOM" on page 18

- "Modifying the configuration template" on page 19

- "Configuring OMM-specific placeholder values" on page 21

- "Verifying the OMM configuration" on page 22

Adding OMM records to the MOM

You must add an entry for every OMM in the system that you want to manage from the MOM. The OMMs must have basic configuration before connecting to the MOM. Since the synchronization of data depends on timestamps, NTP must be configured properly in each OMM.

  Note: The MOM server must also use NTP, not only the OMMs.

To add an OMM record, do the following:

1. Click on **OMMs** to open the list of configured OMMs.

2. Click on **Add new record** to add an entry for a new OMM.

3. Enter the following information for the new OMM:

   - **Name**: name to identify the OMM site.

   - **Description**: information to describe the OMM site (optional).

   - **OMM 1**: the IP address of the OMM 1.

   - **OMM 2**: the IP address of the OMM 2 (if OMM1 is available, automatically detected by the MOM).

   - **User**: user name of the account (with full access rights) used to access the OMM.

   - **Password**: password for the account (with full access rights) used to access the OMM.

   - **Provisioning**: enable if you want to manage OMM provisioning centrally from the MOM.

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

> **Note:** When connecting to the OMM, the MOM configures the Secondary Access Rights Identifier (SARI) on the OMM, which triggers an OMM restart. The MOM also synchronizes user and device data from the OMM (if available).

When the MOM connects to the OMM you added, it derives the Cloud-ID for the OMM from the PARK associated with the OMM (i.e., 00-<PARK>). The MOM populates the Cloud-ID field of the OMM record with this value.

Optionally, you can click on the IP address of the OMM record (**OMM 1** or **OMM 2** field) to open the OMM web interface in a new browser window.

Modifying the configuration template

You can customize the configuration template to set system wide parameters appropriate for your SIP-DECT system.

Use the following checklist for OMM provisioning:

- system settings (Name, Tone, Time, SW Update, DECT authentication code)

- advanced settings (QoS, Voicemail, Dial Editor, NTP, IMA)

- SIP settings (central and local SIP servers, Call Server settings)

- system features (Directory, XML applications, Feature Access Codes, CoA profiles)

- file management (Backup, User Data Import)

- Monitoring (SNMP, Syslog, Remote Access, Core dump, System dump)

> **Note:** The following settings are not provisioned by the MOM and must be configured locally:
>
> - local DECT base station settings (Software update URL, Startup Config, Config Files)
> - DECT base station configuration
> - Wireless LAN settings digit treatment

To customize the configuration template, do the following:

1. Click on **OMMs** to open the list of OMM records.
2. Click on **Configuration file template** in the main MOM window.
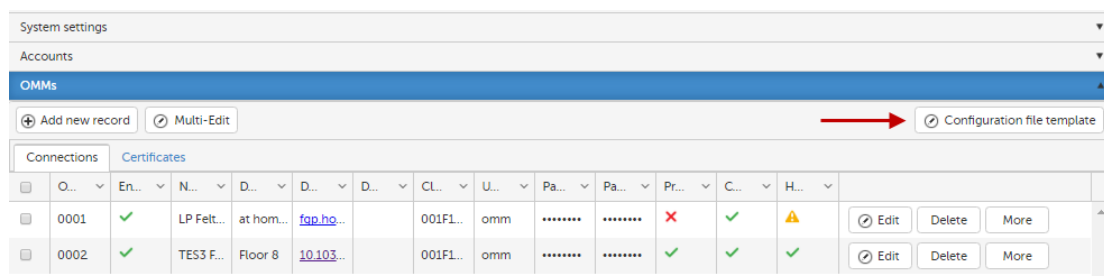
3. In the **OMM configuration template** window, modify the parameters that you want to set for all OMMs in the system.

   a. Uncomment the appropriate AXI command.

   b. Select the attributes you want to set (and remove the attributes you do not want to set).

   - If you want a fixed value provisioned across all OMMs, replace the placeholder value with a fixed value.

     For example, to enable remote access on all OMMs in the system, enter the following:

     ```
     <SetRemoteAccess enable="true" />
     ```

   - If you want to provision different values in different OMMs, leave the placeholder value in the attribute/placeholder pair.

   - If you want to apply an AXI command to one specific SIP-DECT system only, add the cloud-ID attribute to the AXI command and specify the system Cloud-ID as the attribute value.

     ```
     <SetRemoteAccess cloudId="<cloud-Id>" enable="true" />
     ```

     (where <cloud-ID> is the actual cloud-ID of the SIP-DECT system you want to provision).

> **Note:** The values you specify in the configuration file template are applied to all OMM provisioning files generated by the MOM, unless you specify a Cloud-ID for a particular AXI command.

