MiVoice MX-ONE

Management Applications Descriptions

Release 7.4

December 16, 2021

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®)**. 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.

Contents

MX-ONE Management Applications

This document describes the MiVoice MX-ONE Manager suite, comprising the following management applications:
- MX-ONE Service Node Manager (system management)
- MX-ONE Provisioning Manager (user and extension management)
- Mitel Performance Analytics (fault and performance management based on SNMP). Also known as the MPA application (and former MarWatch).

Introduction

This document describes the MiVoice MX-ONE Manager suite, comprising the following management applications:
- MX-ONE Service Node Manager (system management)
- MX-ONE Provisioning Manager (user and extension management)
- Mitel Performance Analytics (fault and performance management based on SNMP). Also known as the MPA application (and former MarWatch).

Figure 1.1: MX-ONE
Manager
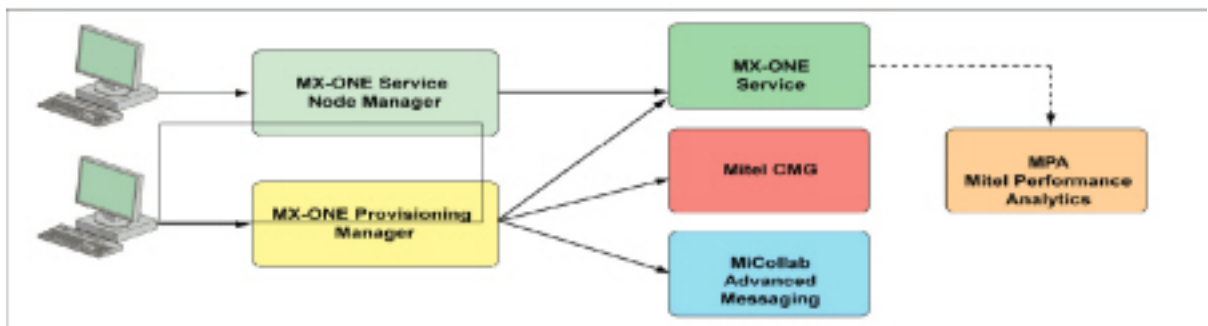
The MiVoice MX-ONE Manager suite has the following capabilities:
- Enables configuration and operation of the MX-ONE.
- Provides a common, single point of entry for user and extension administration.
- Provides advanced fault and performance management that is easy to integrate with existing tools or frameworks.
- Provides consistent management user interfaces across the MX-ONE components and applications.

MX-ONE Manager provides management functions for MX-ONE according to the Fault, Configuration, Accounting, Performance, and Security Management (FCAPS) paradigm.

Scope

This document provides a high-level description of the MX-ONE Manager suite.

Target Group

This document is intended for:
- Users of MX-ONE Manager applications
- IT managers
- System Administrators
- Support personnel.

Glossary

For a complete list of abbreviations and a glossary, see the document ACRONYMS, ABBREVIATIONS AND GLOSSARY.

MX-ONE Service Node Manager

The MX-ONE Service Node Manager is a web-based application, accessed using a web browser. The application provides functionality for configuring and managing the MX-ONE including, for example:
- Setting up MX-ONE
- Managing media gateways
- Managing routes
- Managing operators
- Managing groups, number plans, common categories, and service profiles
- Creating and maintaining configuration files for IP phones
- Monitoring IP phones
- Backing up and restoring data in MX-ONE
- Uploading MML commands in the command line interface
- Viewing information about hardware and software revisions
- Viewing security, event, and audit trail logs

Figure 1.2: MX-ONE Service Node Manager
GUI

The MX-ONE Service Node Manager is a software component running on the MX-ONE. It is based on the JBoss Application Server and is implemented as a Web-based management tool.

MX-ONE Provisioning Manager or Linux user accounts are used for logging in to the MX-ONE Service Node Manager. Which type of user to use for the MX-ONE Service Node Manager log-in is defined by the authentication method.

If the MX-ONE Provisioning Manager is used for authentication, the MX-ONE Provisioning Manager user database is used for authenticating user log-in to the MX-ONE Service Node Manager. If Linux is used for authentication, standard Linux procedures are used for the authentication. Which authentication method to use for SNM is set during installation, when running the MX-ONE Maintenance Utility, option Web server config.

The MX-ONE Service Node Manager supports both HTTP and HTTPS signaling and can be accessed from anywhere, using an ordinary web browser. For HTTPS, it is possible to use either a self-signed certificate or a certificate issued by a commercial Certification Authority (CA).

For more information about the MX-ONE Provisioning Manager and MX-ONE Service Node Manager certificate handling, see the description for *AD Authentication*.

For more information about the MX-ONE Service Node Manager, see the description for *MX-ONE Service Node Manager*.

Features

The following tasks and features are available in the MX-ONE Service Node Manager GUI:

Application ID

Manages the installation (site) name and the add or change information about the site.

Backup & Restore

Performs a backup of the Service Node Manage database as well as exchange data. All data can be restored by using the restore function.

Batch Operation

Batch operations are used to create several configuration tasks in a batch, and can be used for repeated or frequently performed operations.

Call Center

Manages automatic call distribution.

Call Diversion

Manages both the system call diversion and the customer call diversion.

Call Discrimination

Manages group names and permitted numbers.

Command Line Interface

The interface allows administrators to enter commands and view system responses without having to log out or change terminals.

CSTA Server

Sets up a CSTA server. Using CSTA, third-party applications can be used for call control.

DECT System

Sets up the DECT system. This includes system ID, DECT boards, Base Stations, SMS servers and SMS clients.

Emergency Number

Makes it possible to add or change emergency number.

External lines

Manages different external lines features, for example, route.

Groups

Manages different group features, for example, hunt group.

Hardware

Makes it possible to block hardware and view the time zone information.

Information System Connections

Sets up information system connections (for Message Waiting, Voice Mail etc.)

IP Phone Configuration

Manages different IP Phone features, for example, IP Phone Administrator.

Logs

Views the security logs, the audit trails and the event logs.

Messages

Manages message diversion and message waiting setup.

Number Plan

Manages numbers, number series and external number length.

Operators

Manages different operator features, for example, operator groups.

Quality of Service

Provides tools for measurement of Quality of Service.

Revisions

Displays hardware and software revisions for the system.

Routing Server

Sets up a routing server (it can either be an MX-ONE traffic carrying node in the network or an MX-ONE node with server functionality).

Setting up a Branch Office

Makes it possible to set up branch offices (but only if the branch office contains an Enterprise Branch Node (EBN)).

System Data

Manages different equipment and system features, for example, equipment data.

System Data for Extensions

Manages, for example, account codes, common categories and common service profiles.

Voice Announcements

Manages voice announcements.

Interactions with Other Applications and Products

The MX-ONE Service Node Manager makes it possible to configure, for example, number plans, routes, branch offices, SMS for DECT, routing servers, and trunks, in the MX-ONE.

The MX-ONE Service Node Manager is also used to create and update configuration files for the IP phones.

MX-ONE Provisioning Manager

MX-ONE Provisioning Manager is the end-user and extension management application in the MX-ONE, providing a single point of entry for managing user and extension data in the MX-ONE, the MX-ONE MiCollab Advanced Messaging, CMG, and FMC Provisioning Server.

The MX-ONE Provisioning Manager also provides functionality for (for example):
- Managing administrator accounts.
- Adding subsystems, for example, the MX-ONE Service Nodes and CMG servers.
- Importing and exporting user and extension data.
- Performing backup of user and extension data.
- Unlocking locked users.

Figure 1.3: MX-ONE Provisioning
Manager
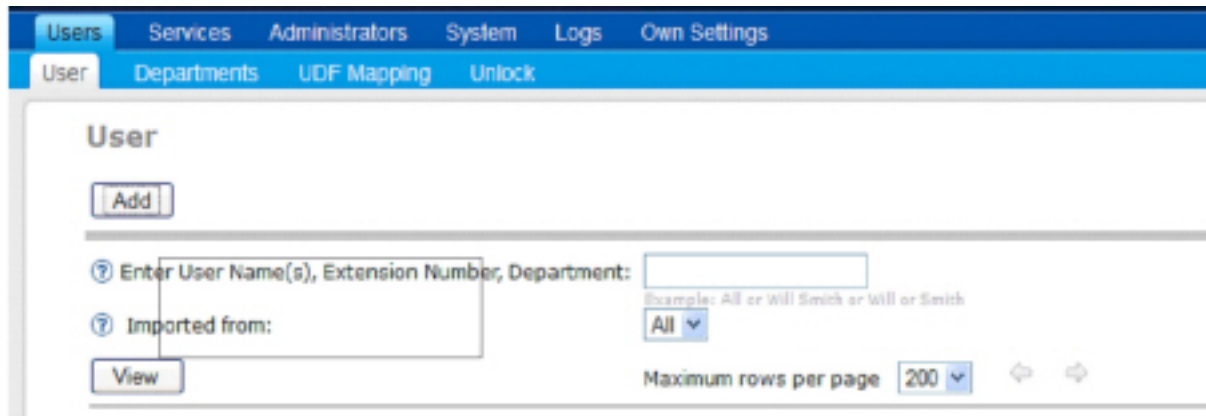
When changing user and extension data in the MX-ONE Provisioning Manager the corresponding data in the MX-ONE, MiCollab Advanced Messaging, and CMG databases is automatically updated accordingly.

NOTE: The MX-ONE Provisioning Manager database is the master user and extension database in the MX-ONE. The MX-ONE Provisioning Manager must therefore be used when, for example, adding or deleting users. Changing user or extension data in CMG or the MX-ONE will cause unsynchronized data in the MX-ONE databases.

Application specific user and extension data, for example, time zone settings in CMG, is managed using the management tool of the specific application. Time zone settings, for example, are managed using CMG's OfficeWeb or Directory Manager.

Figure 1.4: User and extension data flow in
MX-ONE
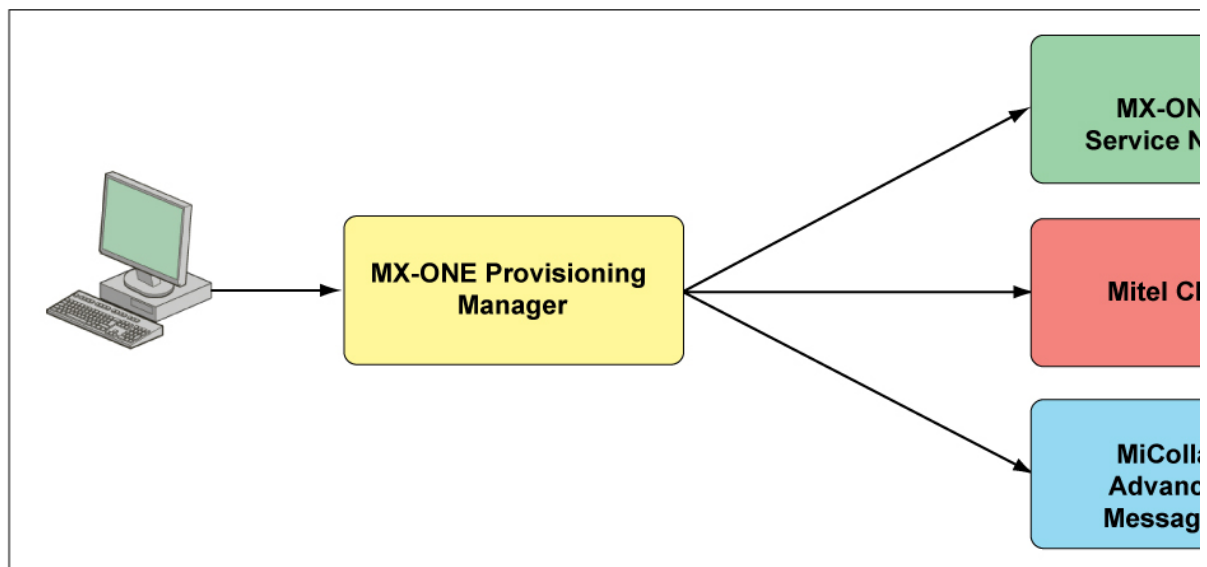
All users created in the MX-ONE Provisioning Manager are assigned a security profile. A security profile is a set of privileges that defines the user's access in the system, that is, what the user is allowed to do.

The MX-ONE Provisioning Manager is a software component that can be installed on a stand alone SuSE Linux server or be co-installed on the MX-ONE Service Node hardware. The MX-ONE Provisioning

Manager is based on the JBoss Application Server and is implemented as a Web-based management tool.

For more information, see description for *MX-ONE Provisioning Manager*.

Features

The following features are part of the MX-ONE Provisioning Manager:

Access Rights

User access is restricted by the privileges included in the user's security profile. The privileges restrict which tasks the user has access to

Assignment of services to users

Subsystems that have been registered in the MX-ONE Provisioning Manager provide a number of services that can be configured for the users.

End-user interface

End-users can log in to the MX-ONE Provisioning Manager and view their own settings and extensions assigned to them

Import of user and department data

User data and department data can be imported to the MX-ONE Provisioning Manager from other systems, e.g. Microsoft Active Directory (AD).

Migration from other system

Migrates users and departments from other systems. For example, D.N.A., data can be extracted from the D.N.A. system and imported into the MX-ONE Provisioning Manager

Synchronization of the MX-ONE Provisioning Manager data and Subsystem data

Inconsistencies between the MX-ONE Provisioning Manager data and subsystem data can occur if the MX-ONE Provisioning Manager has been restored using the Backup & Restore task, and if the subsystems were not restored at the same time. If inconsistencies occur, a synchronization is needed. Inconsistencies can also occur if user or extension data is modified in CMG or the MX-ONE.

Interactions with Other Applications and Products

The MX-ONE components providing user services (such as the MX-ONE Service Node or CMG) are added as subsystems in the MX-ONE Provisioning Manager. The MX-ONE Provisioning Manager is the primary application for user and extension management for the added subsystems and changing user or extension data directly in the subsystem will cause inconsistent data.

The following MX-ONE components can be added in the MX-ONE Provisioning Manager as subsystems:
* FMC Provisioning Server.
* CMG Server
* MiCollab Advanced Messaging (former OneBox/Messaging Server)
* Microsoft Active Directory
* MX-ONE Service Node

User, extension, and department data can be imported from:

- Any system using CSV files.
- CMG
- D.N.A.
- Microsoft Active Directory

Data in MX-ONE Provisioning Manager can be exported to:
- CMG
- XML files.

If the subsystem has a web-based user interface, a link to the subsystem will be available in the MX-ONE Provisioning Manager, making the MX-ONE Provisioning Manager a common interface for reaching all its subsystems.

When the MX-ONE Provisioning Manager and the MX-ONE Service Node Manager coexist on the same server, the MX-ONE Provisioning Manager will have the same certificate as the MX-ONE Service Node Manager. That is, if the MX-ONE Service Node Manager uses HTTPS, the MX-ONE Provisioning Manager will also use HTTPS.

Mitel Performance Analytics

The Mitel Performance Analytics, MPA, is an optional application for supervision of the status of system components and of alarms.

MPA consists of a number of web services running on either a cloud-hosted computing platform or on-premises computing platform. There are several components to MPA. The remote 'Probe' installed in non-Internet accessible networks maintains databases of status and events, and provides a web portal with access security. Additionally, MPA has a Remote Access Service that provides a secure "cross-connect" for remote access to the customer network.

A Mitel/Aastra branded MIB developed for MX-ONE is used.

See the MPA System Guide (2.1 or later) for details.

Supported Device Boards

There are several tasks in the management applications that interact with the MiVoice MX-ONE system HW.

Not all installed HW is supported for all tasks in MX-ONE Service Node Manager (SNM) and MX-ONE Provisioning Manager (PM). Guide lines are provided below.

In general, and except for the tasks add and change, all the boards listed in Parameter Description for BRDID, in Technical Reference Guide, MML parameters, are supported by MX-ONE Service Node Manager/MX-ONE Provisioning Manager.

The supported HW is not identical for the different tasks available in the support systems suite. The tasks described below are view, remove, add, change, board list, blocking and equipment vacancies.

Add/Change

Changing and adding tasks can only be executed for board-id's with signaling type as indicated in the table below.

