# MiVoice MX-ONE MX-ONE Management Applications Installation and Configuration Release 7.2 February 19, 2020



#### Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks**<sup>™</sup> **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: <u>http://www.mitel.com/trademarks</u>.

> ®,™ Trademark of Mitel Networks Corporation
>  © Copyright 2020, Mitel Networks Corporation All rights reserved

# Contents

Chapter: 1	MX-ONE Provisioning Manager, End User Portal Description 1
	Introduction
	New End User Portal GUI
	New Sub-Menus
	Menu Description
	End User Information Menu
	Services
	User Information11
	Personal Number11
	General Menu
	Settings
	Status
	License
	PIN Reset
Chapter: 2	Installing MX-ONE Provisioning Manager, Installation Instruction 16
	Introduction
	Installation Scenarios
	Installation Using mxone_maintenance Script
	Prerequisites
	StandAlone Installation
	Coexistence Installations on Server 1
	Considerations
	Preparations
	Obtaining a Digital Certificate
	Installation
	Accessing MX-ONE Provisioning Manager
	MX-ONE Provisioning Manager Start and Stop
	Upgrade
	Migrating 5.x or 6.x Manager Provisioning Data to 7.x PM
	Migrating from D.N.A. to MX-ONE Provisioning Manager

	Migrating from D.N.A. to MX-ONE Provisioning Manager20
	Exporting User and Department Data in D.N.A.
	Backing Up Data in MX-ONE Provisioning Manager
	Importing D.N.A. Data in MX-ONE Provisioning Manager 21
	Migrating from D.N.A. to MX-ONE PM in Environments21
	Exporting User and Department Data from D.N.A
	Importing D.N.A. Data to CMG
	Downloading and Installing the CMG Export Registry File22
	Exporting Data from CMG
	Backing Up Data in MX-ONE Provisioning Manager 24
	Adding CMG as a Subsystem in MX-ONE Provisioning Manager 25
	Creating Locations for CMG Customer Groups in MX-ONE PM 25
	Importing CMG Data in MX-ONE Provisioning Manager25
	Migrating to MX-ONE PM from Environments
	Backing Up Data in CMG
	Important Post-Migration Considerations
	Post Installation
	Uninstallation
	Log Files
	Fault Recovery
	Increasing Heap Memory Size in Jboss Configuration File
Chapter: 3	MX-ONE Provisioning Manager Deployment
-	Introduction
	MX-ONE PM Deployment Alternatives
	General
	MX-ONE SNM and PM on the same SN
	MX-ONE SNM and PM on different Service Nodes
	MX-ONE PM on Separate Server
Chapter: 4	MX-ONE Provisioning Manager, User Instructions
	Introduction
	Scope
	Target Group
	Internet Browser Settings
	Target Group
	Internet Browser Settings
	MX-ONE Provisioning Manager Overview
	System Requirements
	Key Features of MX-ONE Provisioning Manager
	Preferred Language
	Getting Started
	Manual Workflow When Getting Started
	Integrating With MITEL CMG
	Integration With MiCollab Advanced Messaging

Integration With MS Active Directory	40
Integration With SIP-DECT OMM	40
Integration With MiCollab Server	41
Using MX-ONE Provisioning Manager	41
Logging In and Logging Out	41
Navigating in MX-ONE Provisioning Manager	41
Icons, Symbols and other Graphical Elements	42
Using the Help	45
Basic or Advanced Settings	45
Enabling the Automatic Logout Indicator	45
Actions	45
Self Services	46
Adding Data	46
Viewing Data	46
Filtering Data in List Views	47
Sorting Listviews	47
Comparing Data	47
Searching for Users	48
Changing Data	48
Removing Data	
Printing Data	
Swapping Equipment Positions	
Handling Templates	
Creating a Template for a Configuration Item	
Uploading or Downloading a Template	
Using a Template to Create a Configuration Item	
Using a Multistep Button	
Using Shortcuts	52
Using Backup & Restore	
Subsystem Backup	52
Using Compare with Subsystem	53
Importing Data to MX-ONE Provisioning Manager	
Importing from D.N.A. and CMG	54
Importing from CSV	
Exporting Data from MX-ONE Provisioning Manager	
Exporting Data for CMG	
Exporting General Data	
Exporting Call Accounting Data	
Tenant and Feature Configuration	
Create a Service Provider	57
Create a Reseller	
Create a Tenant Administrator	61
Create a Tenant	
Setup a New MX-ONE PM to Monitor Different Sites	
CPE Mode Setup	
End User Profile Settings to Monitor Group Data	