For example, the following AXI commands include instructions regarding SIP configuration:

```
<SetBasicSIP
   transportProt="%BasicSIP_transportProt%"
   proxyServer="%BasicSIP_proxyServer%"
   proxyPort="5060"
   outboundProxyServer="%BasicSIP_outboundProxyServer%"
   outboundProxyPort="%BasicSIP_outboundProxyPort%"
   regServer="%BasicSIP_regServer%"
   regPort="%BasicSIP_regPort%"
   regPeriod="%BasicSIP_regPeriod%"
   gruu="%BasicSIP_gruu%" />
<SetRemoteAccess enable="true" />
```

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

Configuring OMM-specific placeholder values

When you configure placeholder values for a specific OMM, the MOM uses those values to generate an OMM provisioning file from the configuration file template.

> **Note:** OMM configuration should provide a common feature set for all users. If system features are configured differently across OMMs, users will experience different system behaviour when roaming between sites.

You must perform this procedure for every OMM whose provisioning you want to manage from the MOM.

To configure placeholder values for an OMM, do the following:

1. Click **OMMs** to open the list of connected OMMs.

2. Click **More** beside the OMM entry you want to provision and select **Edit placeholders** from the drop-down menu.

3. In the **OMM configuration data** window, type the placeholder/value pairs for the parameters you want to set on the OMM.

    For example, the following AXI commands include specific values for the SIP placeholders contained in the configuration file template:

    ```
    BasicSIP_transportProt=UDP
    BasicSIP_proxyServer=10.103.35.70
    BasicSIP_proxyPort=5060
    BasicSIP_outboundProxyServer=
    BasicSIP_outboundProxyPort=5060
    BasicSIP_regServer=10.103.35.70
    BasicSIP_regPort=5060
    BasicSIP_regPeriod=3600
    BasicSIP_gruu=true
    ```

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

5. Verify the contents of the OMM configuration file by clicking on **More** and selecting **Show config file** from the drop-down menu.

6. Click **More** beside the OMM entry you want to provision and select **Update OMM** from the drop-down menu.

After a short interval, the OMM requests the ipdect.cfg file from the MOM, and executes the AXI commands contained in the OMM provisioning file provided by the OMM.

7. Verify the health state of the OMMs (Refresh if table changes are suppressed). If not OK, check the Event Log or system log of the OMM(s) for errors in ipdect.cfg.

Verifying the OMM configuration

You can verify the OMM provisioning changes downloaded from the MOM from the OMM web interface or the OM Management Portal (OMP).

To verify that the configuration file has been successfully loaded onto the OMM, do one of the following:

1. To launch the OMP:

   a. Click **More** beside the OMM entry and select **Start OMP** from the drop-down menu. The OMP jar file is downloaded to your local machine.

   b. Double-click on the downloaded OMP.jnlp file and click **Run** when prompted to run the application.

   c. Navigate to the **System** > **Provisioning** menu and verify that the **Configuration files URL** section (on the **Provisioning** tab) identifies the provisioning server with the IP address of the MOM server.

   d. Verify that the system configuration is correct. See the *SIP-DECT System Manual* for a detailed description of the OMP interface and parameters.

   e. Verify the health states and the event log.

2. To launch the OMM web access:

   a. Click the address in the **OMM 1** field of the OMM entry you want to provision. The OMM interface opens in a new browser tab.

   b. Log in with the OMM full access credentials.

   c. Navigate to the **System** > **Provisioning** menu and verify that the **Current configuration file URL** section identifies the provisioning server with the IP address of the MOM server.

   d. Verify that the system configuration is correct. See the *SIP-DECT System Manual* for a detailed description of the OMM interface and parameters.

   e. Verify the health states and the event log.

Centralized user and device data management

When you add an OMM entry to the MOM, the MOM automatically synchronizes the user and device data associated with that OMM. You can create new user and device data records from the MOM interface, and modify existing records.

> **Note:** Devices that are already subscribed to the OMM are imported into the MOM system. If the OMM PARK is equal to the MOM SARI, roaming between all OMMs is enabled. Otherwise the devices are imported with no roaming capabilities.

For more information, see the following sections:

Configuring DECT phone subscription

When the MOM connects to an OMM, the MOM sets the SARI on the OMM. From then on, all DECT phones use the SARI when subscribing to the OMM.

You must enable Auto-create on Subscription functionality on the MOM. This option allows the MOM to create a new (unbound) device data record for every DECT phone that subscribes to the system, if none exists already. If Auto-create on Subscription is not enabled, only user/device datasets that already exist in the MOM can subscribe to the system.

You can configure DECT phone subscription options from the **System settings** menu or using the icons in the bottom ribbon of the MOM interface.

