

MiVoice MX-ONE

Provisioning Manager - Description

Release 7.4 SP1

April 13, 2022



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>.

®, ™ Trademark of Mitel Networks Corporation
© Copyright 2022, Mitel Networks Corporation
All rights reserved

Contents

Chapter: 1	Introduction	1
	Scope	1
	Target Group	1
	Glossary	1
Chapter: 2	Overview	2
	System Requirements	4
	Deployment Scenarios	4
Chapter: 3	User and Extension Data	5
	Example on Data Flow Between MX-ONE PM and Its Subsystem	5
	Initiating the User Task	5
	Creating User and Extension Data	6
Chapter: 4	User Types	7
Chapter: 5	Key Features	9
	Tenant and Feature Configuration	9
	User Provisioning	9
	User Services	9
	Access Restriction	10
	Supported Phone Types	10
	Data Synchronization - MX-ONE PM and Its Subsystems	11
	Import and Export	11
	Reset Password	11
	Self-Provisioning for End-Users	11
	Efficiency Enhancing Features	11
	Third-Party Product Integration	12
Chapter: 6	Performance	13

Chapter: 7	Interfaces and Protocols	14
	Operation and Maintenance14
	Security14
	Hardening14
	Hardening14
	HTTPS14
	TLS/SSL15
	Authentication15
	Passwords15
	Authentication Server for MX-ONE SNM15
	Security Logs16
	Audit Trail Logs16
	Event Trail Log16

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):

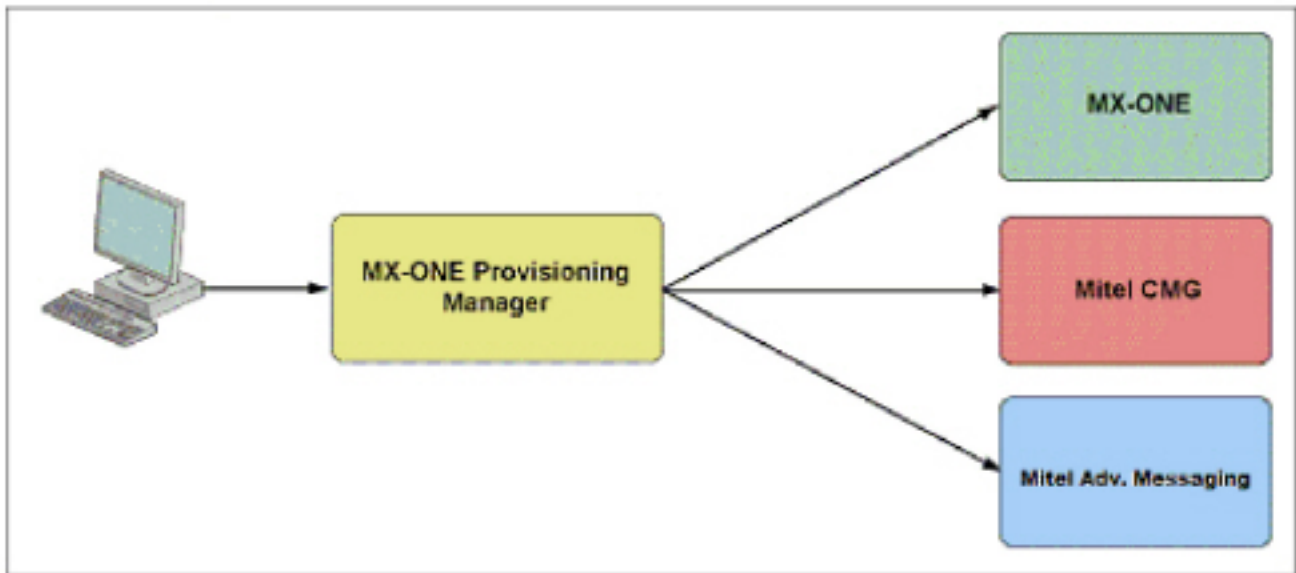
- Managing administrator accounts
- Adding subsystems, for example, MX-ONE Service Nodes and CMG servers.
- Importing and exporting user and extension data
- Performing backup of user and extension data
- Unlocking locked users.