	System and Error Messages
	Logs
	Changing the Log Level
	Post-Installation Configuration Tool
	MX-ONE Provisioning Manager Interface with WebSEAL
	General
	Requirements
	WebSEAL
	Connection to the Provisioning Manager
	PM webserver_configuration for login via WebSEAL
	Registration via WebSEAL
Chapter: 5	MX-ONE Provisioning Manager integration with MS Active Directory 80
	Introduction
	Scope
	Target Groups
	Functionality
	Overview
	Active Directory Connection Setup
	AD – PM Field Mapping
	PM Active Directory Task
	Extension Handling Details
	Name Handling
	Execution Flow
	Limitations
	Additional Info
Chapter: 6	AD Authentication, Description
	Introduction
	Description of AD Authentication
	Prerequisites
	Supported AD versions
	Security
	Secure Socket Layer (SSL)
	Certificates
	Server Certificate
	Root Certificate
	Generating Certificate Signing Request (CSR) and Creating Keystore 94
	Creating Certificate by Signing Request File
	Creating the Key Store by using Signed Certificate
	Importing Certificates for PM and SNM
	Users
	Configuration
	Configure Web Protocol
	Configuring Web from HTTP to HTTPS with Self-Signed Certificate 103

	Configuring from HTTP to HTTPS with Uploaded Server Certificate 104
	Turning SSL off and back on again
	Configure SNM authentication method
	Certificate Management for AD Authentication
	Root Certificate or Signed Server Certificate
	Alternative to Root Certificates
	Search and Delete root certificates
	Configure AD Authentication
	AD Authentication Maintenance
	Modifying AD Authentication Configuration
	Turning AD Authentication Off
	Turning AD Authentication Back on
	AD Authentication Scenarios
	Scenario 1: PM Login
	Scenario 2: SNM Login
	Scenario 3: SNM Login over HTTP
	Scenario 4: PM Login + use case 'Add Extension'
	Scenario 5: In PM "click on subsystem"
	Fault Cases / Exceptions
Chapter: 7	Configuration of AD LDS, User Guide
	Introduction
	General Introduction to AD LDS in MiVoice MX-ONE 6.x 115
	About this guide
	Requirements
	Steps for Getting Started with AD LDS
	Prerequisite
	Enabling AD LDS in Windows Server
	Creating AD LDS Instance
	Creating the Custom LDF File to suit for AD LDS Setup 1.1.134
	Restarting the AD LDS Instance
	Creating an Admin User in AD LDS
	Checking User Authentication
	Adding Attributes to UserProxyFull Class
	Editing Object (UserProxyFull) Class as User Object Class 154
	Modifying MS-AdamSyncConf File
	Synchronizing Users from Active Directory to AD LDS Instance 159
	Checking Synchronized Users in AD LDS
	Enabling LDAPS (SSL) for AD LDS in Window Server
	Using AD LDS as a User Repository in PM Application 167
	Enabling SSL for PM Application
	Enabling AD Authentication in PM Located Server
	Uninstalling AD LDS Instance and AD LDS Roles from Server 171
Chapter: 8	Quick Reference Instructions