Supported Board Id / Name	SW Name (Signaling type)
118 (ELU34)	EL6 (Extension Line Analog)
128 (ELU34/6)	EL6 (Extension Line Analog)
121 (ELU31/3)	CTL (Cordless DECT Telephone Line)
127 (ELU31/4)	CTL (Cordless DECT Telephone Line)
117 (ELU33)	KL1 (Extension Line Digital)
58 (TLU79, ISDN/BRA)	SL60 (Digital ISDN 2B+D)
125 (PRI, ISDN/MGU)	SL60 (Digital ISDN 30B+D)
57 (TLU76/11)	SL60 (Digital ISDN 30B+D)
27 (TLU**3)	EL7 (CAS Extension Line)

View/Remove

The view and remove tasks supports all HW installed in the applicable system(s), i.e. all extensions/trunks/operators/etc are visible irrespective of the HW version initiated on. They can also be removed from the system(s).

Board List

The board list task support all the boards initiated in the MX-ONE, i.e. BRDID 1-255.

Blocking

The blocking task in MX-ONE Service Node Manager supports the following board ID's and signaling.

Supported Board Id / Name	SW Name (Signaling type)
118 (ELU34)	EL6 (Extension Line Analog)
128 (ELU34/6)	EL6 (Extension Line Analog)
121 (ELU31/3)	CTL (Cordless DECT Telephone Line)
127 (ELU31/4)	CTL (Cordless DECT Telephone Line)
117 (ELU33)	KL1 (Extension Line Digital)
58 (TLU79, ISDN/BRA)	SL60 (Digital ISDN 2B+D)

Supported Board Id / Name	SW Name (Signaling type)
125 (PRI, ISDN/MGU)	SL60 (Digital ISDN 30B+D)
57 (TLU76/11)	SL60 (Digital ISDN 30B+D)
125 (PRI, ISDN/MGU)	SL63 (Digital ISDN 23B+D)
71 (TLU77/1)	SL63 (Digital ISDN 23B+D)
124 (TLU83)	TL11 (Trunk Line)
96 (ALU2)	AL (Alarm Line)
102 (TMU/2)	AD (Auxiliary Device, Tone/Multi-pty Line)
27 (TLU**3)	EL7 (CAS Extension Line)

Equipment Vacancies

The table below shows the boards and signaling type that are supported by the MX-ONE Service Node Manager.

Supported Board Id / Name	SW Name (Signaling type)
118 (ELU34)	EL6 (Extension Line Analog)
128 (ELU34/6)	EL6 (Extension Line Analog)
117 (ELU33)	KL1 (Extension Line Digital)
58 (TLU79, ISDN/BRA)	SL60 (Digital ISDN 2B+D)
125 (PRI, ISDN/MGU)	SL60 (Digital ISDN 30B+D)
57 (TLU76/11)	SL60 (Digital ISDN 30B+D)
125 (PRI, ISDN/MGU)	SL63 (Digital ISDN 23B+D)
71 (TLU77/1, US ISDN)	SL63 (Digital ISDN 23B+D)

Equipment Configuration

The equipment configuration task is only checking the configuration of the server, i.e. no relation to board id's.

Reference Documents

Server Redundancy - 157_15431-ANF90114

MX-ONE Provisioning Manager

This topic discusses the MX-ONE Provisioning Manager description.

Introduction

This document describes MX-ONE Provisioning Manager (PM), a tenant, user, and extension management application for MX-ONE.

MX-ONE Provisioning Manager is a part of the MX-ONE Manager application suite.

Scope

This document provides a high-level description of MX-ONE Provisioning Manager.

Target Group

This document is intended for:
- MX-ONE Provisioning Manager users
- IT managers
- Support personnel
- People who work with integration of MX-ONE Provisioning Manager with other systems

Glossary

For a complete list of abbreviations and glossary, see the description for *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

Overview

MX-ONE Provisioning Manager is the user and extension management application in MX-ONE, providing a single point of entry for managing user and extension data in MX-ONE, MiCollab Advanced Messaging, Mitel CMG, and FMC Provisioning Server.

MX-ONE Provisioning Manager also provides functionality for the following (for example):
- Managing administrator accounts
- Adding subsystems, for example, MX-ONE Service Nodes and CMG servers.
- Importing and exporting user and extension data
- Performing backup of user and extension data
- Unlocking locked users.

Figure 2.1: MX-ONE Provisioning
Manager

When changing user and extension data in MX-ONE Provisioning Manager the corresponding data in the MX-ONE, MiCollab Advanced Messaging, and CMG databases is automatically updated accordingly.

NOTE: The MX-ONE Provisioning Manager (PM) database is the master user and extension database in MX-ONE. PM must therefore be used when, for example, adding or deleting users. Changing user or extension data in CMG or MX-ONE or MiCollab will cause unsynchronized data in the MX-ONE databases.

Application specific user and extension data, for example, time zone settings in CMG, is managed using the management tool of the specific application. Time zone settings, for example, are managed using CMG's OfficeWeb or Directory Manager.

Figure 2.2: User and extension data flow in
MX-ONE
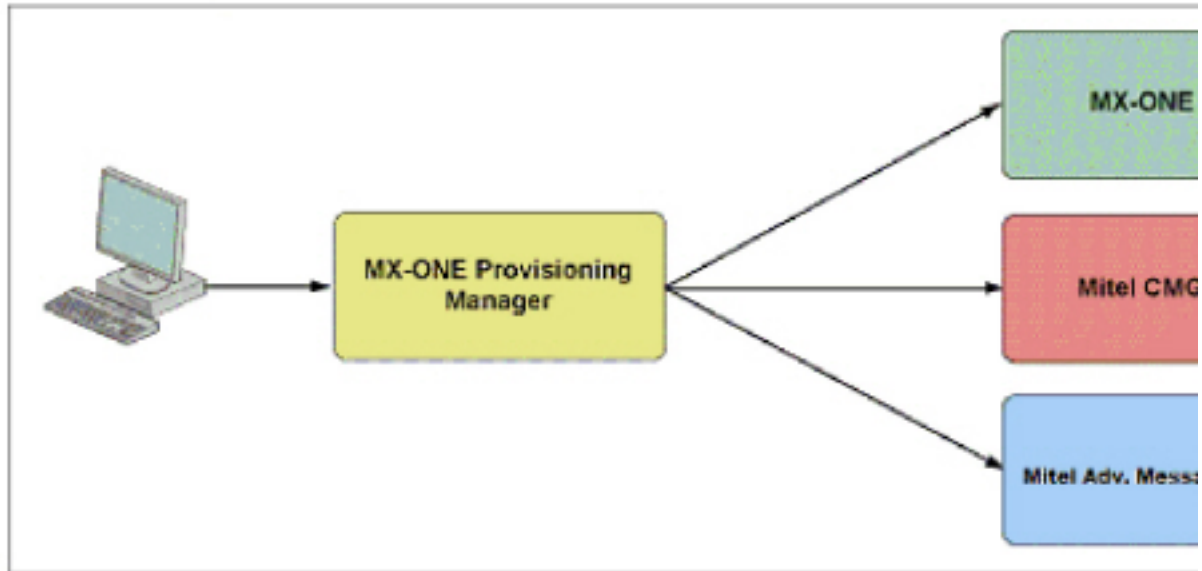
MX-ONE components providing user services (such as MX-ONE Service Node or CMG) are added as subsystems in PM. MX-ONE Provisioning Manager (PM) is the primary application for user and extension management for the added subsystems, therefore changing user or extension data directly in the subsystem will cause inconsistent data.

The following MX-ONE components can be added as subsystems in PM:

- MX-ONE Service Node
- Mitel CMG Server
- MiCollab Advanced Messaging Server
- FMC Provisioning Server
- MiCollab Server
- SIP DECT Manager
- Other management application

User, extension, and department data can be imported from:

- D.N.A.
- CMG
- CSV files
- CSV files in Express format

Data in PM can be exported as:

- CMG files
- XML files
- Call accounting API files
- FMC 4 user data files
- MiCollab user data files

For subsystems with web-based user interfaces, a link to the subsystem will be available in PM, making PM a common interface for reaching all its subsystems.

All users created in PM are assigned to a security profile. A security profile is a set of privileges that defines the user's access in the system, that is, what the user is allowed to do.

PM is designed to allow multiple concurrent log in sessions, and concurrent invocation of its functions.

PM is a software component that can be installed on a stand alone SuSE Linux server or be co-installed on the MX-ONE Service Node hardware. PM is based on the JBoss Application Server and is implemented as a Web-based management tool.

For more information about interfaces and protocols, see *Interfaces and Protocols*.

System Requirements

MX-ONE Provisioning Manager can be accessed using the following browsers:
- Google Chrome (latest version)
- Microsoft Edge 80.0.361.48 (Official build) (64-bit)
- Mozilla Firefox 18 (or later)
- Microsoft Internet Explorer 8.0 (or later)

Deployment Scenarios

MX-ONE Provisioning Manager can be deployed in the following ways:
- Stand alone
- On MX-ONE Service Node (in coexistence with MX-ONE Service Node Manager if installed on the primary MX-ONE Service Node

During the installation, MX-ONE Provisioning Manager can be configured to run with HTTPS. For more information about deployment scenarios and installation, see the installation instructions *INSTALLING MX-ONE PROVISIONING MANAGER*.

User and Extension Data

This section has information in user and extension data in MX-ONE Provisioning Manager and Its Subsystems. When managing data in MX-ONE Provisioning Manager, data is automatically forwarded to the applicable subsystems.

Figure 2.3: User and Extension Data in
MX-ONE
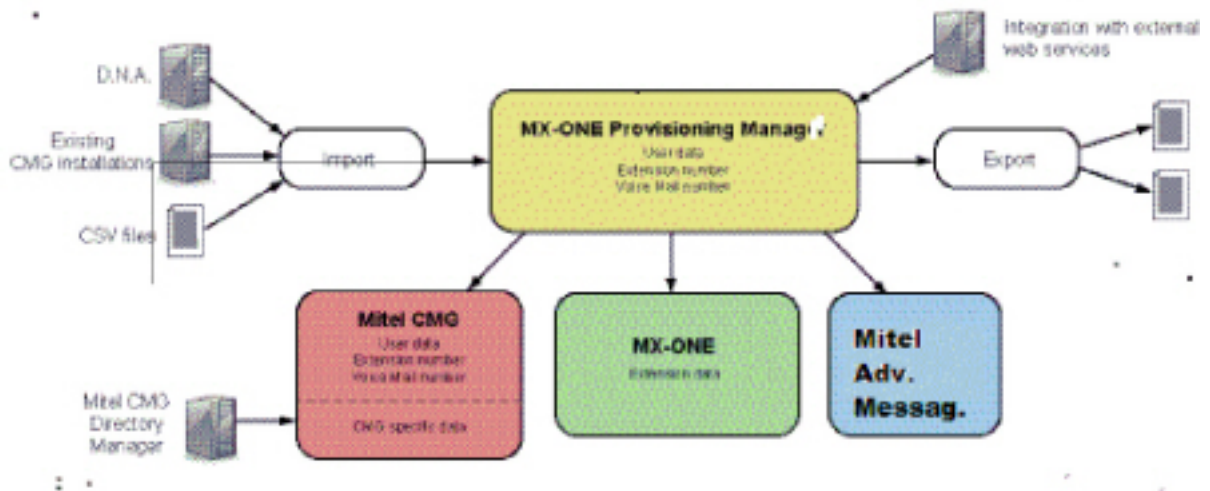
Example on Data Flow Between MX-ONE PM and Its Subsystem

This chapter gives an example on the data flow between MX-ONE Provisioning Manager (PM) and its subsystems when adding a user with the following properties in MX-ONE:

- First name: Jane
- Last name: Smith
- User ID: jsmith
- Time Zone: GMT+01:00

The following services will be assigned to the user:

- IP extension
- Voice Mail mailbox

The procedure is initiated from the User task in PM.

Initiating the User Task

Users are added using the User task in PM. The task includes functionality for creating extensions and voice mailboxes. When initiating the task, PM requests data from the available subsystems, for example:

- Free extension numbers (provided by MX-ONE)
- Available group and categories (provided by MX-ONE)
- Available common service profiles (provided by MX-ONE)
- Available class of service profiles for Voice Mail mailboxes (provided by Mitel MiCollab Advanced Messaging).

Creating User and Extension Data

When the User task is finished, the following actions are performed:

1. A user with the specified user data is created in the MX-ONE Provisioning Manager (PM) user database. This data includes information on which extensions (including mailbox numbers) the user is assigned to (see 1 in the figure below).

2. A user with the same user data is created automatically in the CMG user database. The example includes a CMG specific time zone setting. When the user is created in CMG, this setting it is given a default value. If the setting needs to be changed, this is done using CMG's OfficeWeb or Directory Manager.

3. An IP extension with the selected directory number is created in MX-ONE.

4. A voice mailbox number is created in Mitel MiCollab Advanced Messaging.

Figure 2.4: Creating user and extension data
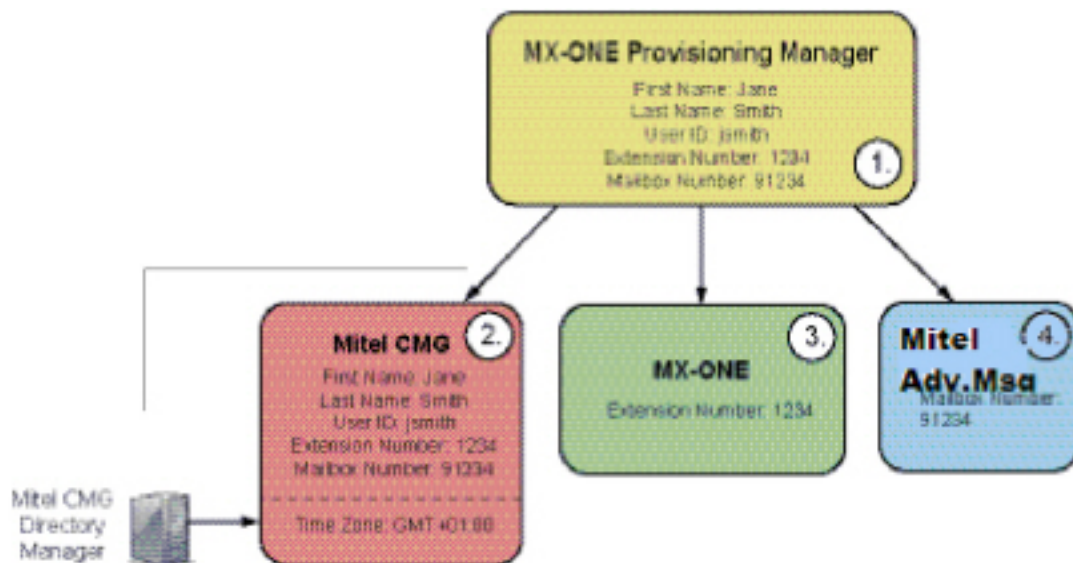
If data fails to be added in a subsystem, PM displays a message indicating failed parts of the operation.

Subsystems to which data is successfully added are not affected by other, failing subsystems (the services provided by the non-failing subsystems will be initiated).

User Types

MX-ONE Provisioning Manager (PM) is a tool for user management in MX-ONE, it is used to configure MX-ONE users and their services. All users created in PM are assigned a security profile. A security profile is a set of privileges that defines the user's access in the system and what the user is allowed to do.

When a user is added in the **User** task, the user is automatically assigned the security profile End User.

User hierarchy is basically divided into two types:

*   Traditional (AlaCarte)
*   Feature based

An end user can be promoted to administrator by assigning that user a different security profile and defining access to departments and locations in the **Administrator** task.

A number of security profiles are predefined. All predefined security profiles, except Super User and End User, can be modified and new profiles can be added to accommodate administrator needs.

The following security profiles are predefined in the system:

- **System Setup Administrator:** System Setup Administrator is created during the installation and has access to all tasks with view option only for Extensions.