To configure DECT phone subscription from the MOM configuration pane, do the following:

1. Click on **System settings** to open the system settings pane.

2. Under **DECT settings**, select the **Auto-create** option to enable auto-create on subscription.

3. In the **Subscription** field, select one of the following subscription modes:

    - **Off**: subscription is disabled

    - **Subscription**: subscription is enabled only for devices with configured IPEIs or auto-to-create on subscription

    - **Wildcard**: subscription is enabled for devices without configured IPEIs (additional ID is required for successful subscription)

4. Click **Save** to apply your changes.

When you apply your changes, the MOM distributes the selected subscription mode in all connected OMMs. DECT phones can then begin the subscription process.

To configure DECT phone subscription using the icons in the MOM interface, do the following:

1. To enable Auto-create on Subscription, click on the Auto-create icon in the bottom-right corner of the MOM interface (the icon has a green check mark when enabled).

> **Note:** For Auto-create on Subscription the authentication code (AC), which is set in the OMM the phone subscribes to, is used.

2. To enable DECT phone subscription, click on the **Subscription** icon in the ribbon at the bottom of the MOM interface and select the appropriate subscription mode from the pop-up menu (options described below).
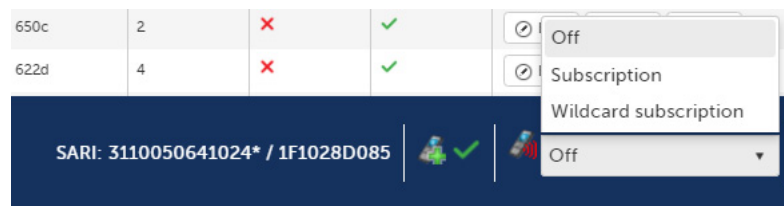
Unsubscribing DECT phones

You can unsubscribe a DECT phone (only with relation type fixed) using the system from the MOM interface.

To unsubscribe one or more DECT phones, do the following:

1. Click on **Users/DECT phones** to open the user/device records pane.

2. Open the pull-down menu in the **Change view** field and select **Devices**.

3. Do ONE of the following:

   a. To unsubscribe a single device, click the **More** button beside the entry and select **Unsubscribe** from the pull-down menu.

   b. To unsubscribe multiple devices, select the entries from the list (by clicking the check box beside each entry), then click the **More** button at the top of the User/DECT phones section and select **Unsubscribe** from the pull-down menu.

The DECT phone is unsubscribed from the system, and the dataset(s) removed from the OMM databases.
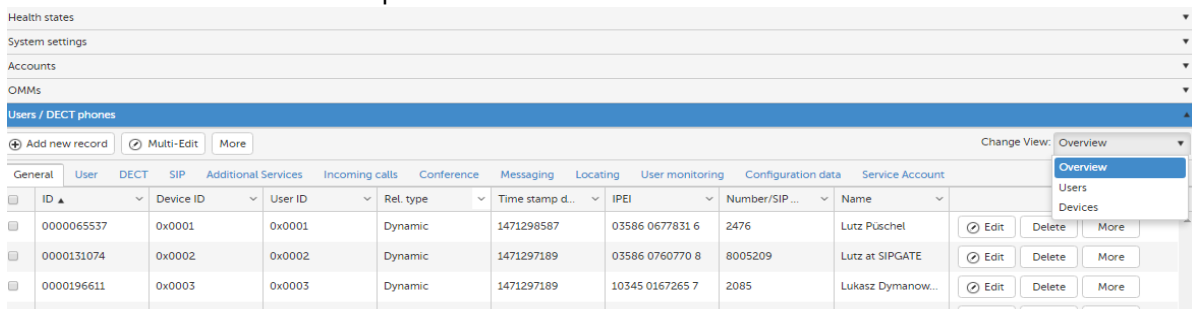
Viewing user and device data sets

You can filter the display of data records in the MOM interface to view only bound user and device records, all user records, or all device records.

To filter the user/ DECT phone data set display, do the following:

1. Click on **Users/DECT phones** to open the user/device records pane.

2. Use the pull-down menu in the **Change view** field to filter the data records shown in the user/device records pane.


a. Select **Overview** to view user and device data sets with a fixed or dynamic relationship.

b. Select **Users** to view only user data sets (bound and unbound).

c. Select **Devices** to view only device data sets (bound and unbound).

The MOM **User/DECT phones** panel updates to show the filtered results.

Adding a new data set

You can use a user (unbound) or user with device (fixed) record to the MOM application manually. The current view selected in the **Users/DECT phones** section of the MOM interface determines the type of record you create when you click **Add new record**.