Create a User with IP Extension and Optional Mailbox	173
Log in to PM	173
Create a user	173
Add an IP extension	173
Add a new IP extension	174
Assign an Existing Extension	174
Add a mailbox	
Add a new Mailbox	
Import a CSV file with user information using PM	
Log in to PM	
Preparation before the import of the CSV file	
Log in to CMG	
Enter Company structure in CMG	
Add a New Unit in CMG	
Import the CSV file in PM	
If something went wrong	
Check list	
Check the Organization Structure in PM	
Check the Structure in CMG	
Search for a User without a Unit in CMG	
Add a User to a Unit in CMG	
Add a new unit in CMG after a CSV File Import	
Edit CSV file	
Create an Extra Directory Number (EDN)	
Create an extra IP Extension	
View an Extension	
Add an Extra Directory Number (EDN)	
Set Group Hunting	
Set Group Hunting	
Add Group Hunting Information	
Select Group Hunting Members	
Set Multiple Name Selection (MNS)	
View Extension	
Set Multiple Name Selection	
Save the Settings	
Set Personal Number (PN)	
Log in to PM	
View User	
Set Personal Number (PN)	
Set Personal Number (PN)	
Set profile 1 - In Office         Set profile 1 - In Office	
Enter Number List Information	192

	Set profile 2 – On a business trip
	Enter Number List Information
	Save the Settings
	Set Boss-secretary
	Login to PM
	View the Extension of the Boss
	Set Personal Number Lists
	Set Profile 1 for the Boss
	Set Profile 2 for the Secretary
	Select Key with Boss-secretary Function
	Save the Settings
	Set Telephone Name Selection (TNS)
	Log in to PM
	View Extension
	Set Telephone Name Selection Information
	Save the Settings
	Delete a User
	Log in to PM
	Delete a User
	Take a Backup of PM/SNM
	Log in to PM
	Take a backup of MP
	Take a Backup SNM
Chapter: 9	Service Node Manager User Instructions
	Introduction
	Scope
	System Requirements
	Prerequisites
	MX-ONE Service Node Manager Overview
	Configuration Areas and Tasks in MX-ONE Service Node Manager 193
	Using MX-ONE Service Node Manager
	Logging in and Logging Out
	Navigating in MX-ONE Service Node Manager
	Enabling the Automatic Logout Indicator
	Actions
	System and Error Messages
	Logs

# **MX-ONE Provisioning Manager, End User** Portal Description

# Introduction

Provisioning Manager is a MiVoice MX-ONE tool, which is used to provision users. This has an end user portal, which is used for self-management of user configurations, such as display name, add TNS keys, change Authorization Code, define and activate Personal Number List, and so on.

From Provisioning Manager 6.2 SP2 a new Graphical User Interface (GUI) is introduced. This is developed to be compatible with accessibility requirements according to the Web Content Accessibility Guidelines (WCAG) 2.0.

"Web Content Accessibility Guidelines (WCAG) 2.0 covers a wide range of recommendations for making Web content more accessible. Following these guidelines will make content accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photo sensitivity and combinations of these. Following these guidelines will also often make your Web content more usable to users in general."

The main changes in the End User Portal are:

- Accessibility work to support WCAG 2.0.
- Function flow review and correction (e.g. tab function in the keyboard).
- Re-work of the functions as well as the GUI.
- More sub-items created in order to make the GUI as clean as possible.
- The pages are now simplified and they present the essential end user information.
- Functions that are not required daily are now under General tab.
- The new implementation is validated by an independent third party company as compliant according the relevant WCAG 2.0 guidelines.

# **New End User Portal GUI**

The new end user portal GUI presents a new look and feel, some colors are changed to keep compatible with the color contrast required by the WCAG 2.0.

For example, the apply button with dark blue as background and white as foreground has a contrast ratio of 12,7:1.

#### Figure 1.1: End User Portal Page

	ig Manager
End User Information Gene	eral
End User Information > Pe	Ittings
	ense VReset
? Extension Numbers:	1500
? Available Profiles:	Profile1
Colour Contrast Analyser	gure 1.2: Color Contrast Result
Options Image Help Foreground	Background
Colour select Hex.	FF #15325F
Text       Foregroit         ✓       Pass (AA)         ✓       Pass (AAA)         ✓       Pass (AAA)         Large text       Text past Text past Text past Large text         ✓       Pass (AAA)         ✓       Pass (AAA)	und:#FFFFF und:#15325F strast ratio is: 12,7:1 ssed at Level AA ssed at Level AA ext passed at Level AA ext passed at Level AA
Show contrast result for colour blindr	Copy results

The menu is also modified and present different colors of the items depending if it is in focus, hovered over or if the drop-down list is shown.