Users fall under Traditional category:

- **Local Super User:** Has the same default settings as Super User. Is used to restrict the administrator's access to locations and departments.
- **System Administrator:** Manages system configuration data, for example, handles installation and the system (node) settings.
- **Service Provider:** Configures services and makes them available.
- **User Administrator:** Manages user data, for example, adds users.
- **AlaCarte Service Provider:** Ala carte can manage configuration data, user data, service data, administrators, advanced feature and access to systems without feature levels.
- **User and Service Administrator:** Manages both users and services.
- **Advanced Telecom Administrator** Manages MX-ONE Service Node data by using the MX-ONE Service Node Manager web interface.
- **End User:** Has access to end user web interface to view the own settings and, if so configured, can a

Use

- **S**
  F
- **F**
  T
  a

Res

- T
  t

Ten

- T
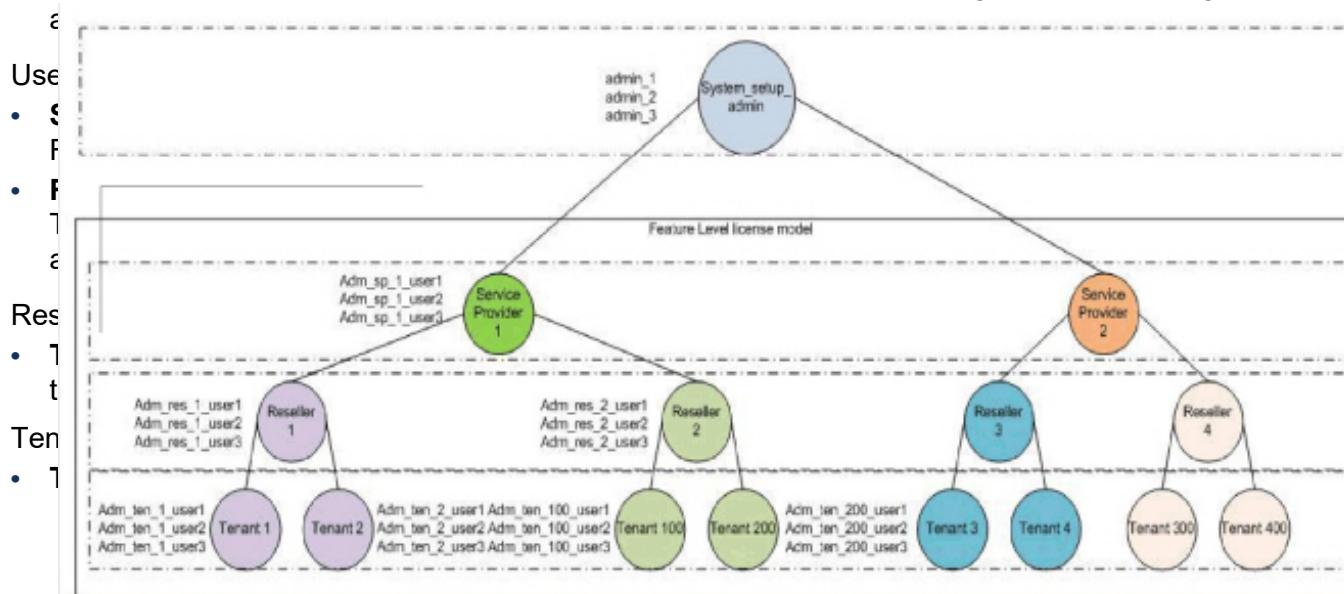
Key Features

The key features of MX-ONE Provisioning Manager (PM) are described in the following sections.

Tenant and Feature Configuration

Tenant Configuration is used to create the tenants, number series and IP Extensions.

Feature Level Configuration is used to map the alias names for feature levels for a specific reseller according to the feature level defined in the MX-ONE.

User Provisioning

PM provides functionality for creating, maintaining, and removing users in MX-ONE. It also provides functionality for assigning user services to users. The services are provided by subsystems such as MX-ONE and Mitel MiCollab Advanced Messaging.

User Services

The below list is an example on services that can be assigned to users in PM. Information within brackets indicates affected subsystems when a service is assigned to a user in PM.

- **IP extension (SIP, H.323, IP-DECT):** An IP extension allows the connection of IP terminals to MX-ONE. (MX-ONE, CMG)
- **Multi Terminal extension:** Multi-terminal extension is a generic extension which has master value greater than one. IP, Mobile, DECT extensions can be initiated as terminals with the same extension number.
- **Mobile extension:** Mobile Extension is an application that lets ordinary mobile phones in the Public Land Mobile Network (PLMN), or terminals in the Public Switched Telephone Network (PSTN) or private networks, to be treated as ordinary PBX extensions. They have access to most of the features of the MX-ONE (MX-ONE, CMG).
- **DECT extension:** DECT extensions are cordless extensions. Using cordless phones enables users to make and accept calls at any location in the coverage area of its base stations (MX-ONE, CMG0.
- **Virtual extension:** A virtual extension is a generic extension which is not associated to any terminal type (MX-ONE, CMG).
- **Digital extension:** A digital extension allows the connection of digital phones to an MX-ONE (MX-ONE, CMG).
- **Analog extension:** An analog extension allows the connection of analog phones to an MX-ONE (MX-ONE, CMG).
- **ADN extension:** One or more Additional Directory Numbers (ADNs) can be assigned to a user. These are programmed on free function keys on the phone (MX-ONE, CMG).
- **IP function keys:** Function keys on an IP phone are programmable. They are used to access predefined functions (MX-ONE).
- **Parallel ringing:** The Parallel Ringing service provides the user with simultaneous ring signal on up to three predefined answering positions for an incoming call to the user. When the user answers the call, the call is directed to the extension where it has been answered (MX-ONE).
- **Group membership:** This service allows the user and associated extensions to be part of groups, for example, Hunt groups and Call Pick-up groups (MX-ONE).
- **Digital function keys:** Function keys on a digital phone are programmable. They are used to access predefined functions (MX-ONE).
- **Personal number:** The Personal number service is designed to provide the user with up to five profiles, each one containing up to 10 possible answering positions. If Personal Number is available,

the traditional extensions (analog extensions) and the generic extensions (IP extension and virtual extension) can use the service (MX-ONE).

• **Least Cost Routing for mobile extensions:** Using Least Cost Routing for mobile extensions, an outgoing call from a mobile extension can be kept within the system if the called number resides within the own system (MX-ONE).

• **Mailbox:** Mailbox is a solution that allows users to send all voice, fax and E-mail messages from a phone or a PC. [MX-ONE, CMG, Mitel MiCollab Advanced Messaging.

Access Restriction

User access is restricted by the privileges included in the user's security profile. Added users are assigned end user privileges by default, and end users can be promoted to different types of administrators.

Administrator access can be restricted to subsystems in specific locations and to specific departments. Two administrators with the same privileges can, for example, have access to subsystems in two different locations, or to different departments in the same location. When an administrator is created, access to departments and subsystem locations is configured.

For example, if a company has one office in Stockholm and one office in London but wants to use PM for both offices, location access restriction can be used. Then one administrator can be assigned access to departments and subsystems in Stockholm, and another administrator can be assigned access to departments and subsystems in London.

Supported Phone Types

The following phone types are supported by MX-ONE Provisioning Manager:
• Analog phones
• Digital phones:
    – – Dialog 32xx (DBC 2xx)
    – MiVoice 42xx (DBC 22x)

• Mitel IP (DBC4xx) and IP DECT phones
• Cordless phones (DECT)
• Mobile phones
• 6900/6800/6700 SIP phones
• BluStar 8000i

Import and Export

Department and user data can be imported from Dynamic Network Administration (D.N.A.) or CMG, or from a comma separated value (CSV) file. After import, the imported data is available in the User and Department tasks.

PM users with authority to import and export user data can export data as XML and CMG format. Also, call accounting data can be exported.

PM exports data in CSV format for FMC 4 user data and MiCollab user data.

Reset Password

When a Mail Server has been configured, a new password can be sent by e-mail to users who has forgotten their password. This is done by pressing the link **Reset Password** that will be visible on the log in page when a mail server has been configured. After providing a valid user name, the system delivers a new, randomly generated password to the previously provided e-mail address.

Self-Provisioning for End-Users

End-users can log in to PM and view their own settings. If required, users can be allowed to the change certain own settings, such as password, user defined fields, and function key assignment for phones.

Efficiency Enhancing Features

To improve the user experience and facilitate the usage of the application, efficiency enhancing features are available in PM. A selection of the features are described in the following list:

- Online help providing information about tasks and properties in the tasks.
- The web interface can support multiple languages, namely: Chinese, Dutch, English, French German, Polish, Russian, Spanish, and Swedish. This means both the online help texts and the web interface changes to the selected language.
- Using templates when adding new configuration items. A template is a set of predefined values, and it is used to simplify the process of adding many configuration items with similar property values.
- Templates can be transferred from one system to another by downloading them from the first system and then uploading them to the other system.
- Settings for an existing configuration item can be copied and used for creating a new item.
- Templates can be created based on existing configuration items.
- Multistep buttons can be used to make a detour from task A to task B to add or change configuration items in task B before continuing the configuration of an item in task A. Multistep buttons are used when values in a list are configuration items set in another task.
- In some tasks, there is a search function that can be used to find specific configuration items. In the search criteria, wildcards can be used.
- Some configuration item lists can be filtered to make it easier to find specific configuration items
- Two configuration items can be compared, differences are highlighted in orange.
- Two or more configuration items can be viewed side by side.
- Departments are displayed in a tree structure that represents the department organization in the company.
- User Defined Fields (UDFs) are available for collecting additional information specific for your organization about users and departments.
- Response messages are displayed for both successful and unsuccessful operations.

For more information about how to use the features, see the *MX-ONE PROVISIONING MANAGER USER GUIDE*.

Third-Party Product Integration

MX-ONE Provisioning Manager provides a web service interface enabling integration with third party products, for example, human resource management systems.

For more information on web service interfaces, see *MX-ONE Service Node Manager and MX-ONE Provisioning Manager Web Services, INTERWORKING DESCRIPTION.*

Performance

During high call intensity, call processing is prioritized in MX-ONE. As a result, less capacity is reserved for administrative operations invoked from, for example, MX-ONE Provisioning Manager. This might result in longer response times for administrative operations.

Performing extensive operations in MX-ONE Provisioning Manager may cause increased load in MX-ONE. It is recommended that this type of operations are performed during periods with low call intensity.

For information on server performance requirements, see *MX-ONE SYSTEM PLANNING.*

Interfaces and Protocols

The following interfaces and protocols are available for MX-ONE Provisioning Manager:
* HTTP/HTTPS
* Web services

For more information about SOAP, see *MIVOICE MX-ONE SERVICE NODE MANAGER AND MX-ONE PROVISIONING MANAGER WEB SERVICES.*

Operation and Maintenance

For information about the user interface, the navigation, and a recommended work flow for adding data into PM, see the *MX-ONE PROVISIONING MANAGER USER GUIDE.*

For information about specific tasks and properties, see the Online help in PM.

For information about troubleshooting, see *FAULT HANDLING OF MX-ONE PROVISIONING MANAGER.*

Security

Hardening

For a stand alone installation hardening is handled by Linux. For an installation with coexistence on the MX-ONE Service Node, the hardening is the same as for MX-ONE Service Node Manager.

Hardening

For a stand alone installation hardening is handled by Linux. For an installation with coexistence on the MX-ONE Service Node, the hardening is the same as for MX-ONE Service Node Manager.

HTTPS

In MX-ONE Provisioning Manager (PM) both HTTP (TCP Port 80) and HTTPS (TCP Port 443) are supported. For higher security, it is recommended to use a commercial digital certificate issued by a commercial Certification Authority (CA).

HTTPS can be enabled after PM is installed. After HTTPS is enabled, all requests to/from PM must use HTTPS:

- web browser access to PM
- authentication requests from MX-ONE Service Node Manager (SNM) when PM is used as authentication server for SNM
- requests from PM to the SNM. This is set in the **Subsystem** task

If the Server Node Manager and Provisioning Manager use HTTPS, and the certificate installed is issued to the FQDN of the server only (that is, there is no IP address in Subject Alternative Names or CN), the FQDN shall be used in the:

- Subsystem for 'IP Address' parameter
- 'IP Address for Authentication Server' when configuring Set SNM to authenticate to 'PM Use FQDN', which also applies for AD authentication when the AD Server's certificate is issued to FQDN only.
- If MiCollab is integrated to the solution deployed, configure the MX-ONE/SNM FQDN in IP Address/FQDN of the Network Element (Users and Services).

Enabling 'High End Encryption', when configuring HTTPS/TLS Level requires unlimited restriction policy JAR files from IBM. Download these files from the below-mentioned link and transfer the files to the server (to any suitable place; path to the files will be specified while configuring the feature).

https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

TLS/SSL

If desired, the customer can set up TLS/SSL for the communication between the PM and MX-ONE Service Node subsystems.

TLS/SSL are protocols for securing IP communications by authenticating or encrypting each IP packet in a data stream. The protocols also include cryptographic key establishment.

Authentication

Each time a user tries to log in, PM authenticates that the user is authorized to log in, that is, checks the User ID and password. After three failed login attempts the user is locked and must be unlocked by an administrator assigned the privilege to unlock users. A user assigned with the privilege Auto Unlock, for example: Super user will be automatically unlocked every 20 minutes time interval.

PM can additionally be configured for authentication in Active Directory. The user still needs to be defined in the PM database, but PM Authentication enables the possibility to use the same password in PM as when logging in to the domain. See further Description, AD Authentication.

Passwords

Passwords are stored in hashed format. The hash function takes the password as input and transforms it into a fixed length string as output. The output is called the hash value, and it is concise representation of the password.

Authentication Server for MX-ONE SNM

MX-ONE Provisioning Manager (PM) can be used as authentication server for MX-Service Node Manager. In this scenario, PM user accounts are used for logging on to MX-Service Node Manager.

The authentication method for MX-Service Node Manager (that is, using PM or Linux user accounts for logging in) is selected during installation of MX-ONE Service Node Manager.

For more information on how to use PM user accounts for logging in to MX-Service Node Manager, see *User Account Management, Operational Directions*.

Security Logs

In the **Logs** task, there is a security log that shows information about successful and unsuccessful login attempts. A log file is created every day, even if there is no logged data. If a log file does not contain any log information, the log file states the text string `No logging information`.

Log files older than 90 days are overwritten. For traceability purposes, it is recommended that security log files are copied to an external system for long time storage on a regular basis.

Audit Trail Logs

All operations and responses in PM, and information on whom they are performed by, are logged. The logs are stored as XML files.

Log files older than 90 days are overwritten. For audit trail purposes, it is recommended that operation log files are copied to an external system for long time storage on a regular basis.

Event Trail Log

The Event Log is a collection of traced actions performed by the user, such as procedure calls for navigation, logins and command executions. It is useful for fault tracing.

A log file is created every day, even if there is no logged data. If a log file does not contain any log information, the log file states the text string No logging information. Logs older than 90 days will be overwritten

MX-ONE Service Node Manager

This topic discusses the MX-ONE Service Node Manager description.

Introduction

This document describes MX-ONE Service Node Manager (SNM), which is a part of MX-ONE Manager. SN Manager is used to configure the MX-ONE.

Scope

This document provides a high-level description of MX-ONE Service Node Manager.

Target Group

This document is intended for:
- Users of MX-ONE Service Node Manager
- IT managers
- System Administrators
- Support personnel

Glossary

For a complete list of abbreviations and a glossary, see the description for *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

Overview

MX-ONE Service Node Manager (SNM) is a management tool that makes it possible to configure the MX-ONE through a Graphical User Interface (GUI). It is also used to create and update configuration files for the IP phones.

SNM is part of the MX-ONE Manager concept that consists of several operation and maintenance applications providing management functions for MX-ONE.

System Requirements

MX-ONE Provisioning Manager can be accessed using the following browsers:
- Google Chrome (latest version)
- Microsoft Edge 80.0.361.48 (Official build) (64-bit)
- Mozilla Firefox 18 (or later version)

- Microsoft Internet Explorer 8.0 (or later version)

Installing MX-ONE Service Node Manager

Installation of MX-ONE Service Node Manager is performed automatically during installation of the MX-ONE Service Node software. This is to make sure that MX-ONE Service Node Manager and the MX-ONE Service Node are using the same software version (required). MX-ONE Service Node Manager is always installed on server 1 in systems comprising several servers. The application cannot be installed or upgraded separately.

When installing MX-ONE Provisioning Manager (PM) on a server on which MX-ONE Service Node Manager runs, MX-ONE Provisioning Manager must have the same software version (for example, 7.0) as MX-ONE Service Node Manager and the MX-ONE Service Node. For information on how to install MX-ONE Provisioning Manager, see MX-ONE Provisioning Manager, Installation Instructions (9/1531-ANF 901 15).

Before the MX-ONE Service Node Manager is installed, the rpm webserver_config will also be installed or upgraded (when a newer version is available). This is used to configure web server specifics on your server, such as which protocol to be used, certificate management when running HTTPS and authentication method between SNM and PM (when applicable).

To configure web server specifics, open **mxone_maintenance** tool and select **Webserver_config**.

NOTE: Installation of MX-ONE Service Node Manager on top of Standalone Provisioning Manager is not a valid Installation scenario.

Security

Service Node Manager can run in HTTP and HTTPS, the system is configured by default in HTTP. However, Mitel recommends that HTTPS with TLS 1.2 is used.

Provisioning Manager and Service Node Manager supports both RSA and ECDSA digital signature algorithm. However, the ECDSA key is not available when a Self-Signed certificate is created.