For example, if the current active tab is the **General** tab, a new (fixed) user/device record is created. If the current active tab is the **User** tab, a new (unbound) user record is created. You configure the parameters in the same way as you configure them in the OMM web service or the OMP.
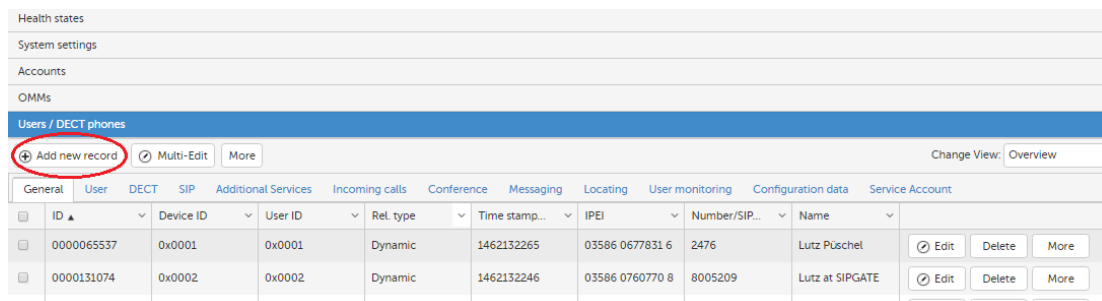
For more information, see the following sections:

- "Adding a fixed user/device record" on page 25

- "Adding an unbound user record" on page 26

- "Creating a user/device data set from an existing record" on page 26

Adding a fixed user/device record

To create a new user/device record, do the following:

1. Click on **Users/DECT phones** to open the user/device records pane.

2. In the **Change View** field, select **Overview**.

3. Select the **General** tab.

4. Click on **Add new record**.

5. In the new record entry, specify values for the following parameters:
    *   **IPEI:** the unique identifier for the DECT phone.
    *   **Number/SIP user name**: the SIP account number or extension for the DECT phone
    *   **Name**: the SIP display name for the DECT phone.

6. Click **Update** to apply your changes.

Adding an unbound user record

To create a new user record, do the following:

1. Click on **Users/DECT phones** to open the user/device records pane.

2. In the **Change View** field, select **Users**.

3. Click on **Add new record**.

4. In the new record entry, specify values for the following parameters:
    *   **Number/SIP user name**: the SIP account number or extension for the user
    *   **Name**: the SIP display name for the user
    *   **Login/Additional ID**: additional identifier for the user account (can be used to for select a record during wildcard subscription of a device)
    *   **Description 1**: optional text string with additional information on the user
    *   **Description 2**: optional text string with additional information on the user
    *   **PIN**: a unique identifier that the user must enter on the phone at login
    *   **PIN confirmation**: confirmation of the PIN for the user
    *   **Permanent**: flag to indicate that the user dataset is deployed to all OMMs, so that the user can roam between sites even if the connection between OMM and MOM is down. The number of permanent users is limited to 512.
        Permanent users cannot be provisioned externally (i.e., have type "External").

5. Configure additional parameters on the remaining tabs in the same way that you configure user data parameters on the OMM web service or the OMP.

6. Click **Update** to apply your changes.

Creating a user/device data set from an existing record

You can use an existing user or device record to create a new record, without having to re-configure common information.

To create a new user or device data record from an existing record, do the following:

1. Click on **Users/DECT phones** to open the user/device records pane.

2. Select the record you want to copy.

3. Click on **More** and select **Copy** from the drop-down menu.

    A new record appears (in Edit mode) with pre-populated parameters (i.e., populated with the values of the record you copied).

4. Specify the necessary values for the new record and click **Update** to apply your changes.

Modifying user and DECT phone data sets

You can manage configuration of user/DECT phone data sets from the MOM interface.

For more information, see the following sections:

Changing the relation type of bound user/device data sets

User/device data sets that are bound to each other have a fixed or dynamic relationship. The system changes the user/device relationship type.

To change the user/device relationship type, do the following:

1. Click on **Users/DECT phones** to open the user/device records pane.

2. Open the pull-down menu in the **Change view** field and select **Overview** to display only user/device data sets that are bound.

3. Do ONE of the following:

   a. To change the relation type for a single user/device data set, click the **More** button beside the entry and select **Rel. type** from the pull-down menu. The option is only available if the device is subscribed and the current type of relation is Dynamic or Fixed.

   b. To change the relation type for multiple user/device data sets, select the entries from the list (by clicking the check box beside each entry), then click the **More** button at the top of the User/DECT phones section and select **Rel. type** from the pull-down menu. The option is only available if within all selected data sets the devices are subscribed, and the current types of relation are uniformly Dynamic or Fixed.

   You can filter the records displayed by clicking the down arrow in the field header and selecting the **Filter** option. Select the operator (e.g., 'is equal to'), specify the field value you want to sort on (for example, Fixed), and click **Filter.**

   Note: When modifying multiple entries at once, the selected entries must have the same type of user/device relationship. If you select entries with mixed relation types, the **Rel. type** option is disabled in the pull-down menu.

The system changes the user/device relationship type.