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:

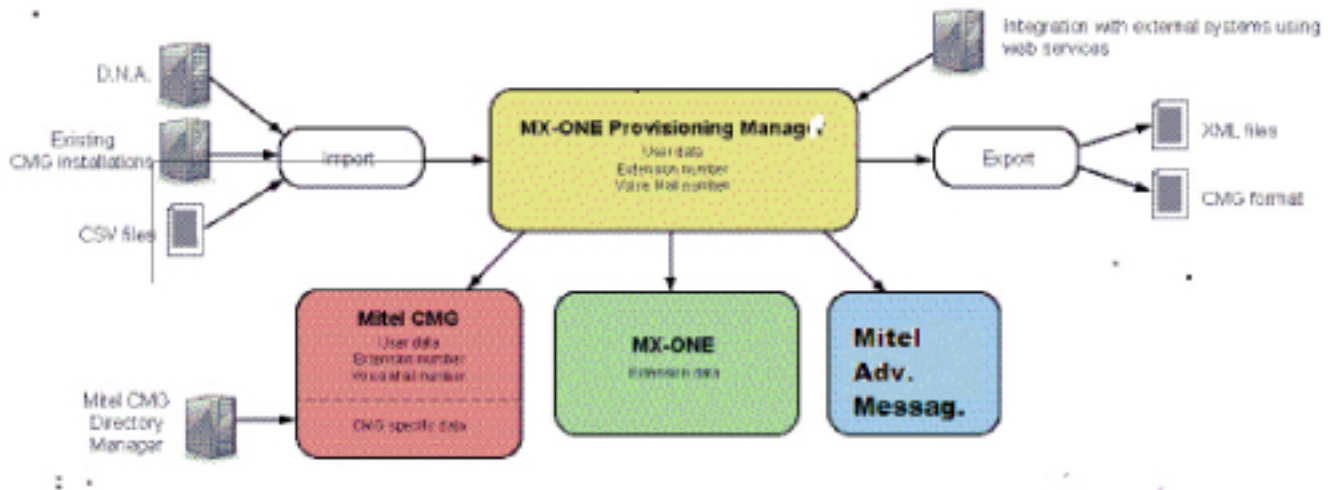
- Stand alone
- On MX-ONE Service Node (in coexistence with MX-ONE Service Node Manager if installed on the primary MX-ONE Service Node)

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 3.1: 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)

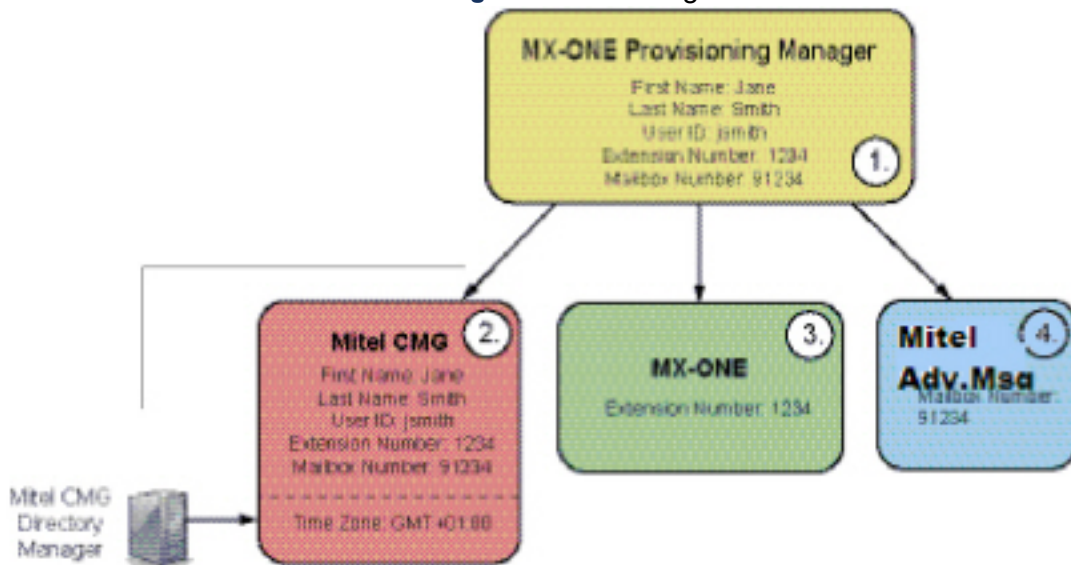
- Available common service profiles (provided by MX-ONE)
- Available class of service profiles for Voice Mail mailboxes (provided by Mitel MiCollab Advanced Messaging).