For information on how to generate a Certificate Signing Request, check the procedure to generate a Certificate Signing Request to be used by Provisioning Manager and Service Node Manager in the document *Installing MX-ONE Provisioning Manager - Installation Instruction*.

Privileges and User Types

SNM users can be authenticated either as a Linux user or an MX-ONE Provisioning Manager user. It is selected during the installation. The authentication method for SNM can be modified after the installation through **mxone_maintenance** tool and select **Web server config**.

The following privileges exist in SNM:
- Manage user data
- Manage configuration data
- Manage advanced feature
- Command line interface

In Linux the users belongs to different SN-levels depending on what they are allowed to do in the GUI.

Table 3.1: Privilege Levels

Privilege	SN-level
Manage user data	1
Manage configuration data	2 - 4
Manage advanced feature	5 - 6
Command line interface	7

In PM the administrator types are based on privileges included in the security profiles. These privileges defines the administrators access in the system.

The following privileges are used in MX-ONE Provisioning Manager to restrict administrator access to the SNM:

- Manage user data
- Manage configuration data
- Manage advanced feature
- Command line interface

Efficiency Enhancing Features

To improve the user experience and to facilitate the usage of the application, efficiency enhancing features are available in MX-ONE Service Node Manager. A selection of the features are described in the following list:

- Online help providing information about tasks and properties in the tasks.
- In SNM there are a number of walk-through. A walk-through is a guided tour through all the steps that are needed to set up, for example, an exchange with the basic features. The following walk-through are available:
  - Full Setup

    Sets up an exchange with the basic features.
  - Route

    Sets up IP and ISDN routes.
  - Operator

    Sets up one or more operators for the exchange.
  - Voice Announcement

    Sets up voice announcements.
  - Branch Office

    Sets up a branch office with basic features.
  - Routing Server

    Sets up a routing server with basic features.
  - Routing Satellite

    Sets up a routing satellite with basic features.

- Using templates when adding new configuration items. A template is a set of predefined values, and it is used to simplify the process of adding many configuration items with similar property values. A template can be downloaded from one system and then transferred to another by uploading it.
- Templates can be transferred from one system to another by downloading them from the first system and then uploading them to the other system.
- A previously added configuration item can be used as a template when adding a new one.
- A template can be created based on a previously added configuration item.
- Multistep buttons can be used to make a detour from task A to task B to add or change configuration items in task B before continuing the configuration of an item in task A. Multistep buttons are used when values in a list are configuration items set in another task.
- In some tasks there is a search function that can be used to find specific configuration items. In the search criteria, wildcards can be used, and alternative spelling is automatically handled by the system.
- Some configuration item lists can be filtered to make it easier to find specific configuration items
- Two configuration items can be compared, differences are highlighted in orange.
- Two or more configuration items can be viewed side by side.
- Response messages are displayed for both successful and unsuccessful operations.
- Batch Operations can be used to record user actions in real time and to run batches of operations that have been recorded earlier. Batch operations can be used to create several configuration tasks in a batch, for repeated or frequent operations that are time consuming to do manually.
  It is also possible to change the order of operations within a batch. Changing the previously recorded operations of a batch task could be done by navigating to change page of task.

- It is possible to perform a backup of the SNM database as well as exchange data. All data can be restored by using the restore function. The screen shows a list of all available backup files. The system will store the five latest backup directories. If more backups are made, the oldest backup directory is deleted. Each backup file is identified by a backup number, a time stamp and the system release version number.
  Restoring data is appropriate when there is reason to believe that there is mismatch in the system data. The system data will be restored to the status it had at the last successful backup occasion. Alteration of exchange data is inhibited during restore and backup.

- The Site Map shows all the tasks in the GUI. The task names are links that leads to the task in question.
- A short cut can be created, which makes it possible to do a one way jump to another task in the GUI.

For more information about how to use the features, see the *MX-ONE SERVICE NODE MANAGER USER GUIDE*.

Key Features

Application ID

The installation (site) name and the add or change information about the site are defined in MX-ONE Service Node Manager, for example contact persons and support information.

The site name is displayed in the upper right corner of the SNM, as well as on the login page. This makes it easier for a user to identify the site that has been logged on to - without having to identify the site from information presented in the URL field of the browser.

Number Plan

The following number plans are available:

Number Series

Numbers and number series for numbering plans can be managed in SNM. To enable the system to be able to state to which function a number belongs, it is necessary for the number to be defined as a specific number type. This is achieved by affiliating a number or number series to a number type. As a way of separating numbers for extensions, operators and other nodes in the network, a set of number types has been defined in the system.

The number type distinguishes the various complete and shortened form of numbers, and it is separated from the number itself.

The following number types are available:
- Directory numbers
- Common operator numbers
- Individual operator numbers
- Common abbreviated numbers
- Emergency numbers to operator
- Individual abbreviated numbers
- Route directory numbers
- Dialed Number Information Service (DNIS)
- External destination
- Least cost routing access numbers

External Number Length

Number length data helps to reduce seizure time of tone code receiving and digit sending units, as well as faster through-connection of the speech path regardless of B-answer.

If the number length of an external number consists of a fixed number of digits, Minimum Number Length and Maximum Number Length should be set to the same value. If the number length is unknown Maximum Number Length should be omitted, switch through-connection will be the result on time out, End of Selection (EOS) or B-answer.

Number Conversion

Number conversion and bearer capability substitution are features that perform conversion of sent and received numbers and of bearer capabilities and tele-services from database tables.

There are two methods for Number Conversion:
- Bulk conversion from an uploaded CSV file
- Initiating Number Conversion

Number conversion can be done per system or at route level. If the parameters **Route** and **Target Destination** are omitted, the number conversion will be made for the whole system. By stating the parameter **Route** the number conversion will be route-dependent. By stating the parameter **Target Destination** the number conversion will be destination-dependent. The route- or destination-dependent number conversion will override number conversion per system.

System Number

The System Numbers are the common numbers for the whole system. The common numbers are used, for example, to automatically set up Least Cost Routing for extensions.

The common numbers are:
- The International Prefix, which is the number to add in the beginning of the phone number to dial out of the country.
- The Country Code, which is the number to add in the beginning of the phone number to dial in to the country.
- The National Prefix, which is the number to add in the beginning of the phone number when calling a person in the same country but outside the own numbering area. The national prefix shall be removed from the number when calling an international number.

These numbers are used by tasks in both MX-ONE Service Node Manager and in MX-ONE Provisioning Manager, for example, Least Cost Routing for Mobile Extension.

Service Codes

Service codes are initiated using the `number_initiate` command with `number_type=SC`.

Call Diversion

System Call Diversion

System call diversions are common for the entire system. A system diversion number is a number of a common divertee position. The system diversion numbers are used for direct diversion and message diversion, provided that the extension lacks an individual diversion position and individual message diversion position.

A diversion position can be one of the following:
- An extension
- An individual operator
- A common operator group
- A hunt group
- A position defined by a procedure (for example, *21#)
- An external number within a private network of type SIP/H.323/ISDN

System call diversions can also be used for diversion on busy and diversion on no answer. This applies if a general individual diversion number is initiated but not valid for the current call origin. System call diversions can only be used for analog and digital extensions. For the call diversion to take effect, the extensions must be correctly categorized in MX-ONE Provisioning Manager. There can be up to three system diversion numbers. One number for internal calls, one for calls within private networks, and one for calls from public networks.

Customer Call Diversion

Customer call diversions are common for a specific customer. A customer diversion number is a number of a divertee position for that customer. The customer diversion numbers are used for direct diversion and

message diversion, provided that the extension lacks an individual diversion position and individual message diversion position.

There can be up to three customer diversion numbers per customer. One number for internal calls, one for calls within private networks, and one for calls from public networks.

Call Discrimination

Group Names

Call discrimination groups are used to restrict outgoing calls for certain groups. Descriptive names are set on call discrimination groups to facilitate the handling of the groups. By default the name of each group are set to the call discrimination group number.

Permitted Numbers

Permitted numbers are internal or external numbers that extensions are allowed to dial. The permitted numbers must be associated to one or more of the call discrimination groups.

When an extension is dialing a number, the number and the call discrimination group is checked against the list of permitted numbers. If there is no match, the calling extension will receive a congestion tone.

Each extension is, when initiated in MX-ONE Provisioning Manager, assigned one of the call discrimination groups. It is important that this information corresponds to the permitted numbers for each call discrimination group.

Emergency Number

The emergency calls (SOS calls feature) enables emergency calls to an emergency center from any phone type. With the DBC 422 02 and DBC 425 02, and also with the Mitel 6700/6800 terminals, the user is able to make an emergency call even when the phone is logged off from the exchange. When the emergency call is made, a dial-back number (A-number) associated with the geographical area is sent to the emergency center, which is then able to callback.

When an emergency number is set up, the public access code (PAC) should already be initiated, which is dialed in the beginning of a number to be able to make an external call, for example 00. Emergency calls can be made both with and without the PAC. A telephony domain should also already be initiated when the emergency number is set up.

The Least Cost Routing (LCR) tables will be automatically set up in the emergency number task, so that the original destination numbers will work in the same way as before - the changes just enables the emergency number handling as well.

Supported scenarios:
- If the PAC is an LCR. When LCR exists, then the emergency number handling will be added automatically to the LCR tables.
- If the PAC is an external destination and all the LIMs are in the same area code. When there is no LCR, the LCR will be set up automatically to handle the emergency number and public calls.
- For all other scenarios the LCR tables must be set up manually.

NOTE: The emergency number has to be based on a domestic number plan. Which means that all the numbers should start with the area code.

Extensions

Account Code

Account codes are used to charge a call to an account code, which can represent a particular project, department or client, instead of charging the calling directory number. Account codes are also used to prevent unauthorized telecommunication usage by forcing the extension to dial an account code before dialing an external number.

Common Category

Common category settings used for analog and digital extensions can be managed from SNM.

The privileges and settings for all analog and digital extensions can also be defined in SNM. All privileges are organized in profiles, which are later applied to each extension number when setting up that type of extension. Most systems have less than 10 profiles, which covers all types of users.

Common Service Profiles

Common service profiles define the privileges and settings for all IP and mobile extensions. All privileges are organized in profiles, which are later applied to each directory number when setting up that type of extension. Most systems have less than 10 profiles, which covers all types of users.

The common service profile given in the authorization code is used when a valid code is dialed from a generic extension. To an authorization code a common category code or a common service profile is affiliated. It is used to give the calling party another, higher, category or service profile when a valid authorization code has been dialed.

Common Abbreviated Number

A common abbreviated number is a short number which expands/translates into a complete number. It must be assigned a class and can have a presentation restriction. A common abbreviated dialing number does not have to be affiliated with any directory number. It can also be limited to one extension.

Common Authorization Code

The common authorization code provides two different functions:
- Locking and unlocking of an extension (when locked, a lower class of service is used).
- Authorization code dialing, which enables the calling party to use other class of services than the extension is programmed with.

When a valid authorization code is dialed from an extension, the common category code or common service profile given in the authorization code will be used. This type of authorization code is suitable when there is need for a code that can be used from any extension, or for visitors that do not have their own extension in the system. A common authorization code does not have to be affiliated with any directory number, but it can be limited to one extension.

Delay Seizure List

A delay seizure list defines the time delays from a call are received until signals are given on phones associated with an extension. The time delay is used for extensions using the functions parallel ringing or personal number, and the delay time is set per extension type (IP, digital, etc.).

An extension can be associated with one delay seizure list per function, where the list defined for the personal number function has the highest priority.

Force Mobile through PBX

Force Mobile through PBX is a service offered in the mobile network. The Force Mobile through PBX will force every call made with the mobile phone to route via the PBX.

Calls made to the mobile phone will also be routed via the PBX MX-ONE Provisioning Manager and MX-ONE Service Node Manager support initiation and removal of Mobile Extensions with the Originating Service Access Code (OSAC), Terminating Service Access Code (TSAC), Public Call Prefix (PCP) and Access code for the route to the mobile network. OSAC, TSAC and PCP need to be synchronized with the mobile operator for forced on PBX functionality.

This feature may only be used when forced on PBX services are offered from mobile operator.

Operators

Different operator features can be managed from the SNM. Note that this section is not valid for InAttend, only for integrated operators and attendant work stations older than the InAttend client.

Operator Groups

An operator group name or call origin group name is associated with a call origin group number. There can exist up to 100 operator groups. A unique combination of call type, route number (if any), and operator call number from a call origin type. Different origin types can be combined into one call origin group (operator group).

Group Members

Operator group members can be manage by specifying which operator that handles the different operator groups as well as specifying answer choices for the operator.

Operator Individual

Before adding an operator individual, common and individual operator numbers, common direct in-dialing numbers, emergency and external destination numbers as well as route data for origin types need to have been configured using Number Plan on the Number Analysis tab.

Operator Display Messages

Display messages are route names and simplified diversion messages that are displayed on the Operator Assistant. The route name is displayed in the Operator Assistant when the operator receives a call from a route. Simplified diversion messages for the ten languages in the system are displayed on diversion.

Central Operator Number

Central operator numbers for common operator calls in an exchange are supported.

Common Access Code

The common access code allows all customers to have the same common operator call number for internal, diverted and rerouted calls.

Day/Night Mode

The day/night class of service is controlled by the exchange day/night status. The exchange day/night status is used to give some services or features different characteristics in a night switched exchange than in a day switched exchange.

Operator Assistant Server Port

An operator individual needs an initiated Operator Assistant server to be able to send and receive information. The server and any associated Operator Assistants must be initiated in the same LIM. A TCP server port is initiated for registration in a LIM with a specific port.

NOTE: To be able to remove or change a port number for a LIM, no operators are allowed to exist in that specific LIM. Operator Individuals are removed in the Operator Individual task.

Call Center

Automatic Call Distribution is an automated solution to distribute a large quantity of incoming calls to predetermined services which are requested by the caller. Each service is connected to a CTI group which consists of one or more agents handling the calls. It is then possible to handle a large number of incoming calls without the corresponding need for operators to route the calls.

ACD Group

Automatic Call Distribution is an automated solution to distribute a large quantity of incoming calls to predetermined services which are requested by the caller. Each service is connected to an ACD group which consists of one or more agents handling the calls. It is then possible to handle a large number of incoming calls without the corresponding need for operators to route the calls.

ACD Group Member

This task is used when managing members of the available Automatic Call Distribution groups, as defined in the ACD Group task. The task includes defining clerical times and selection priorities for the group members.

ACD Parameters

The ACD Parameters task is used for configuring the behavior of ACD groups within the system. The settings are general and applied to all ACD groups.

Groups

Group Do Not Disturb

Groups and members can be added to the Group Do Not Disturb feature using SNM.

To add members or groups to the Group Do Not Disturb feature means that calls to an extension included in the group are not signaled on the telephone device. If the extension has activated any diversion or an individual divertee position exists the call will be diverted.

NOTE: An appropriate class of service (or for analog and DTS terminals 'master extension' setting) must have been configured in order to use the Group Do Not Disturb function.

Group Do Not Disturb is only applicable when at least one extension with GDND class of service or master extension has been initiated. Master extensions and GDND class of service can be initiated in MX-ONE Provisioning Manager.

Customer

The customer group feature provides for companies to subdivide their resources or make it possible for several smaller companies to share the same system. Each subdivision or company is defined as a customer. There can be one customer group with up to 50000 members. When adding customers to a group, each customer is assigned a customer number automatically.

Hunt Group

A group of extensions can be called with a common number. Incoming calls are routed to a free extension in the group, either with sequential hunting or evenly distributed. All extensions in a group keep their own private number and CoS. An extension can be a member of several hunt groups.

An extension can temporarily withdraw from the group by either activating Follow-me to its own phone, or by using the dedicated hunt group logout procedure. Calls to a group from which all members have excluded themselves are diverted to the group's divertee position.

Hunt Group Member

A group of extensions can be called with a common number. Incoming calls are routed to a free extension in the group, either with sequential hunting or evenly distributed. All extensions in a group keep their own private number and Class of Service. An extension can be a member of several hunting groups.

An extension can temporarily withdraw from the group by activating Follow-me to its own phone, or by using the dedicated hunt group logout procedure. Calls to a group from which all members have excluded themselves are diverted to the group's divertee position.

Pickup Group

A call pickup group comprises a number of extensions (members) that have been assigned as a common group number (sequence number). A member in a group can pick up a call to other members in the same group by dialing a code on the telephone. Maximum four answer groups can be assigned to a call pickup group.

The order of priority for answering calls to a call pickup group is:

• Call to the own group

- Call to the answer group in the sequence, in which the answer groups have been affiliated to the call pickup group.