Changing the provisioning source for a user data set

A user data set can be provisioned on an external user data server or locally in the OMM database. You can move user data sets from an external user data server (External) into the local OMM database (Internal).

You cannot move datasets from the OMM database (Internal) to an external data server (External).

To change the provisioning source for an unbound user data set, do the following:

1. Click on **Users/DECT phones** to open the user/device records pane.

2. Open the pull-down menu in the **Change view** field and select **Users** to display all user data sets.

3. Do ONE of the following:

   a. To change the provisioning source for a single user data set, click the **More** button beside the entry and select **Source** from the pull-down menu. This option is only available if the current relation type is Dynamic.

   b. To change the provisioning source for multiple user data sets, select the entries from the list (by clicking the check box beside each entry), then click the **More** button at the top of the User/DECT phones section and select **Source** from the pull-down menu. This option is only available if the current relation type for all selected data sets is Dynamic.

The system changes the provisioning source for the user data set(s).

Editing user or device data sets

You can change the configuration of user and device data sets in the MOM database.

The parameters available for configuration correspond to the device and user data record fields that you can configure from the OMM or OMP. For a description of each parameter, see the *SIP-DECT OM System Manual*.

To edit an existing user / DECT phone record, do the following:

1. Click on **Users/DECT phones** to open the user/device records pane.

2. Open the pull-down menu in the **Change view** field and select the option to display the data sets you want to modify:

   • **Overview** to display only user/device data sets that are bound

   • **Users** to display all user data sets

   • **Devices** to display all DECT phone data sets

3. Select the record you want to change and click **Edit**.

   Note: You can modify multiple records in one operation. Select the entries that you want to configure, and click on **Multi-Edit**. Any value that you enter in an active field is applied to each selected record. Multi-Edit only works within the current page (selecting and editing some or all entries of the current page).

4. Click on the tab that contains the parameters you want to change and make any necessary changes. You can change parameters in more than one tab, as required.

5. Click **Update** to apply your changes.

Deleting a user or DECT phone record

You can delete an existing device or user data record from the MOM interface. The dataset is also removed from the local OMM if connected.

To delete an existing user / DECT phone record, do the following:

1. Click on **Users/DECT phones** to open the user/device records pane.

2. Select the record you want to change and click **Delete**.

3. Click OK in the **Delete confirmation** dialog window.

The record is removed from the MOM database. In case, the local OMM is not connected with the MOM, the data records is recreated within the MOM after reconnection.

Additional system configuration

You can configure the following functionality for the SIP-DECT system from the MOM interface:

- "Setting a global FAC prefix" on page 30
- "Managing MOM user accounts" on page 30
- "Managing conference rooms" on page 31

Setting a global FAC prefix

You can configure a system wide Feature Access Code (FAC) prefix to be dialed whenever a DECT phone user wants to enter a FAC access code associated with a specific system function.

When you configure a global FAC prefix via the MOM interface, the setting is propagated to individual OMMs in the system (i.e., in the **System Features** > **Feature Access Codes** page in the OMM web service and the **System features** > **General settings** page in the OMP).

The FACs configured for different actions (e.g., user login) can be set individually per OMM. However, it is recommended that you provision identical FACs in all OMMs (e.g, through provisioning files) to ensure that roaming users can use the same FACs at all SIP-DECT sites.

To configure system wide FAC prefix, do the following:

1. Click on **System settings** to open the system settings pane.

2. Under **System features**, specify a value in the **FAC number** field.

3. Click **Save** to apply your changes.

   Note: When deploying the MOM, it overwrites the FAC prefix set in the OMMs.

Managing MOM user accounts

You can create additional accounts for MOM access, for login through the web service or access via the MAXI interface (used by applications). You can assign read-only permissions, or read-write permissions to each account.

All accounts have messaging permission for MAXI-to-OMM messaging.

See the following sections for more information:

- "Adding or modifying a MOM user account" on page 30
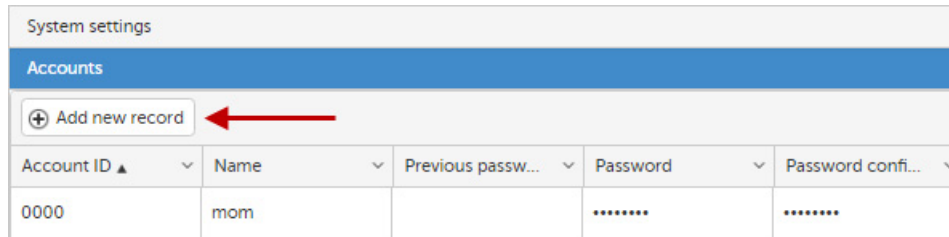- "Deleting a MOM user account" on page 31

Adding or modifying a MOM user account

To create or modify a MOM user account, do the following:

1. Click on **Accounts** to open the system user accounts pane.

2. Do ONE of the following:
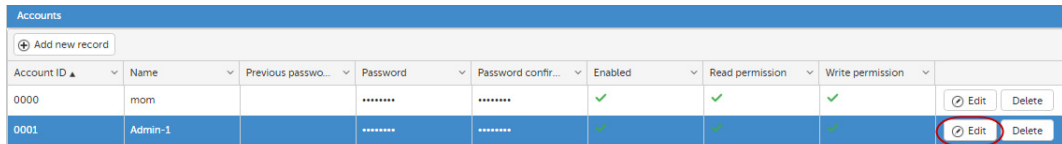
a. To create a new account, click **Add new record**.

b. To modify an existing account, locate the entry for the account and click **Edit**.

3. Specify a value for one or more of the following parameters, as required:
   - **Name**: login name for the account
   - **Previous password**: the current password for an existing account
   - **Password**: the new password for the account
   - **Enabled**: activates or deactivates the account (if not selected, all fields are disabled)
   - **Read permission**: allows read permissions for the system; always enabled.
   - **Write permission**: enables permissions to make system changes for the account

4. Click **Update** to apply your changes.

   The system displays the updated account information in the accounts list.

Deleting a MOM user account

To remove an existing MOM account, do the following:

1. Click on **Accounts** to open the system user accounts pane.

2. Locate the table entry of the account you want to remove and click on **Delete**.

3. In the **Delete confirmation** dialog, click **Ok**.

   The system removes the account from the accounts list.

   Note: It is not possible to delete the default account.

Managing conference rooms

The Integrated Conference Server (ICS) feature offers three-way conferencing to SIP-DECT users who are hosted on SIP servers that do not provide a conference solution. You can manage individual conference rooms for the SIP-DECT system from the MOM interface.

See the following sections for more information:
- "Adding or modifying a conference room" on page 31
- "Deleting a conference room" on page 32

Adding or modifying a conference room

To create a conference room, do the following:

1. Click on **Conference rooms** to open the conference room pane.

2. Do ONE of the following:

   a. To create a new conference room, click **Add new record**.

   b. To make changes to an existing conference room, locate the entry in the list and click **Edit**.

3. Specify values for the following parameters:

   • **Name**: Display name for the SIP account to be used to register the conference room on the SIP registrar

   • **Number**: SIP user ID

   • **OMM ID**: the identifier of the OMM hosting the conference room

     - by changing one OMM ID value to another, the conference room is 'moved' from the former OMM to the new OMM system.

     - supplying the invalid OMM ID value 0 is possible to save the conference room data, but the room is not assigned to a specific OMM system.

   • **SIP user**: SIP authentication name

   • **SIP password**: password required by the SIP server for authentication

   • **Fixed port**: port used explicitly for SIP signaling. If set to 0, the system uses an automatically calculated port for the conference room.

4. Click **Update** to apply your changes.

Deleting a conference room

To remove an existing conference room, do the following:

1. Click on **Conference rooms** to open the conference rooms pane.

2. Locate the entry of the conference room you want to remove and click on **Delete**.

3. In the **Delete confirmation** dialog, click **Ok**.

   The MOM removes the conference room from the system.

Chapter 3

Multi-OMM Manager Maintenance and Administration

MOM system maintenance

You can perform standard maintenance procedures from the MOM interface, such as downloading a system dump file or importing and exporting the MOM database.

For more information, see the following sections:

- "Managing the MOM database" on page 34
- "Upgrading the MOM software" on page 35
- "Removing the MOM software" on page 35
- "Downloading the system dump file" on page 36
- "Managing browser notifications" on page 36

Managing the MOM database

The MOM database contains all of the configuration settings and user and device data sets in the system. You can import or export the MOM database manually from the MOM interface.

For more information, see the following sections:

- "Exporting the MOM database" on page 34
- "Importing the MOM database" on page 34

Exporting the MOM database

You can create a backup of the MOM database by exporting a copy of the database to your local machine.

To export the MOM database to your local machine, do the following:

1. Click on **System settings** to open the system settings pane.

2. Under **DB management**, click **Download** beside the **Export** field.

   The web browser copies the MOM database to your local Downloads folder.

Importing the MOM database

You can restore a MOM database using the import function. You must restart the system after importing the database for changes to take effect.

To import a database file from your local machine, do the following:

1. Click on **System settings** to open the system settings pane.

2. Under **DB management**, click **Select file** beside the **Import** field.

3. Navigate to the location of the database file to be imported and click **Open**.

   The MOM imports the file into the database.

4. Click **Restart** to restart the system and apply the changes.

> **Note:** When the MOM starts up again, it synchronizes data with connected OMMs. OMM data with more recent timestamps might replace older data that exists in the MOM backup database.