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 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 3.2: 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 also change the own settings.

Users fall under Feature Based category

- **Service Provider:** Service Provider can manage services, can create users and promote them as Resellers only.
- **Reseller:** Reseller can manage user, service data, subsystem services data (only generic extensions), Tenant configuration data, Feature level configuration data, available extensions, mailboxes and administrators.

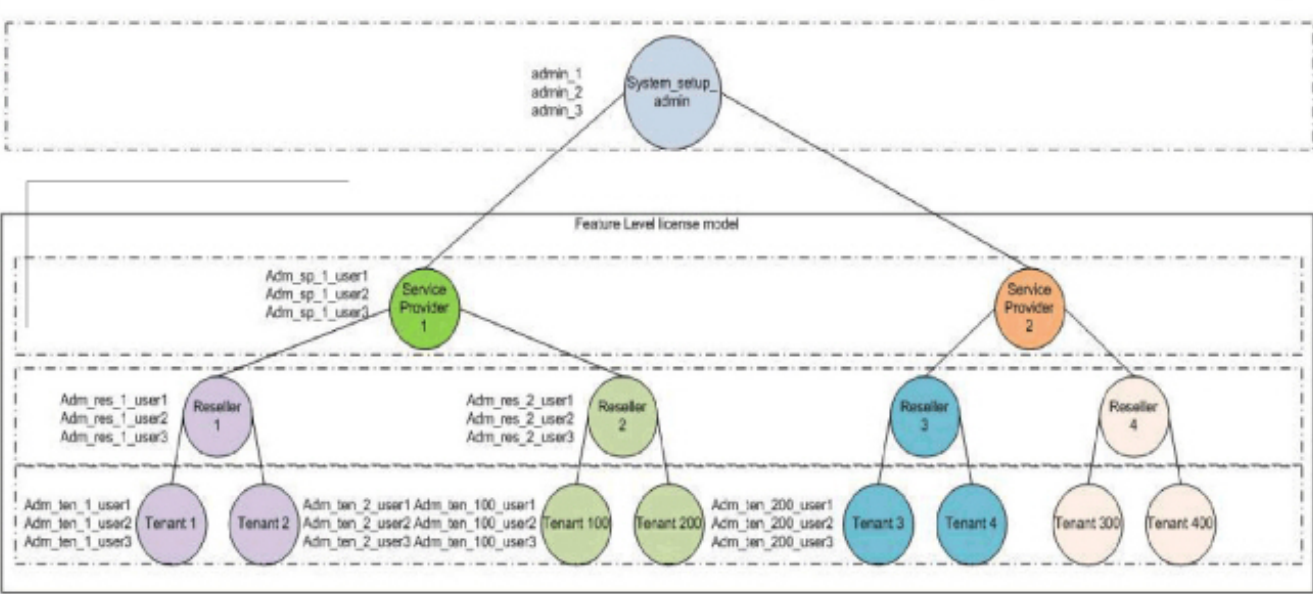
Reseller can create users and promote them as Tenant Administrators for specific customer.

- **Tenant Administrator:** Tenant Administrator can manage user data, service data, Tenant configuration data, Manage Available extensions and Mailbox.

Tenant Administrator can create users and will be Tenant viewers of specific customer.

- **Tenant Viewer:** Tenant Viewer can view his own settings and access to Tenant Viewer Self Service.

Figure 4.1: User hierarchy



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

Data Synchronization - MX-ONE PM and Its Subsystems

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

Changing user or extension data in CMG or MX-ONE will cause unsynchronized data in the MX-ONE databases.

Unsynchronized data in PM and its subsystem can also occur if PM is restored using the **Backup & Restore** task and the subsystems are not restored at the same time.

Unsynchronized data in PM and its subsystems can be identified using the **Compare with Subsystem** task in PM.

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, Swedish, and Portuguese (Brazil). 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.