External Lines

Corporate Name

Corporate name is used to set the calling party name for DMS 100 protocol. It can either be an individual name or a company name which is presented to the public network users.

Route

Network traffic between an MX-ONE and a public exchange or an interworking exchange requires an external line that is assigned to a free equipment position in the MX-ONE. A number of external lines with the same characteristics is a route.

Routes can be initiated with different signaling, service, and traffic characteristics to suit different types of external lines. A route can have external lines in several LIMs, providing distribution of the traffic load. For each route that permits outgoing traffic, one or more external destinations should be associated.

It is possible to initiate up to seven alternative routes to one external destination. Hardware is optional for IP routing. But for the four types of ISDN routing (ISDN 30B+D Private, ISDN 30B+D Public, ISDN 23B+D Private, and ISDN 23B+D Public), hardware is mandatory to carry traffic on initiated routes.

Destination

One or more destinations should be associated to each route that permits outgoing traffic. Customers created in the task Customer Group can be associated with a destination. It is necessary to create a master destination (primary routing choice) before associating a customer with the destination or creating an alternative route choice.

Busy No Answer Rerouting

Busy No Answer Rerouting is used to initiate day and/or night service positions within the own exchange for one or more routes or external lines within a route.

Vacant Number Rerouting

Vacant numbers can be used to define which directory number direct in-dialing traffic will be rerouted to when calling a vacant number, an incomplete number or no digits are entered. Specific directory numbers can be defined for day and night.

Customer Rerouting

Customer Rerouting is used to define to which directory number a call from a customer will be rerouted due to for example no answer. It is possible to define one rerouting position per customer for a day switched PBX and one per night switched PBX.

Public Exchange Number

The public exchange numbers is used when composing a complete number for the public network.

Charging

In SNM it is possible to initiate charging models, as well as change the call metering characteristics, that is, set the cost per unit pulse.

The type of charging model for a particular route should have been selected when setting up routes for extensions before initiating a charging model. Whenever a request for Advice Of Charge is received from the public ISDN network, the cost per unit pulse values are used to calculate the total amount. AOC is a service that displays charging information (in a specific currency) to a charged extension. You can change the cost per unit pulse for one or more tariff models at the same time. At least one of the fields must be assigned a cost per unit pulse value. Note that the additional tariff models are normally not used.

Mobile Direct Access Dest.

Each external destination can be assigned a name. The names set for the destinations will be used by other tasks in MX-ONE Provisioning Manager, for example, the Extension task.

System Data

Own Exchange

The own exchange number is used by the exchange for route optimization.

Route optimization will be used when a path has been established through several exchanges in a private network and a more suitable path is available.

When a permanent call is established the system tries to set up this optimal path via a minimum of exchanges.

The own exchange number for route optimization is of the same type as the normal own exchange number. In a private net, every exchange should be given an own unique exchange number for route optimization, it must not be used for any other purpose. The unique exchange numbers should be initiated as external destination codes in the other exchanges in the net. This means that every exchange number for route optimization states a specific exchange.

System Data

In SNM it is possible to change system data property values for conference, transfer and diversion. These are general options, valid for all users in the system.

Time Supervision

On this screen you can change property values for Time Supervision.

IP Phone Configuration

The configuration of IP phones is handled in the SNM. The IP Phone configuration task consists of many parts and in this section the sub menus under **Telephony > IP Phone** are described.

The figure below shows an example of how the different units interacts. There are three telephony domains defined. There is one IP phone software server in the main site with a folder structure that is mapping the domains. The IP telephones in each domain fetch configuration files under the corresponding folder from the IP phone software server.

Figure 3.1: Example of an IP Phone Configuration File
scenario
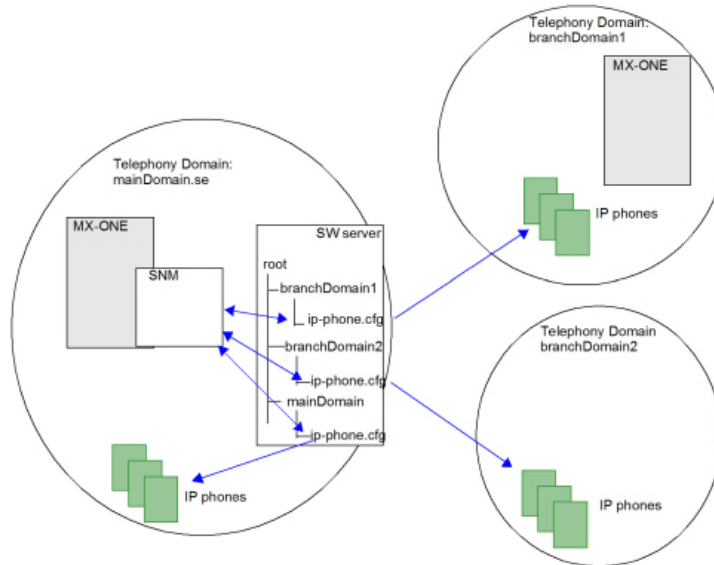
IP Phone Administrator

The IP phones in the network can be monitored. This is useful when trying to find the IP address of a specific IP phone, to get an overview of all IP phones even the phones that are not registered, or to see the firmware version in different IP phones.

Each IP phone sends a message to the IP Phone Administrator at status changes for example registered, not registered, log on rejected, the phone has not sent any message for a long time, etc. The phones sends also data in these messages for example mac address, IP address, directory number, firmware and hardware version etc.

The following IP phone families have support towards IP Phone Administrator:
*   DBC 42x (MiVoice 442x)
*   DBC 43x and DBC 44x (Mitel 7400)
*   SIP Phone (68xx and 69xx)

Security Policy

In this sub menu the administrator can select which security policy that should be used in the system. By default no security policy is used.

To provide more flexibility in administration and for sufficient system security, there are three different security policies:
*   All secure, only extensions with support for security functions (Transport Layer Security (TLS)) are allowed to log on.
*   All secure and extension exception, extension numbers with a security exception are allowed to logon insecurely. If an extension number that is not allowed to have a security exception tries to logon insecurely the registration will be rejected.
*   All secure and type exception, terminals with a security exception are allowed to logon insecurely. This applies for example to:

- Mitel BluStar Client
- DBC42x01 (version 1)
- H.323-compatible soft clients

If a terminal type that is not allowed to have a security exception, for example, a DBC42x02 or Mitel 6700/6800/6900, tries to logon insecurely, the registration will be rejected.

Telephony Domain

Telephony Domains are clusters of IP addresses (IP phones) that are defined in the MX-ONE.

In this submenu the system administrator can define:
- Emergency number settings.
- Telephony domains (or directories) used to host different configuration files on the software server.

Emergency Number

Telephony domains are associated to a local emergency number and area code, as well as the dial-back number for emergency calls.

When an IP phone makes an emergency call it is not possible to see its physical location or which number to callback to. The IP phones are therefore divided into telephony domains, and by using a list over the domains and their dial-back numbers, the emergency center can callback.

The telephony domains are also used in the exchange to route the call from the emergency center to the right extension.

An advantage with grouping the IP phones into domains is that when an emergency call is made from an IP phone that is not logged on and therefore has not been given a number, the server can route the emergency centers call to the extension that dialed the emergency number.

Multiple Configuration Files

A certain group of IP phones can often have different characteristics compared to other groups of IP phones concerning which codecs to use, emergency number data etc.

Each group of phones reads a separate configuration file stored under a directory with the same name as the telephony domain. It is also possible to create a domain folder named as the subnet address (for example 192.100.26.128-26).

In this sub menu it is possible to create both these types of folders on the IP phone software server.

This option can only be used for the families DBC42x, DBC43x and DBC44x.

SIP External Domain

The system administrator can initiate external domains, which makes it possible for phones that are registered at domains outside a telephony system domain to get access to the telephony system. This can be, for example, soft-phones belonging to a Microsoft Lync Server domain.

IP Phone Software Server

The IP phone software server is used to host configuration files and software to the IP phones. The SNM `IP Phone Configuration File` simplifies the management of IP phone configuration files, the system

administrator gets help to fill in all parameter values and the configuration files are automatically stored on the IP phone software server.

The IP phone software server is a stand alone server and must contain a component called IP Phone Software Server Configuration Management Application for Windows to be able to communicate with SNM. This component has the product number CXC 109 0055/1 and includes also the Tomcat web server.

In large systems there may be several IP phone software servers in different domains. Each IP phone software server may support multiple domains and multiple families of IP phones, which means there can be multiple configuration files on each server.

For information on how to install an IP phone software server, see installation instructions for different IP phone families.

Connect IP Phone Configuration File

In this sub menu the system administrator can connect (register) already existing configuration files to SNM. The task Connect IP Phone Configuration File contacts the chosen server, and makes a search for configuration files. The found configuration files are presented in a list. The list shows the properties of the configuration files:

- File Name, which is the name of the configuration file Folder, shows in which folder the file is located
- Family Name, shows which configuration file family the file belongs to
- Connected, shows if the file is registered (saved using SNM) or not

If the configuration file is registered, the property Connected will be displayed as YES. If the file is saved manually or outside SNM, the property Connected will be displayed as NO. The aim is that all configuration files shall be connected.

When a file is being connected, the system validates the file (checks if it is in a different format or if there is something corrupt with the file). If no faults can be found in the file, it will be registered and automatically included and available in the IP Phone Configuration File task. Several files can be connected at the same time.

Manage IP Phone Configuration File

The IP phones use configuration files to initiate parameters in the phone. Examples of properties that can be set in the configuration file are:

- IP addresses to the gatekeeper or SIP server
- Software versions
- Codec priority
- Tones
- Function keys
- Security and encryption

The task `IP Phone Configuration File` helps the system administrator to fill in the values in all parameters in configuration files for the different types of IP phones. Integrated help text minimize the need for separate documentation. The file is automatically stored on the software server, see *SIP External Domain*.

The following IP phone families have support in SNM for creating the configuration files:

- DBC 42x (MiVoice 442x)
- DBC 43x and DBC 44x (Mitel 7400)

- Mitel 6700/6800/6900
- Mitel BluStar 8000i

It is possible to perform a backup of the configuration files. All data can be restored by using the restore function. Only one backup can be stored, a new backup will overwrite the old one.

PMSNM to Support Encrypted Phone Configuration

PMSNM now supports .tuz encryption of configuration files for Mitel SIP phones. This encryption is required for security of IP phone configuration.

Enabling Encryption of IP Phone Configuration

Following are the steps of IP Phone Encryption:
- In the **General Settings** page of Mitel SIP Phones, select the **Enable Encryption**.
  Note that once encryption is enabled, encryption password and firmware version fields will be visible.
- Enter the Encryption Password, which is used for encrypting file in IPP server.
  The same password is used to encrypt the phone configuration file in .tuz format.
- Select the appropriate Firmware version for encryption installed in the phone from the drop-down list.
- The selected phone model series configuration will be encrypted and .tuz encrypted files will be stored in its corresponding directory.

Figure 3.2: IP Phone Configuration
File

Un-registration

Un-registration is used to remove registered IP phones from the system and can be performed for all IP phones in specified servers, IP phones associated to specific extensions, or all IP phones in a system.

Un-registration can also be used for bringing IP phone configuration file changes into effect. By unregistering the IP phones that uses a specific, updated configuration file, the phones will download the updated configuration file data at next registration.

By using forced un-registration, the specified IP phones are immediately unregistered. This means that present calls will be terminated for these phones. For non-forced un-registrations, only idle IP phones are unregistered.

Media Encryption

To protect Voice over IP media streams, MX-ONE supports Secure Real-time Transport Protocol (SRTP). Support for SRTP is given in the IP phones (Mitel 6700/6800 phones, DBC 42x 02, DBC 43x 01, and DBC 44x 01) and in the MGU type of media gateway. SRTP support is not implemented in the Media Gateway version 1 (BFJ 901 03), in the Operator Assistant media device, or in softphone clients.

Function

SRTP makes use of the Advanced Encryption Standard (AES) with a 128 bits key to protect the media streams. The encryption keys are exchanged according to the ITU-T H.235.8 specification or to RFC 4568 for SIP. For a two-party phone call, four keys will be needed to be exchanged between the two parties. Each party originating a media stream will generate two keys, a Master Key and a Master Salt and send them to the other party during the call control phase. These values are generated using high-entropy pseudo-random number generators in the IP telephones and in the MX-ONE Service Node. The actual keys used by SRTP (one encryption key for each direction, one integrity key for each direction) are being calculated using the procedures defined by the SRTP specification. The signaling messages carrying the encryption keys are encrypted by TLS before being sent.

BluStar 8000 Configuration

For Mitel BluStar 8000i Desktop Media Phone it is mandatory to read the user unique configuration file `<user>.cfg` to be able to register towards the SIP Call Server. SNM comes with the component "BluStar Configuration" that creates this file automatically and this component does not contain any user interface.

For details of the interface between the phone, SNM and MX-ONE Service Node, see installation instructions for Mitel BluStar 8000i Desktop Media Phone with MX-ONE:

The `<user>.cfg` files are stored in the MX-ONE server where SNM is located.

DECT system

DECT systems can be set up in the MX-ONE Service Node Manager.

System ID

The DECT System ID value is received at the installation. It is a identity that every telephone listens to because it is the system that it belongs to. The Primary Access Right Key (PARK) value can be entered into the portable device to force it to lock to a certain DECT system.

NOTE: hanging the SARI leads to that all the Portable devices needs to be restarted and manually connected to the DECT system again.

DECT Board

DECT Board is a hardware (the ELU31 board) that must exist in a LIM. Every base station is connected to a ELU31 board. All the ELU31 boards are connected to each other with a synchronization cable.

DECT Base Station

The DECT base station is the sender and receiver that communicates with the phones. It is connected to the DECT board with a cable. The DECT base station is also called Radio Fixed Part.

DECT SMS

The Short Message Service (SMS) is handled through SMS Service Centers that are located outside the MX-ONE. The SMS service centers store and transmit the text messages. Text messages can be received in any call state, for example, during an ongoing call. The MX-ONE always listens for incoming text messages and sends them to the SMS Service Center. An SMS session is handled as two separate calls, partly for the A-extension to send its message to the server, and partly for the server to transmit the message to the B-party, which can be one or many receiving extensions. The SMS service center act as a server when sending messages and as a client when receiving messages. Both the DECT SMS Server and the DECT SMS Client must be initiated, for the SMS service to work.

Server

There can only be one SMS server in each LIM. The DECT SMS Server is initiated by assigning it a directory number, a LIM number, a common service profile and a customer name. The SMS service center sends the SMS to the IP address of the specified LIM, and the LIM distributes it to the B-party.

Client

The DECT SMS Client is initiated by assigning it an IP address, the port number of its communication port, and the number of the LIM where it shall be located. The extension sends the SMS to the MX-ONE, and the MX-ONE distributes it to the SMS service center on the IP address specified for the SMS client.

Connections

Information System

Up to 16 information systems (e.g. voice mail systems) can be connected directly to the PBX. Additional systems can be connected to a directly connected information system and are thereby indirectly connected to the PBX. All systems connected to the PBX - directly or indirectly - have unique system numbers to permit the PBX to identify them.

CMG Connection

CMG Connection is used to establish and manage the media link between the CMG Server and MX-ONE.

Messages

Message Diversion

Message Diversion is activated by an extension procedure containing an interception message. The interception message is sent to the connected intercepted computer.

On a call to the extension with the message diversion function activated the call will be diverted to a defined divertee position (answering position) for message diversion.

The purpose is to provide answering position personnel with a better means of giving callers meaningful interception messages.

Message Waiting Setup

An information system can consist of, for example, a message switching system of the type interception computer, text messaging system or voice mail system. It is connected to the exchange through the general interface for information systems. The message waiting function is included in the general interface for information systems. When message waiting is activated, the extension is notified on the telephone if it has received a message in an information system.

Notification can take place in the following different ways:
- Ring signal. Ringing is achieved as a single burst (pling) on the bell for an analogue telephone. The period between two plings is 15 minutes (changeable by application system parameter PARNUM=45). If the extension is diverted (direct diversion, follow me, or message diversion), no notification will be given.
- Special dial tone.
- Lamp indication. Applicable only for telephones with a dedicated message waiting lamp and connected to an extension board that is capable of providing message waiting lamp indication. When message waiting is initiated, the lamp on the telephone set is turned on.

Message Waiting

Message waiting is used to manage and print existing Message Waiting entries.

If Message Waiting entries have been previously configured, the main screen will show basic configuration details in a list, such as **Information System Identity Name**, **Display text**, **Key Function**, and **Digit property values** for each message waiting.