Upgrading the MOM software

For systems where the MOM application is already installed, you can upgrade the MOM software version without removing the existing application.

> **Note:** Upgrading the MOM software does not result in an upgrade of any connected OMMs. OMM software must be upgraded separately.

To upgrade the MOM software, do the following:

1. Log in as root, or use the `su` command to change to the root user on the workstation hosting the MOM.

2. Download the new MOM package (SIP-DECT-MOM-<version>.i686.rpm).

3. If the MOM is currently running, stop the MOM service with the following command:

   `/etc/init.d/sip-dect-mom stop`

4. Enter the following command at the prompt:

   `rpm -U SIP-DECT-MOM-<version>.i686.rpm`

   (where SIP-DECT-MOM_<version> is the name of MOM software file you are installing)

5. When the upgrade is complete, enter the following command to start the MOM service:

   `/etc/init.d/sip-dect-mom start`

   > **Note:** This procedure terminates the AXI connection to the OMMs.

If the protocol versions of OMM and MOM differ the AXI connections stay disconnected until the OMMs are updated. The MOM does not enable roaming or publish any changes in the user / device configuration while the AXI connection to the OMMs is down.

When you update the OMMs to recover the AXI connection with the OMMs, the MOM reconnects to the OMMs and starts to sync data again. The MOM tries to reestablish the connection every minute until the protocol version matches.

Removing the MOM software

You can remove the MOM application software from the service, but preserve the MOM database and resource files.

To remove the MOM software from the server, do the following:

1. Log in as root, or use the `su` command to change to the root user on the workstation hosting the MOM.

2. If the MOM is currently running, stop the MOM service with the following command:

   `/etc/init.d/sip-dect-mom stop`

3. Enter the following command at the prompt:

   `yum remove SIP-DECT-MOM`

If you want to install a new version of the MOM software, see "Installing the MOM software" on page 14.

Downloading the system dump file

A system dump is a file for diagnostic purposes that contains information about the MOM and its configuration. You can download the system dump file to your local machine from the MOM interface.

To download the system dump file, do the following:

1. Click on **System settings** to open the system settings pane.

2. Under **System dump**, click **Download** to download the system dump file (mom_sys_dump_<uniqueID>.txt.gz) to your local machine.

General settings	
System name	TES 3 MOM
DECT settings	
SARI	1F1028D085
Auto-create	☐
Subscription	Off ▾
System features	
FAC number	
System dump	
Store system dump file	Download
DB management	

The system copies the file to your local Downloads folder.

Managing browser notifications

All changes in the MOM are communicated to connected web browsers. If the MOM is processing large amounts of data, these notifications increase the traffic load on the browser application.

You can suppress updates to the connected web clients to reduce notifications and limit the burden on the browser application. With this feature enabled, the user must refresh content manually to see updated information.

> **Note:** By default notifications are suppressed. So, configuration is needed to get live updates.

To suppress browser notifications, do the following:

1. Click on **System settings** to open the system settings panel.

2. Under **General settings**, select a mode from the pull-down menu in the **Suppress Table Updates** field:

    *   **Off**: all updates are sent to the browser (no manual refresh required except for statistics)

    *   **Users / DECT phones**: updates to user/device information are suppressed (manual refresh required in **Users/ DECT phones** panel)

    *   **All**: all data updates are suppressed (manual refresh required for all panels)

3. Click **Save** to apply your changes.

MOM monitoring and troubleshooting

You can view system statistics and event logs from the MOM interface.

> **Note:** MOM log files are stored in the `/opt/SIP-DECT-MOM/mom_trace_<date>.log` file.

For more information, see the following sections:

Viewing system health state

The MOM provides information about the license and OMM connection status in the Health states panel.

To view the system health state, do the following:

1. Click on **Health states** to open the health states pane.

    The system displays a table showing the health state for:

    - **License**: indicates that a system license is sucessfully installed on the MOM.

    - **OMM connections**: indicates that all OMMs registered with the MOM are connected successfully

      If an OMM (for which the MOM has a record) is not connected, the MOM interface displays a warning icon in the **Severity** field, and a message that the OMM is not connected in the **Reason** field.

Health states		
Health state	Severity	Reason
License	✗	No license available
OMM connections	⚠	OMM not connected

2. Click on **OMMs** to open the OMMs pane. The OMM pane displays consolidated health state information for individual OMMs, including connection status.

Viewing system statistics

You can view statistics for connections from applications, or from OMMs.

To view system statistics, do the following:

1. Click on **Statistics** to open the system statistics pane.

    The system displays a table of the following statistics.