The menu and its items are modified and presented in different colors when it is in focus, hovered over or any drop-down list is shown/selected.

The table below shows different types colors used in the Menu of the pages.

Image	Page Area	Background Color	Foreground Color
End User Information	Menu	#FFFFFF	#404141
End User Information	Menu (hover)	#FFFFF	#BB1122

	Menu (focus)	#FFFFF	#15325F
End User Information			

The used icons is implemented by a PNG (Portable Network Graphics) image and now is being implemented by a SVG (Scalable Vector Graphics) image, which means that image in the computer screen can be increased in the browser without distortion.

The below shows the page with 240% of zoom.

Figure 1.3: Zoom with 240%			
End Us	er Information		
General			
Enc	User Information > Servi	ces	
Ext	Extension - Change - 700004		
?	Extension Number:	700004	
?	Extension Type:	MultiTerminal	
?	Customer:	None	

# **New Sub-Menus**

Now the end user page has two menus, each of them with 3 sub-items.

The menus are divided in two parts to separate between day-to-day tasks that are commonly accessed and managed by the user themselves (End User Information) versus tasks that are more informational and rarely changed by the user (General).

Figure 1.4: Menu End Oser Information
Mitel Provisioning Manager
End User Information General
Services > Services
User Information
Personal Number
Sub-items

## Figure 1.4: Menu End User Information

#### Figure 1.5: Menu General

Mitel Prov	isioning Manager
End User Information	<u>General</u>
General > PIN Reset	Settings
	License PIN Reset

# **Menu Description**

The End User portal has two menus:

- The End User Information menu, which presents the tasks that are typically managed by the end-user.
- The General menu, that provides general information about the extension.

The End User Information menu contains the following 3 sub-items:

Services

The extension/extensions call manager feature or services belonging to that user are shown in this task.

User Information

User information such as first name, last name, and change password are shown in this task.

 Personal Number (Activation/Deactivation) Information regarding the configured Personal Number list are shown in this task.

The General menu contains the following 3 sub-items:

Settings

Additional information regarding the extension is shown in this task, for example the MiVoice MX-ONE that the extension belongs to and other features that are setup by the admin, which are not so relevant to the end user, but are required in some cases when the user needs support for his phone configuration.

Status

The extension status is shown in this task (Line, Diversion and Traffic status). The status feature varies according to the type of extension.

Licenses

The licenses used by the extension/extensions are shown in this task.

Pin Reset

The Pin Reset is used to update the pin number for extension and mailbox.

# End User Information Menu

The End User Information menu is composed of tasks that are most often managed by end users. The end-user will be able to access the features they would be most likely to modify on a day to day basis. Most of the relevant end-user features are grouped under the Services subtask, which starts with a simplified view mode page.

To make changes in the Services subtask, do the following:

- 1. Click Change This button at the bottom to bring up a new page that offers the possibility to modify one or several options on the page.
- 2. Click on the relevant Change button associated with that option to open up a dialog box and do the required changes before moving to next step.
- 3. Click on Apply to ensure the changes are saved before going to the next task. The following sections will go through each of the sub-tasks and associated menus for each feature.

#### Services

The Service task is presented below showing the default page when a user login to the end user portal. A list of extensions is also presented if the user has more than one extension (in the example below the user has two extensions). The user can switch between extensions by clicking the view followed by the extension number (View 700001).

#### Figure 1.6: Extension Service Page

Mitel Provisionin	g Manager					Logged in as : dda	_test	About	Logo
End User Information Gene	eral								
End User Information > Services									
Extensions View View700001									
Property	Value								
Extension Type	Multi-Terminal								
Extension Number	700004								
Customer	None								
Common Service Profile	0 - CSPZero (None)								
Phone Language	Default								
Backup Answering Position Number	799999								
Maximum Terminals	4								
First Name	DDA								
Last Name	Test								
Manual IP Terminal									
Maximum Manual IP Terminals	4								
Group Setup									
Call Pickup Group	GP1								
Group Do Not Disturb	GDBD								
Personal Number List									
List Number , List Name , Status	1, VM1, Set								
List Number , List Name , Status	2 , Secretary , Active								
Change This									
D17 Mitel Networks Corporation									

## Change Extension

To make changes to the extension, the user needs to click on the Change This button.