Voice Announcements

Voice announcements are used to inform callers using pre-recorded messages, for example a speaker voice or music if the called extension is busy or for calls that are placed in a queue. The voice announcements in SNM are valid for groups and extensions.

Voice announcements can be uploaded to the web, to make them available to other MGWs in the system. Voice announcements can also be distributed automatically to all MGWs in the system.

A prerequisite for setting up recorded voice announcements for IP and mobile extensions is that the system has been initiated with extensions, groups and so on. Any voice or music messages that are going to be added to announcements must also be present on a file system in PCM format (A-law or u-law,

mono, sampling frequency 8000 Hz). Any sound recording application supporting this format can be used. Before setting up voice announcement, it is also required to know for which types of incoming call situations that recorded voice messages are needed.

Voice Messages

This is to manage voice messages, as well as to listen to existing voice messages.

Announcement Setup

Announcement setup assigns messages to announcements, both the default message and a message based on the estimated waiting time. More than one message can be assigned to an announcement, provided the estimated waiting time ranges vary for different messages.

Operator Group Announcement

This is to manage, view or print a voice announcements for operator groups.
NOTE: MX-ONE Service Node Manager only supports management of voice messages for servers using MGU media gateways.

Operator Individual Announcement

This is to manage, view, or print announcements for operator individuals.

When a call is made to an operator individual, a queue announcement can be provided to the calling party when the preset time in queue has been reached
NOTE: MX-ONE Service Node Manager only supports management of voice messages for servers using MGU media gateways.

Announcement Group Setup

This is to manage, view or print announcement groups.

On initiation, an announcement group is allocated to a table which makes it possible to determine separately for every call origin group which recorded voice announcement an incoming call is to be given before it is connected to the operator. Only the call origin groups which are given a recorded voice announcement can be associated with an announcement number. Calls to omitted call origin groups are connected directly to the operator.

Members of announcement groups are defined in
NOTE: MX-ONE Service Node Manager only supports management of voice messages for servers using MGU media gateways.

Announcement Group Member

This is to manage, view or print announcement group members. A prerequisite is that announcement groups have been defined in Announcement Group Setup.

Announcement Group Member allocates one or more operators to an announcement group. Only one announcement group can be associated with an operator's directory number. The same announcement group can be associated with several operators (directory numbers).

When the operator answers an incoming call, a recorded voice announcement is selected from the announcement group that has been assigned to the operator with this command. The choice of announcement from the announcement group is based on information about the call origin group

NOTE: MX-ONE Service Node Manager only supports management of voice messages for servers using MGU media gateways.

Hunt Group Announcement

This is to manage, view or print announcements for hunt groups.

The Recorded Voice Announcement feature allows recorded voice announcements to be provided to a calling or connected party to inform of the status of the call in various traffic cases.

Depending on the status of the group, different kinds of announcement can be provided to the calling party

NOTE: MX-ONE Service Node Manager only supports management of voice messages for servers using MGU media gateways.

Extension Announcement

This is to manage, view or print extension announcements.

When a call is made to an individual extension, different announcements can be provided depending on the status of the extension. There are two types of announcement that can be provided for an extension call; welcome announcement and continuous announcement.

A welcome announcement can be provided to the calling party based on the called party's directory number, when the call is made to an extension. When a call is diverted to an individual, the diversion announcement will be played first to the calling party before a welcome announcement.

NOTE: MX-ONE Service Node Manager only supports management of voice messages for servers using MGU media gateways.

Vocal Guidance

This is to manage, view or print vocal guidance traffic cases.

Some of the traffic cases are identified and are considered as vocal guidance traffic cases for which a vocal guidance, that is, a recorded voice announcement can be played to the user. With this feature, the user receives a recorded voice announcement in addition to the tone messages when encountering the vocal guidance traffic cases. Vocal guidance can also be made customer specific by assigning customer number to the traffic cases and its announcements.

After voice announcement is disconnected, appropriate tone message for the traffic case is provided. When the recorded voice announcement is not available, appropriate tone message for the traffic case is provided.

NOTE: MX-ONE Service Node Manager only supports management of voice messages for servers using MGU media gateways.

ACD Group Announcement

This is to manage, view or print announcements for ACD groups.

NOTE: MX-ONE Service Node Manager only supports management of voice messages for servers using MGU media gateways.

The Recorded Voice Announcement feature allows recorded voice announcements to be provided to a calling or connected party to inform of the status of the call in various traffic cases.

Depending on the status of the group, different kinds of announcement can be provided to the calling party:

- Group welcome announcement
- Group queue announcement
- Group repeat queue announcement
- Group continuous announcement

Setting up a Branch Office

Only Branch Offices that contains a Survivable Branch Node (SBN), that is, the branch office has its own public access, can be created in the Branch Office task in SNM.

A branch office, also called a remote office, is a selection of IP phones that can be located anywhere in the world, for example in another country or on the second floor of a building where the main office is located. A branch office can have an SBN, which is located at the branch office. If the IP network fails, the phones will automatically fall back and register to the SBN.

A branch office can also be one of the following two types (both solutions are without an SBN):

- Only contain IP phones
- A small office with another area code than the main office

The branch office task uses the least cost routing (LCR) function to enable local-breakout, which is used to route a call internally before it goes out public. For example, the exchange is located in Stockholm and the branch office is located in Oslo. If an emergency call is made in the branch office, the call will be routed to the exchange in Stockholm. The LCR function in the exchange routes the call to the SBN in Oslo, and from there the call is connected to the public network and received by the emergency center in Oslo.

For an overview of the Branch Office scenario, see the figure below.

Figure 3.3: Branch Office
scenario
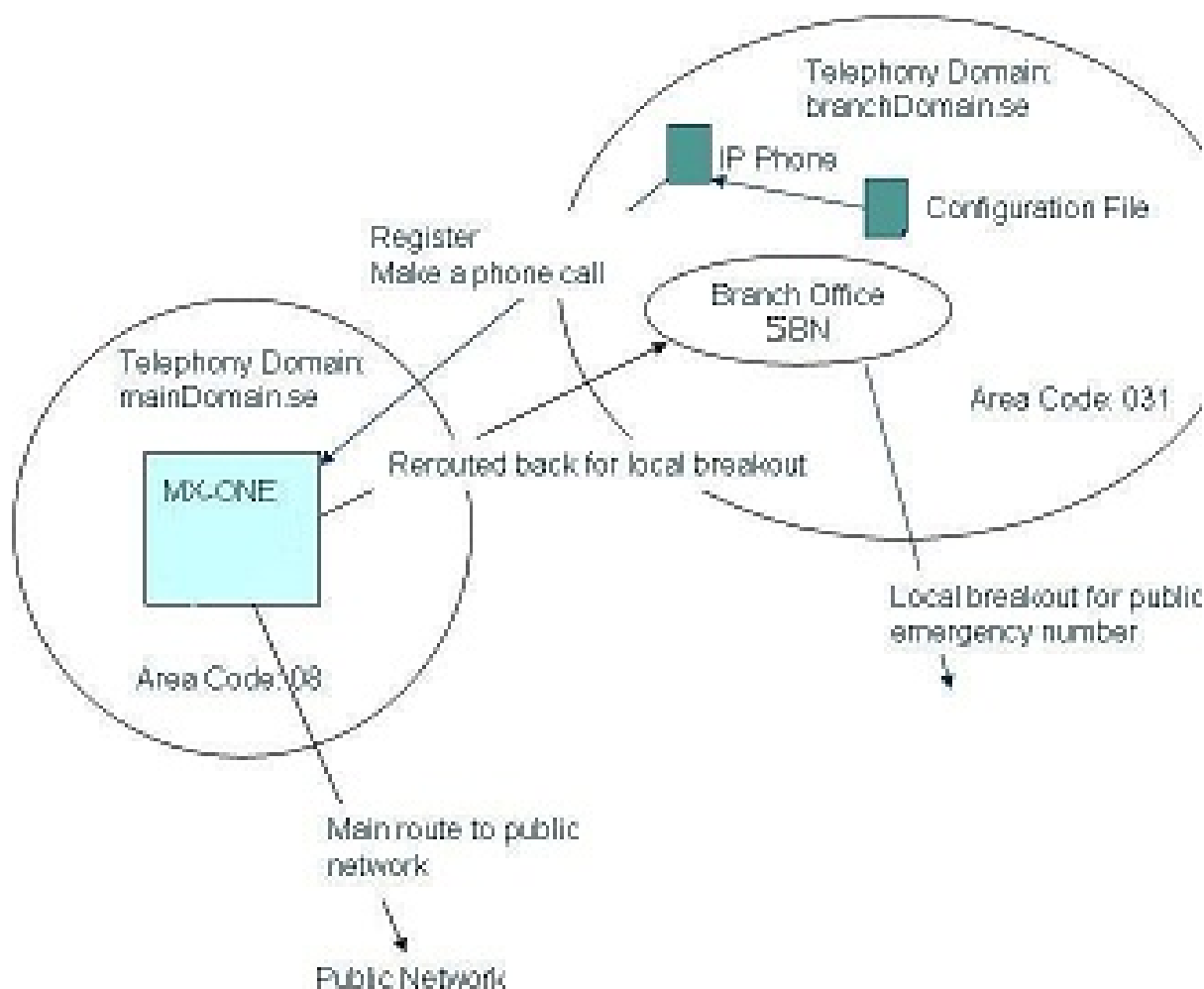
Routing Server

The routing server can either be an MX-ONE traffic carrying node in the network or an MX-ONE node with server functionality. The routing server stores the IP routing and alternative routing information on a permanent basis. This means that all the routing satellites (clients) can retrieve the same routing information without storing it permanently. When requested the routing server sends the routing information to the routing satellite (client).

The routing server stores the IP routing and alternative routing information on a permanent basis (reload data) while the routing satellite (or client) stores the routing information on a temporary basis. The routing satellite requests the routing information from the routing server, to update the stored routing information. Example: When a call or execution of a feature (for example Deflection) is being established towards a destination, the routing satellite requests and retrieves the required IP network information either locally or from the routing server.

Routing Satellite

The routing server stores the IP routing and alternative routing information on a permanent basis (reload data) while the routing satellite (or client) stores the routing information on a temporary basis. The routing satellite requests the routing information from the routing server, to update the stored routing information.

Example: When a call or execution of a feature (for example Deflection) is being established towards a destination, the routing satellite requests and retrieves the required IP network information either locally or from the routing server.

Time Supervision

The time supervision is used for starting and stopping:
- The time-based update routine for all the stated entries in the routing satellite.
- The time-based satellite check routine in the routing server

CSTA Server

The Computer Supported Telecommunications Applications (CSTA) is an application protocol that allows the interfacing of a computer domain with a telephony domain. It supports applications or services normally provided by one domain to be available to the other domain that normally does not support such application without major enhancement or redesign. The purpose of this functionality is to support a Computer Telephony Integration (CTI) protocol. The CSTA application in MX-ONE Service Node functions as a server to support the CSTA clients.

Each CSTA Server is installed on a LIM, but only one CSTA Server protocol type can be in each LIM. The CSTA Server is either Initialized, Enabled or Disabled.

The main type of application for the CSTA implementation is call centers, where agents handling incoming calls can get synchronized screen updates with the telephone calls. Other types of applications could be outbound call centers, like telemarketing or debt collection.

The CSTA Application supports the Web Service clients through a Web Server on a port different from the one used for CTI clients. The CSTA Server in MX-ONE supports the CTI application or the Web Service clients through the following functions:
- Generating CSTA events for monitored objects, that is, the status of the object or the queue status of the object.
- Performing telephony functions that are requested from the CTI application, for example, to make calls.

The CSTA Server can be removed even though if there are extensions monitored by that CSTA server at that moment.

Monitored Devices

The CSTA Server in MX-ONE supports the CTI application or the Web Service clients by generating CSTA events for monitored devices, that is, the status of the device or the queue status of the object.

The monitored devices are shown in the list. The list is based on the Server Number and the protocol (ECMA323/TR87 uaCSTA or both).

A monitored device can be:
- Analog extension
- CAS extension

- Digital extension
- Operator or a Call Origin Group
- IP extension
- Remote extension
- ACD Group
- API User
- CTI Group
- CXN
- DTS_ADN
- PBX Group
- Generic Extension

Enterprise Gateway

Using this option, you (admin) can configure and manage Mediatrix Sentinal 400 (EX-Controller) and Sentinal 100 (GX-Controller) Gateways as Media Gateway in Service Node Manager.

NOTE: The Gateway has to be configured before the configuration from SNM is done.

The Mediatrix Gateways bundles the capabilities of a Session Border Controller and a Media Gateway. Robust, field-upgradable, and ready for third-party software integration, this multi-service business platform is designed for medium and large enterprises. These Gateways are ideally targeting applications for up to 2000 users.

Configuring Enterprise Gateway

This task is only for creating Enterprise Gateway (EG) and the same can be done by providing the Enterprise Gateway IP that has already been provided to a EX/GX setup. By configuring the IP of the gateway, you can directly go to the GUI of the EX/GX gateway and configure the same. For more information, see the details about Sentinel 100 and 400.

To Configure Enterprise Gateway, do the following:

1. Enter your valid **User ID** and **Password** to login to SNM application.
2. Select **Services** > **Enterprise Gateway**. The following screen appears.

Figure 3.4: Configuring Enterprise Gateway
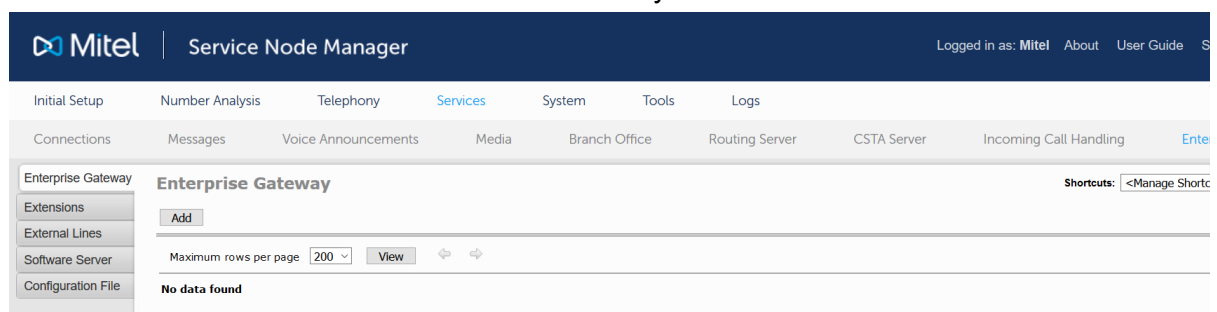
While adding enterprise_gateway, you must make a Database (DB) entry to enter required details of the Enterprise Gateway in the DB.

Adding a New Enterprise Gateway

In this, you need to enter valid Enterprise Gateway IPs or Host Name that are used to add the EX/GX Gateway and post adding the gateway. The same can be configured by using the hyperlink on the Enterprise Gateway page. Similarly, enter the IP of the Subsystem, which is associated with the corresponding EX/GX Gateway and the same can be configured in EX/GX Gateway GUI under **SIP**--> **Servers**. A confirmation screen is shown if the EGs are created successfully.

```
Basic
```

To add a new **Enterprise Gateway**, do the following:

1. Click the **Add** button to add a new Enterprise Gateway. The following screen appears.

Figure 3.5: Basic Parameters of
EG

2. Enter the **Enterprise Gateway IP** to add the EX/GX Gateway. A Database entry is made to update the details of the Enterprise Gateway in the DB.

> **NOTE:** A user can add multiple Enterprise Gateways.

3. Enter the IP address or Host name of the **MX-ONE** or Subsystem, which is associated with the corresponding EX/GX Gateway, the same can be configured in EX/GX Gateway GUI under **SIP** --> **Servers** as shown in the following screen.

Figure 3.6: Servers

4. Choose the **Enterprise Gateway Type** (GX/EX). Two different types of Gateways are listed. Select the appropriate type while configuring the Gateway.

5. Enter the **Enterprise Gateway Name** of EX/GX and click **Apply** button to view the newly added EX/GX configuration details. Otherwise, you can click the **Advance** button to add more details as described in the following section.

`Advanced (Primary Configuration)`

Using this option, the user can add or modify the primary configuration details, such as **Static Default Router**, **NTP Server Name**, **DNS Server Priority 1**, and **DNS Server Priority 2**. All these configurations are mapped to a command file and will be executed in the EG server.