    - MAXI: Total number of failed client connections

    - MAXI: Total number of client requests

- MAXI: Total number of failed requests
- MAXI: Total number of events sent to clients
- MAXI: Total number of data in Kbytes received from clients
- MAXI: Total number of data in Mbytes sent to clients
- MAXI: Maximal parallel client connections
- Number of 'SendMessage' requests from MAXI clients
- Number of 'SendMessage' requests from OMM
- ...

2. To view a graphical representation of a specific statistic, click on the arrow beside the statistic to expand the entry.
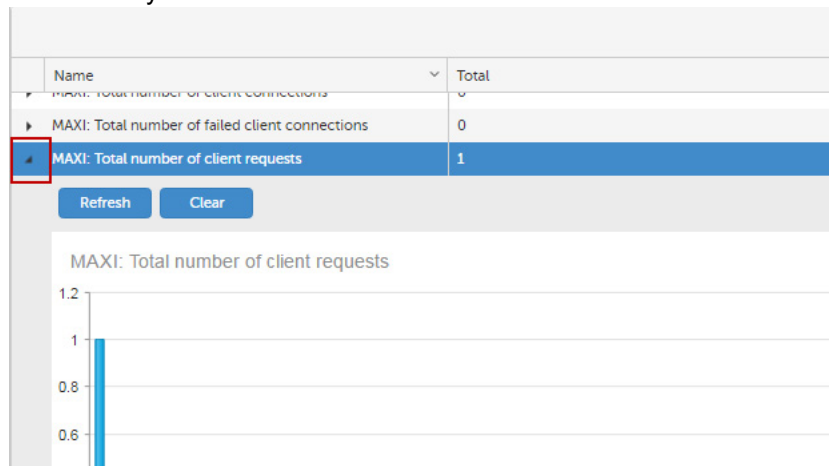
a. To refresh the statistic counter, click **Refresh**.

b. To clear the statistic counter, click **Clear**.

3. Click **Clear all** to remove all current statistic counters.

   Note: Only the current counter is cleared, not historical data.

4. Click **Refresh all** to trigger a refresh of all current statistic counters.

Viewing the system event log

The MOM provides information about system events. The Event log contains a list of up to 100 events.

To view the system event log, do the following:

1. Click on **Event log** to open the system event log pane.

   The system displays a table of system events, with the following information for each event:

   - **Severity**: the relative importance of the event
   - **Subsystem**: the subsystem associated with the event
   - **Count**: the total number of events of the type indicated
   - **Time**: the date and time the event was generated
   - **Event**: the type of event

2. To clear the event log, click **Clear all**.

Viewing the End User License Agreement (EULA)

The End User License Agreement (EULA) describes the terms of use for the SIP-DECT software.

To view the SIP-DECT EULA, do the following:

1. Click on **EULA** to open the system event log pane.

    The system displays the full text of the End User License Agreement.

Migrating existing SIP-DECT systems

Before you migrate an existing SIP-DECT system to a MOM-provisioned system, you must ensure that all OMMs are running a software version that is compatible with the MOM.

The following scenarios assume that you have installed and configured the MOM application.

- "Single OMM system with multiple sites" on page 41
- "Multi-OMM system with multiple sites" on page 41
- "Dual-homed OMM systems" on page 41

Single OMM system with multiple sites

You can migrate an existing system that has one OMM with multiple sites to a system with multiple OMMs (for local redundancy).

Follow these steps to migrate the single OMM system:

1. Connect the existing OMM to the MOM (SARI = PARK).

2. Create a local OMM for each site in the system.

3. Add the new OMMs to the MOM.

4. Redirect the DECT base stations to connect to the local OMMs at their site.

Multi-OMM system with multiple sites

You can migrate a system with multiple locally-managed OMMs to a centrally-managed MOM system (to permit roaming between sites).

Follow these steps to migrate the multi-system:

1. Connect the largest OMM in the existing system to the MOM (SARI = PARK).

   Note: It is recommended to use the OMM system with the biggest number of mobile devices.

2. Add each additional OMM in the existing system to the MOM.

3. Resubscribe any devices on the OMMs that must be able to roam between sites.

Dual-homed OMM systems

When you migrate a system that uses DECT Phone Synchronization (also known as Dual Homing or UDS), the MOM license must use the same SARI as the existing Dual Homing system.

Follow these steps to migrate the dual-homed OMM system:

1. Add each OMM to the MOM.

   Once the MOM connects to the OMM, dual homing is disabled on the OMM.

2. After all other OMMs have been added to the MOM, add the central OMM to the MOM.

Network Port Overview

Protocol		Multi-OpenMobility Manager	
		Server port	Client port
HTTPS server	tcp server	443 or as configured	any
HTTP server (redirect to https)	tcp server	80 or as configured	any
OM AXI (MOM as client)	tcp client	12622	any
MOM MAXI server TCP	tcp server	12623 or as configured	any
MOM MAXI server TLS	tcp server	12624 or as configured	any