The user can change the following options:

- Phone Language
- Authorization Code
- Personal List
- Phone type
- Phone panel
- Function Keys
- Hunt Group Number
- Pickup Group Number
- Group Do Not Disturb

## Figure 1.7: Extension Change Page

Mitel Provision	ing Manager	Logged in as : dda_test	About	Logout
End User Information Ge	eneral			
End User Information > Servio	ces			
Extension - Change - 700001	700001			
? Extension Type:	IP			
? Customer:	None			
? Common Service Profile:	0 - CSPZero			
? Phone Language:	Português do Brasil			
? Allow Security Exception:	YES			
? Boss/Secretary:	None			
? First Name:	DDA			
? Last Name:	Test			
? Change Authorization Code:	Change			
? Personal Number List :	Change			
Phone Setup				
? Phone Type	Mitel 6869i			
? Panel Type	M680 - 3 Panels			
? Function Keys:	Change			
Group Setup				
? Hunt Group Number	799999			
	799998			
	799997			
	799996			
? Call Pickup Group:	12			
? Group Do Not Disturb:	GDND3			
Advanced				
Apply Cancel				
© 2017 Mitel Networks Corporation				

### Personal Number List

The user can add/change/delete the extension Personal Number List as part of the extension change. The personal number page is shown below.

	J				
치 Mitel 🛛	Provisioning Man	ager	Logged i	in as : dda_test About	Logo
End User Informatic	on General				
End User Information	> Services				
Personal Number Li	ist				
List Name	List Number	Status	Delay Seizure List		
List1 -VM	1	ON	Not Assigned	Q / X	
Profile2	2	Not Set	Not Assigned	Q /	
Profile3	3	Not Set	Not Assigned	Q /	
Profile4	4	Not Set	Not Assigned	Q /	
Profile5	5	Not Set	Not Assigned	Q 🖌	
2017 Mitel Networks Corpo	oration				

#### Figure 1.8: Change Personal Number List

# Function Keys

The end user can change the setup of TNS keys.

The function keys pages are shown below.

End User Information       General         End User Information       > services         Function Reps:       messeds - 3.4600         Upper general messeds - 3.4600       Image:		Figure 1.9: Cl			About I	0.000
		ovisioning Manager	Log	<del>geu in as .</del> uua_test	About	Jogot
<complex-block></complex-block>	End User Information	General				
	End User Information >	Services				
Image: Second		3-M680				
New Position     Key Label     Function     Digit       1     Oversion       2     TNS     1234       3     1234     TNS     1234       4     TNS     1234       5     TNS     1234       7     TNS     1234       8     TNS     1234       9     TNS     1234       10     TNS     1234       11     TNS     1234       12     TNS     1234       13     TNS     1234       14     TNS     1234       15     TNS     TNS       16     TNS     TNS       17     TNS     TNS       18     TNS     TNS       19     TNS     TNS       10     TNS     TNS       11     TNS     TNS       12     TNS     TNS       13     TNS     TNS       14     TNS     TNS       15     TNS     TNS       16     TNS     TNS       17     TNS     TNS       18     TNS     TNS       19     TNS     TNS       19     TNS     TNS       19     TNS						
1       Diversion         2       3       1234       TNS       1234         4		Panel 2 Panel 3				
1       Diversion         2       1234       TNS       1234         4	Key Position	Key Label	Function	Digit		
3       1234       TNS       1234         4			Diversion			
4         5         6       Test2       TNS       12345         7         8         9						
5       TNS       12345         7		1234	TNS	1234		
6       Test2       TNS       12345         7						
7         8         9         10         11         12         13         14         15         16         17         18         19         20         21         22		Tort?	TNC	12745		
8         9         10         11         12         13         14         15         16         17         18         19         20         21         22		TESTE	INS	12343		
9         10         11         12         13         14         15         16         17         18         19         20         21         22						
11         12         13         14         15         16         17         18         19         20         21         22						
12         13         14         15         16         17         18         19         20         21         22	10					
13         14         15         16         17         18         19         20         21         22	11					
14         15         16         17         18         19         20         21         22	12					
15         16         17         18         19         20         21         22						
16         17         18         19         20         21         22						
17         18         19         20         21         22						
18 19 20 21 22						
19 20 21 22						
20 21 22						
21 22						
22						
2017 Mitel Naturader Corporation						
2017 Mitel Nativerte Corporation						
	2017 Mitel Networks Corporatior					