Figure 3.7: Advanced (Primary Configuration)

6. Enter the IP address of the **Static Default Router** for EG.

7. Enter the IP address of the **NTP Server Name** for EG.

8. Enter the IP address of the Primary **DNS Server Priority1** for EG.

9. Enter the IP address of the Secondary **DNS Server Priority2** for EG.

10. Click **Apply** button to create a EG configuration according to the settings done, which is shown in the following screen.

Figure 3.8: Added Enterprise Gateway
IP
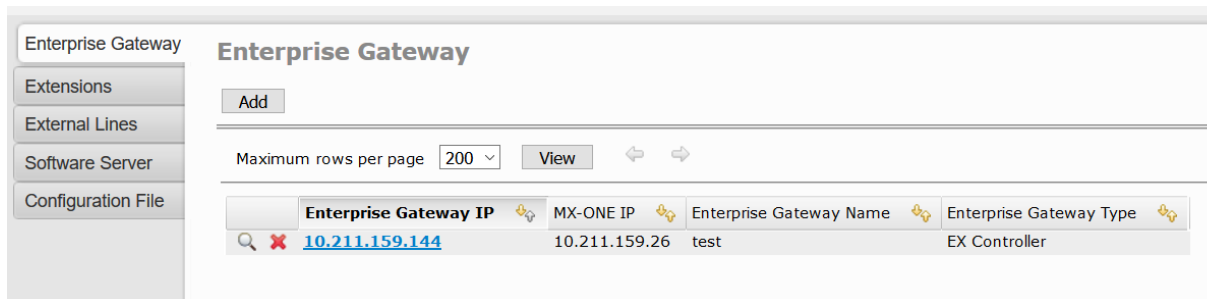
Viewing the Enterprise Gateway

While viewing the media_gateway as shown in the Figure 2, a DB call is made to the Service Node and the details of the initiated Enterprise Gateways are fetched. If any Enterprise Gateway is previously configured, the main screen will show basic configuration details in a list. Note that it shows only the Basic parameters not the Advanced parameters.

For each row, you can click one of the icons to the left of the list to:

1. View the Enterprise Gateway details

2. Change the Enterprise Gateway details

3. Remove the Enterprise Gateway

To change the sorting of the list, click the sorting direction arrow next to the appropriate column heading. Each column can be sorted in ascending or descending order.

NOTE: Note that when you click the newly created EG hyperlink, it takes you to the landing page of the EX/GX Controller, where you need to enter your valid User ID and Password to view the configuration details.

Adding or Changing Extensions

Click **Change** to modify settings for the created extensions for the selected Enterprise Gateway. This opens the **Extensions Configuration - Change** screen, in which extensions are to be added to create the extension on the EG.

Figure 3.9: Extensions Configuration -
Change

Enter the Extension details in the desired fields and click **Apply** to create the Extensions. A confirmation screen appears as shown in the following screen if the Extensions are created successfully.

Figure 3.10: Extensions Configuration Change
Successful
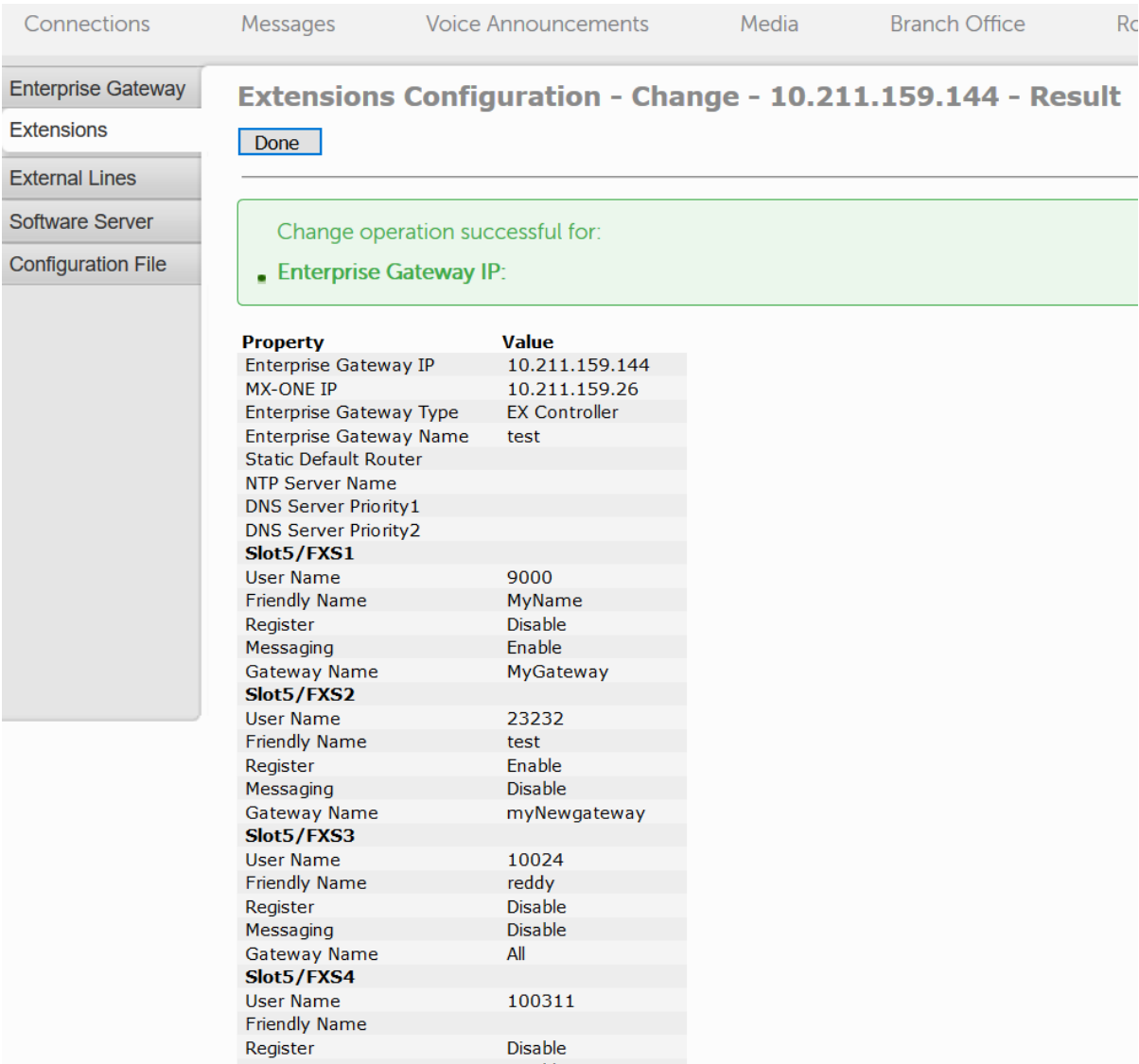
Click **Done** to return to the main Extensions Configuration screen.

If you click the **Enterprise Gateway IP** hyperlink of Extensions Configuration, then the following screen appears based on your EG type that you have selected.

Figure 3.11: EX Controller
Extensions

Figure 3.12: GX Controller
Extensions

Click **Cancel** to cancel and return to the Extensions Configuration screen.

Click **Remove** to remove the created Extensions.

Adding or Changing External Lines

Click **Change** to modify settings for the for the selected Enterprise Gateway in which External Lines (Trunks) are to be added. This opens the following **External Lines Configuration - Change** screen.

Figure 3.13: External Lines
Change

Enter the details on the desired fields for either **Analog (FXO) trunks Configuration** or **PRI Ports Configuration (E1/T1 setup)** or both and click **Apply** to create the Trunks. The following confirmation screen is shown if the External Lines are created successfully.

Figure 3.14: External Lines Change
Successful

Click **Done** to return to the main External Lines Configuration screen.

If you click the **Enterprise Gateway IP** hyperlink of External Lines, then the following screen appears based on your EG type that you have selected.

Figure 3.15: External Lines FXO
Configuration

Figure 3.16: Primary Rate
Interface

Configuring - Software Server

This provides an option to configure software server for EG to store and deliver configuration files for every EG configured in SNM. Also, allows to register EG Software Server and state where and how to communicate with it.

The configuration files are used by the Enterprise Gateways to load their default data at startup. The system administrator can register from a single place to manage all Enterprise gateway configuration files. The Enterprise Gateway SW server is a stand alone server. There may be multiple configuration files on the server. Configuration files are created and placed in the Software Server using the Enterprise Gateways MAC address.

To configure or add software server to EG, do the following:

1. Click **Software Server**. The following screen appears.

Figure 3.17: Software Server

2. Enter the **Server Name** of the IP phone or Enterprise Gateway server.

3. Enter the IP address or Host Name to the IP phone or Enterprise Gateway server.

4. Enter the physical port number of the IP phone or Enterprise Gateway server.

5. Click **Apply**. The following successful screen appears.

Figure 3.18: Software Server
Add
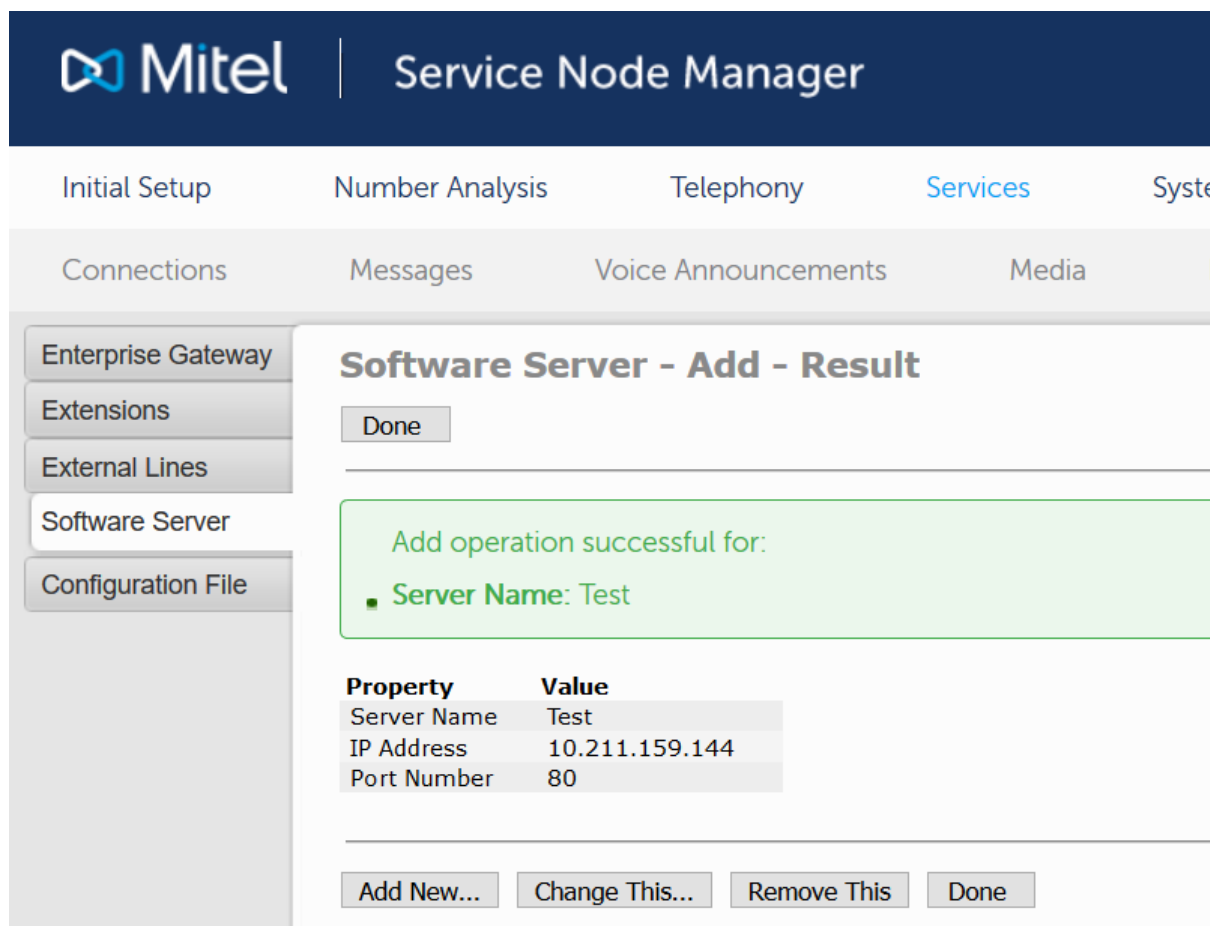
6. Click **Add New** to add **Server Name** and **IP Address**of the EG.

7. Click **Change This** to modify **IP Address** and **Port Number.**

8. Click **Remove This** to delete the added Software Server details.

9. Click **Done** to save the entered details.

10. Click **Cancel** to go back to return to the **Software Server** screen.

Adding or Managing Configuration File

Using this option, the user can manage the Enterprise Gateway configuration files. The configuration files are stored on the Enterprise Gateway SW server (which is a Tomcat web server) and the Enterprise gateway uses the http protocol to read the file. It is possible to do a Backup of the configuration file, and save a copy of the file locally on the Enterprise Gateway SW server.

To add a new Enterprise Gateway configuration file, do the following:

1. Select the required Enterprise Gateway (hyperlink) as shown in the following figure.

Figure 3.19: Configuration
File

2. Click **View Details** to view the added file configuration details.

3. Click the **Change** option. The following screen appears to go to the Configuration - Change screens that will guide you through specifying the property values for the Enterprise Gateway configuration file.

Figure 3.20: Configuration
Change

Hardware

Blocking

If a device needs to be repaired or changed, it has to be blocked before it can be removed.

The blocking function does not terminate ongoing calls but no new calls is permitted for the device or devices that are going to be blocked. When a hardware is deblocked, it will allow new traffic over the device.

Time Information

Internally, in the system, the time is stored in Universal Time Coordinated (UTC) format, that is in seconds and microseconds. UTC time is received from atomic clocks and is very close to Greenwich Mean Time (GMT). In UTC every second has exactly the same length.

The time is formatted into readable UTC or local time, in the output. The time zone information is displayed as part of the formatted time to indicate how it should be read. The time zone is displayed in parenthesis after the date or time. If no time zone information is shown the time is assumed to be in UTC.

Date and time is shown in ISO format which means year-month-day hour:minute:second.microseconds. For example: Universal time, 2007-11-21 14:52:33.670501 (UTC) and Local time, 2007-11-20 20:22:33.670501 (IST).

Media Gateway

Media gateways are used to convert the media from the format available in the PSTN to the format required in the IP network, or from the format in the IP network to the format required in the PSTN.

Hardware Description

Hardware description is used to view the board ID and to manage free text descriptions on equipment positions for analog and digital extensions. You can select to filter the search on server number and/or on board ID. The description may be shown in other tasks in MX-ONE Service Node Manager and MX-ONE Provisioning Manager where there are selection fields for equipment positions for analog and digital extensions.

Board List

The **Board List** task provides a **View** function for board data, where a search can be based on the following data:
* Board ID
* Board position
* Server number

This task provides a **Scan** function for board List, where a search can be based on the following data:
* Media Gateway Individual

Transport Media

To view transport media data.
* View registered transport media, registered connection media, synchronization data, and seized media connections
* Set class and priority for logical links
* Set class and priority for synchronization sources
* Order resynchronization for a media gateway

Equipment Configuration

The number of initiated line individuals in a LIM or in the system can be viewed in SNM. The listed type of extensions is of the type ordinary/primary or own directory number.

Equipment Data

Data regarding equipment positions and board positions in specified LIMs can be viewed in SNM.

Equipment Vacancies

In SNM, it is possible to view the free equipment positions of the specified type in LIM or in the system for extensions, PBX operators, external lines, IP extensions and machine equipment.

Back-Up & Restore

Restoring data is appropriate when there is reason to believe that there is mismatch in the system data. The system data will be restored to the status it had at the last successful backup occasion.

It is possible to perform a backup of the Service Node Manager database as well as exchange data. All data can be restored by using the restore function.

The system will store the three latest backup directories. If more backups are made, the oldest backup directory is deleted. Each backup file is identified by a backup number, a time stamp and the system release version number.

Alteration of exchange data is inhibited during restore and backup.

Batch Operation

In SNM, it is possible to record user actions in real time and to run batches of operations that have been recorded earlier. Batch operations can be used when you want to create several configuration tasks in a batch, for repeated or frequent operations that are time consuming to do manually.

It is also possible to change the order of operations within a batch, change previously recorded operations and upload (import) user action batch files in XML-format from a file system.

Revisions

The Revisions task is used to view version information for the Service Node, Media Gateway software, hardware, firmware and resources as well as version information for Linux, PostgreSQL, Java VM, Apache Tomcat, JBoss and RPM Packages.

Quality of Service Logging

Quality of Service (QoS) information and call information for Voice over IP (VoIP) calls are used to collect data concerning end-to-end delay, jitter, and packet loss for RTP media traffic.

Number Conversion

Number conversion and bearer capability substitution are features that perform conversion of sent and received numbers and of bearer capabilities and tele-services from database tables.

There are two methods for Number Conversion:
- Bulk conversion from an uploaded CSV file
- Initiating Number Conversion

Number conversion can be done per system or at route level. If the parameters **Route** and **Target Destination** are omitted, the number conversion will be made for the whole system. By stating the parameter **Route** the number conversion will be route-dependent. By stating the parameter **Target Destination** the number conversion will be destination-dependent. The route- or destination-dependent number conversion will override number conversion per system.

Initiating Number Conversion

Based on the type of conversion the Graphical User Interface (GUI) displays the appropriate fields. It is also possible to modify the previously initiated conversions.

When printing or viewing the initiated number conversion types, the selection can be based on conversion type and/or entry and/or number type and/or pre or route or target destination. Numbers after conversion are also displayed in the list page. Removal is supported on the list of records displayed on view action. Multiple removals of the records are also supported.

Upload

A CSV file containing the required parameter values for number conversion can be uploaded in the GUI. The CSV file shall contain a list of conversion types, numbers to be converted and other parameters in rows.

The parameter values in the CSV file are separated with a semicolon (;). The following is the order of the parameters: `conversiontype`; `entry`; `numbertype`; `trucate`; `prefix`; `newtype`; `\ continue`; `route`; `targetdest`; `;` `bcap`; `hlc`

The parameters for number conversion vary based up on the conversion type.

The list page displays the successful items, failed items and log date and time. Log data can be removed by clicking the delete (X) icon of the specific row.

Signal Tracing

The purpose of this task is to see track the internal signaling in the system. It is mainly used for fault tracing and identification.

This is to initiate traces in the system. Tracing can be initiated for the following types:
- Unit
- Directory number
- Equipment position
- Board position
- Media gateway.

Logs

Audit Trail

Audit Trail shows information about changes in the MX-ONE Service Node that is made by any user in the system. The log saves information on all operations that changes data, such as adding, changing or removing configuration data. A log file is created every day, even if there are no logged data. If a log file

does not contain any log information, the log file states the text string `No logging information`. Logs older than 90 days will be overwritten.

Events

The event log is a collection of traced actions performed by the user, such as procedure calls for navigation, logins and command executions. It is useful for fault tracing. A log file is created every day, even if there are no logged data. If a log file does not contain any log information, the log file states the text string `No logging information`. Logs older than 90 days will be overwritten.

Security

For information about the Security log, see the Security Log chapter.

MDSH

A dedicated log file that contains its MDSH interaction. The log is added for trouble-shooting purposes. SNM will start a new log file when the current file reaches 10 MB in size, and will retain the 15 most recent files.

The Command Line Interface

The Command Line Interface can be used to execute commands that web based interface of SNM do not cover.

NOTE: Synchronization problems towards external databases may occur when the command line interface is used.

NOTE: Interactive commands are not supported by the command line interface.

The latest 20 commands are stored in the system, and any of them can be selected and executed. It is possible to load an input file, containing several commands instead of entering each command separately.

The results of the operations can be downloaded as a .txt file.

The following types of commands can be entered:

- UNIX-style: Separate executable files in the UNIX™/Linux™ environment outside the shell of the MX-ONE Service Node; mdsh. Some of these commands are standard UNIX tools, like the commands `less` and `emacs`, while other files belong to the MX-ONE Service Node service system software. The parameters of these commands deviate from standard unix commands in one aspect, namely that they cannot be concatenated. Each parameter must be separate.
- Built-in: UNIX/Linux commands that are executed by mdsh as an integrated part of the shell. Examples are the commands `cd` and `threads`.
- MML: Complies with the CCITT MML format familiar to, for example, the ASB 501 04 user. These commands are sent by mdsh to a program (CIOR), which finds the appropriate command handler to execute the command.

  NOTE: No confirmation questions are provided for dangerous commands.

To have access to the Command Line Interface (CLI), the user must be logged in to an account with administrative privileges.

Interfaces and Protocols

The following interfaces and protocols are available for SNM.
- HTTP/HTTPS
- SOAP

For more information about the SOAP interface, see the interface description for *MX-ONE SERVICE NODE MANAGER AND MX-ONE PROVISIONING MANAGER WEB SERVICES, Reference [4]*.

Operation and Maintenance

For information about the user interface and the navigation, see the user guide for *MX-ONE SERVICE NODE MANAGER, Reference [5]*.

For information about specific tasks and parameters, see the online help in SNM GUI.

Security

Service Node Manager can run in HTTP and HTTPS, the system is configured by default in HTTP. However, Mitel recommends that HTTPS with TLS 1.2 is used.

Provisioning Manager and Service Node Manager supports both RSA and ECDSA digital signature algorithm. However, the ECDSA key is not available when a Self-Signed certificate is created.

For information on how to generate a Certificate Signing Request, check the procedure to generate a Certificate Signing Request to be used by Provisioning Manager and Service Node Manager in the document *Installing MX-ONE Provisioning Manager - Installation Instruction*.

Authentication

A valid user account is required for logging on the SNM application. The following types of user accounts can be used for logging on to SNM:
- MX-ONE Provisioning Manager user account
- Linux user account on the SNM server.

For installations using MX-ONE Provisioning Manager (PM), MX-ONE Provisioning Manager user accounts are used for logging on to SNM. For installations not using MX-ONE Provisioning Manager, Linux user accounts on the SNM server are used for logging on to SNM.

For both scenarios, the user account must have the appropriate privileges.

Selecting Authentication Method

The type of user account to use for logging on to SNM is set after installation through command **mxone_maintenance** tool and select **Web server config**.

Choose **Set SNM to authenticate to PM or Linux**.

Note that even if MX-ONE Provisioning Manager (PM) is installed on the same server, the authentication method is not automatically set to PM authentication.

Authentication Using MX-ONE Provisioning Manager

When using MX-ONE Provisioning Manager (PM) user accounts for logging on to SNM, log on requests in SNM are authenticated using the MX-ONE Provisioning Manager user database. If the user is authorized to log on SNM, the log on is executed.

A user's authorities in SNM depends on the privileges assigned to the user in the MX-ONE Provisioning Manager user database. When logging on to SNM using a MX-ONE Provisioning Manager user account, MX-ONE Provisioning Manager provides SNM with data regarding the user's authority to:

- modify user data
- manage configuration data
- manage advanced features
- access the command line interface.

Each task in SNM is associated to one of the above authority levels. To be able to, for example, perform an initial setup of SNM, a user must be authorized to manage configuration data. Note that when using MX-ONE Provisioning Manager user accounts for logging on to SNM, this authority setting is defined in the MX-ONE Provisioning Manager user database.

Authenticating users using the MX-ONE Provisioning Manager user database provides a number of features not available when authenticating users using Linux accounts on the SNM server:

- the user's SNM privileges are defined using PM
- the PM feature for locking users after three incorrect log on trials can be used
- locked out users can unlock their accounts using PM.

NOTE: When clicking a link to a MiVoice MX-ONE, the log-on to the subsystem (MiVoice MX-ONE) is performed automatically. The user is logged on using the user credentials that was used for logging on to Provisioning Manager (not the user credentials that was defined when the MiVoice MX-ONE subsystem was added, these are used only for the communication between Provisioning Manager and the MiVoice MX-ONE).

Authentication Using Linux Accounts on the SNM Server

For installations not using MX-ONE Provisioning Manager or MX-ONE Provisioning Manager authentication, Linux user accounts on the SNM server are used for logging on to SNM. Using this method, a user's privileges in SNM are defined by the authority levels for the user's Linux account.

User privileges in SNM and Linux account authority levels approximately correspond according to the table below:

Table 3.2: Privileges and authority levels

Privilege in SNM	Corresponding Linux authority level in MX-ONE (approximate)
Modify user data	snlev1
Manage extension data	snlev2
Manage configuration data	snlev3
Manage advanced features	snlev6
Command line interface access	snlev7

For information on Linux authority levels in MX-ONE, see the operational directions for *User Account Management*, 66/154 31-ANF 901 14.

Tasks and Privileges in the Web GUI

The table below shows tasks in the SNM Web GUI and the privilege required for performing each task.

Table 3.3: Tasks and privileges in the SNM web GUI (Sheet 1 of 6)

Menu	Task	Privilege in MX-ONE Provisioning Manager
Initial Setup	Walkthroughs	Manage configuration data
	Application ID	Manage configuration data
Number Plan	Number Series	Manage advanced feature
	Service Codes	Manage advanced feature
	External Number Length	Manage advanced feature
	Number Conversion	Manage advanced feature
	Number Conversion Upload	Manage advanced feature
	System Numbers	Manage advanced feature
Number Analysis	Emergency Number	Manage advanced features
Call Diversion	System Call Diversion	Manage configuration data
	Customer Call Diversion	Manage configuration data
Call Discrimination	Group Names	Modify user data
	Permitted Numbers	Modify user data

Table 3.3: Tasks and privileges in the SNM web GUI (Continued) (Sheet 2 of 6)

Menu	Task	Privilege in MX-ONE Provisioning Manager
Extensions	Account Code	Manage extension data/Modify user data
	Common Category	Manage extension data/Manage configuration data
	Common Service Profiles	Manage extension data/Manage configuration data
	Abbreviated Dialing	Manage extension data/Modify user data
	Common Authorization Code	Manage extension data/Modify user data
	Force Mobile Through PBX	Manage extension data
	Delay seizure list	Manage extension data/Modify user data
Operator	Operator Individual	Manage configuration data
	Operator Group	Manage configuration data
	Group Members	Manage configuration data
	Operator Display Messages	Manage configuration data
	Central Operator Number	Manage configuration data
	Common Access Code	Manage configuration data
	Day/Night Mode Operator	Manage configuration data
	Assistant Server Port	Manage configuration data
Call Center	Automatic Call Distribution Group	Manage extension data
	ACD Group Member	Manage extension data
	ACD Parameters	Manage configuration data

Table 3.3: Tasks and privileges in the SNM web GUI (Continued) (Sheet 3 of 6)

Menu	Task	Privilege in MX-ONE Provisioning Manager
Groups	Group Do Not Disturb	Manage extension data/Manage configuration data
	Customer Group	Manage extension data/Manage configuration data
	Hunt Group	Manage extension data/Manage configuration data
	Hunt Group Member	Manage extension data/Modify user data
	Pickup Group	Manage extension data/Modify user data
External Lines	Route	Manage advanced feature
	Destination	Manage advanced feature
	Busy No Answer Rerouting	Manage advanced feature
	Vacant Number Rerouting	Manage advanced feature
	Customer Rerouting	Manage advanced feature
	Public Exchange Number	Manage advanced feature
	Charging	Manage advanced feature
	Mobile Direct Access Dest	Manage advanced feature
System Data	Own Exchange	Manage configuration data
	System Data	Manage configuration data
	Time Supervision	Manage configuration data
IP Phone	Administrator	Manage configuration data
	Security Policy	Manage advanced feature
	Telephony Domain	Manage configuration data
	SIP Domain	Manage configuration data
	SW Server	Manage configuration data
	Configuration File	Manage configuration data
	Unregistration	Manage configuration data
	Media Encryption	Manage configuration data

Table 3.3: Tasks and privileges in the SNM web GUI (Continued) (Sheet 4 of 6)

Menu	Task	Privilege in MX-ONE Provisioning Manager
DECT	System ID	Manage advanced feature
	DECT Board	Manage advanced feature
	Base Station	Manage advanced feature
	DECT SMS Server	Modify user data
	DECT SMS Client	Modify user data
Services	Branch Office	Manage advanced feature
System	Backup and Restore	Manage configuration data
	Batch Operation	Manage configuration data
	Revisions	Modify user data
Information system connection	Information system connection	Manage configuration data
Messages	Message Diversion	Manage configuration data
	Message Waiting Setup	Manage configuration data
	Message Waiting	Manage configuration data

Table 3.3: Tasks and privileges in the SNM web GUI (Continued) (Sheet 5 of 6)

Menu	Task	Privilege in MX-ONE Provisioning Manager
Voice Announcements	Voice Messages	Manage extension data/Manage configuration data
	Announcement Setup	Manage extension data/Manage configuration data
	Operator Group	Manage configuration data/Manage configuration data
	Operator Individual	Manage extension data/Manage configuration data
	Announcement Group Setup	Manage extension data/Manage configuration data
	Announcement Group Member	Manage extension data/Manage configuration data
	Hunt Group	Manage extension data/Manage configuration data
	Extension Announcement	Manage extension data/Manage configuration data
	Vocal Guidance	Manage extension data/Manage configuration data
	Diversion	Manage extension data/Manage configuration data
Routing Server	Routing Server	Manage advanced feature
	Routing Satellite	Manage advanced feature
	Time Supervision	Manage advanced feature
Hardware	Blocking	Manage advanced feature
	Media Gateway	Manage advanced feature
	Time Information	Manage configuration data
	Equipment configuration	Manage configuration data
	Equipment data	Manage configuration data
	Equipment vacancies	Manage configuration data
	Hardware Description	Manage configuration data
	Board list	Manage configuration data
	Transport Media	Manage configuration data

Table 3.3: Tasks and privileges in the SNM web GUI (Continued) (Sheet 6 of 6)

Menu	Task	Privilege in MX-ONE Provisioning Manager
Tools	Command Line	Command line interface
	Quality of Service	Manage configuration data
	Signal Tracing	Manage configuration data
Logs	Audit Trail	Manage advanced feature
	Events	Manage advanced feature
	Security	Manage advanced feature
	MDSH (command shell)	Manage advanced feature

Tasks and Privileges in the SNM Web Service Interface

The table below shows tasks in the SNM web service interface and the privilege required for performing each task.

Table 3.4: Tasks and privileges in the SNM web service interface (Sheet 1 of 2)

Task	Privilege in MX-ONE Provisioning Manager
IPExtension	Modify user data
CommonServiceProfile	Manage configuration data
CommonCAT	Manage configuration data
MobileExtension	Modify user data
ExtInitData	Modify user data
PersonalNumber	Modify user data
AccountCode	Modify user data
AnalogueExtension	Modify user data
PickupGroup	Manage configuration data
AuthorizationCode	Modify user data
NumberSeries	Manage configuration data
CommonAbbNum	Modify user data
GetLatestResponse	Modify user data
HuntGroup	Manage configuration data
HuntGroupMember	Modify user data
ExtensionTexts	Modify user data

Table 3.4: Tasks and privileges in the SNM web service interface (Continued) (Sheet 2 of 2)

Task	Privilege in MX-ONE Provisioning Manager
GroupBelongings	Modify user data
TaskType	Modify user data
Backup	Manage configuration data
VirtualExtension	Modify user data
IPFunctionKey	Modify user data
ParallelRinging	Modify user data
DigitalExtension	Modify user data
DTSFunctionKey	Modify user data
Fax	Modify user data
AdditionalDIRNumber	Modify user data
MultipleRepresentation	Modify user data

Profiles and Privileges

Profiles and privileges in SNM correspond according to the table below:

Table 3.5: Profiles and privileges in SNM

Profile	Privileges in MX-ONE Provisioning Manager
Domain Administrator	Modify user data Manage configuration data
System Administrator	Modify user data Manage configuration data
User Administrator	Modify user data
SystemSetupAdmin	Modify user data Manage configuration data Manage advanced features Command line interface
No privileges	-

Passwords

Passwords are stored in hashed format. The hash function takes the password as input and transforms it into a fixed length string as output. The output is called the hash value, and it is concise representation of the password.

Hardening

Hardening is the process of securing a system, for example, to protect the system against attackers. The following steps are taken when hardening a system:

1. Minimizing installed software.
2. Patching the system.
3. Securing file system permissions and S*ID binaries.
4. Improving login and user security.
5. Setting some physical and boot security controls.
6. Securing the daemons via network access controls.
7. Increasing logging and audit information.
8. Configuring supplied security software (IDS, firewalls)

Linux is handling the hardening.

HTTPS

In SNM both HTTP and HTTPS are supported. For higher security, it is recommended to use a commercial digital certificate issued by a commercial Certification Authority.

Security Log

In the Logs task, there is a security log that shows information about successful and unsuccessful login attempts. A log file is created every day, even if there is no logged data. If a log file does not contain any log information, the log file states the text string "No logging information".

The log files will be overwritten after 90 days.