Figure 1.9: Change Phone Keys

The user can do the key selection in two places.

Function Keys			
Phone type: Mit	tel6869i-3-M680		
? Key Position:	7		
0			
? Key Label:			
? Function:	TNS		
? Digit:			
Apply Canc	el		
	Diversion	 	
	1234 Test2	 	
	<ul> <li>&gt;</li> </ul>	 	
	1 2 <sup>AC</sup> 3 <sup>HP</sup>	 	
8	4 dell 5_m 6 Hino		
	0 [2 7 N(1) [3 TW ]9WM [1		
	7 10 0 10 0 10		

### Figure 1.10: Change Phone Keys (clicking the phone picture)

Select the required key on the phone screen displayed; or,

Top Softkeys

Select the required key from the keys list and the task is presented below the row.

Figure 1.11: Change Phone Keys (clicking the key list)

Softkeys						
ain Phone	Panel 1 Pane	l 2 Panel 3				
Key Pos	ition		Key Label	Function	Digit	
1	siton		Key Laber	Diversion	Digit	
2			hello	TNS	123456	
3						
4						
5						
6						
7						
	? Key Position:	7				
	? Key Label:					
	? Function:	TNS				
1	? Digit:					
	Apply Cance					
0						
8						
10						
10						
12						
13						
14						
40						

### **User Information**

In the User information task, the user can change the following information:

- First name •
- Last name •
- Password .
- Alternate First Name
- Alternate Last Name •
- Keywords •

Select the end user portal language from the ones available in Provisioning Manager End User Portal

The available languages are:

- English •
- German .
- Polish •
- French •
- Russian •
- Spanish •
- Dutch •

The User Information task is presented below.

Figure 1.12: User Information Page										
Mitel   Provisionin	ng Manager			Logged in as : dda_1	est About	Logout				
End User Information Ger	neral									
End User Information > User In	formation									
User Information ? First Name : ? User Id:	DDA dda test	?	Last Name:	Test						
Oster III.     Current Password:     New Password:     Department(s):	Enterprise_system: somewhere	?	Confirm New Password:							
? Email Address:	dda_test@domain.com	?	SMS:							
? Alternate First Names:	Ze_test	?	Alternate Last Names:	12345678						
? Keywords:	DDA									
? Provisioning Manager Language:	English									
Apply										
© 2017 Mitel Networks Corporation										

#### **Personal Number**

If the user has personal number defined for his/her extension/extensions, they can select the active profile in the personal number task. When any one of the profile is selected, the current one is deactivated.

#### Figure 1.13: Personal Number Page

Mitel Provisioning	Manager	Logged in as : dda_test	About	Logout
End User Information Gener	al			
End User Information > Personal I	Number			
Personal Number  Personal Numbers:  Available Profiles:  Apply	700004 Secretary None VM1			
I	Secretary			

## **General Menu**

The General Menu is where system wide functions related to the extension/extensions are presented.

If the user has more than one extension, all extensions are shown in a sequence and the user is able to switch between them by clicking in the View + number of the extension (for example, View 7000001).

#### **Settings**

In the Settings, some additional information regarding the extension is presented.

Figure 1.14: Settings Page

Mitel Provisioning Manager	Logged in as : dda_test About Logout
End User Information General	
General > Settings	
Settings View 700001	
Property	Value
MiVoice MX-ONE	44
Extension Type	Multi-Terminal
Extension Number	700004
Allow Security Exception	Yes
Boss/Secretary	None
Free on Second Line	Yes, but can be changed via terminal menu
Include in Dial by Name Database	No
Name Presentation Order	Second name is presented
Restrict Presentation	No

© 2017 Mitel Networks Corporation

### Status

In the Status task, the extension's current status is shown.

	Figure 1.15: Status Page									
🛤 Mitel 🕴 P	rovisioning Manager	Logged in as : dda_test	About	Logout						
End User Information	General									
General > Status										
Status Information View View 700001 Property		Value								
Extension Number		700004								
Line Status		Terminal not assigned								
Diversion Status		Personal number								
Traffic State		No information								

© 2017 Mitel Networks Corporation		
w 2017 Pillet Networks Corporation		

#### License

In the License task, the extension license is shown.

Figure 1.16: License Page

DI MITEL Provisioning Manager	Logged in as : dda_test Abou	it Logout		
End User Information General				
General > License				
License Information <u>Miew</u> <u>View 700001</u>				
Property	Value			
Extension Number	700004			
Allow EDN	No	No		
BluStar Client Model	None			
Allow Video Functionality	No			
Enable MMC Functionality	No			
Allow Third Party SIP Client	No			



### **PIN Reset**

The end user can change the authorization code for an extension. Enter valid Old Authorization Code to update it with a new authorization code for the selected extension.

Use Forgot PIN links to reset the extension and Mailbox PIN numbers.

Note: These links appear only if Mail server is configured in Provisioning Manager and email ID is assigned to the end user.

If no extensions (with authorization codes) and Mailboxes are assigned to the user, a pop up message gets displayed stating that "No PIN numbers assigned to extensions/ mailbox available for the user".

Figure 1.17: PIN Reset			
Mitel Provisioning Manager			
End User Information G	eneral		
General > PIN Reset			
<ul> <li>Change Authorization Code</li> <li>Select Extension:</li> <li>Old Authorization Code:</li> <li>New Authorization Code:</li> <li>Confirm Authorization Code:</li> </ul>	5667,TSSubsystem		
? Forgot your Extension PIN?	Receive a new Extension PIN by email		
? Forgot your Mailbox PIN?	Receive a new Mailbox PIN by email		

© 2017 Mitel Networks Corporation

A random authorization code of selected PIN length will be generated for the selected extension in MiVoice MX-ONE and an email will be sent out to the user with the generated PIN number. The PIN number will be updated in MiCollab Server if the user exists in MiCollab Subsystem.

#### Figure 1.18: Extension PIN Reset

Mitel Provisioning Manager		
End User Information Ger	<u>ieral</u>	
General > PIN Reset		
Receive a new Extension PIN by en	nail	
? Select Extension:	5667,TSSubsystem	
? Select Extension PIN Length:	6	
Apply Cancel		

A random password of selected PIN length is generated for the selected mailbox number in MiCollab Advanced Messaging Server and an email is sent to the user with the generated PIN number.

**NOTE:** If only one Mailbox is assigned to the user, then selected Mailbox field changes to non-editable mode.

If multiple mailboxes are assigned to user, a drop down field will be displayed.

Figure 1.19: Mailbox PIN Reset

	ing Manager
End User Information Ge	neral
General > PIN Reset	
Receive a new Mailbox PIN by em	ail
? Select Mailbox:	56677, MailboxSubsystem
? Select Mailbox PIN Length:	6
Apply Cancel	

# Installing MX-ONE Provisioning Manager, Installation Instruction

# Introduction

This document describes the installation and configuration procedure of MX-ONE Provisioning Manager (PM). There are different installation scenarios for MX-ONE Provisioning Manager available. It can either be installed as a standalone application, or together with a MX-ONE Service Node on one of the included servers.

# **Installation Scenarios**

There are two installation scenarios to consider:

- Coexistence with MX-ONE Service Node Manager (SNM). This applies when MX-ONE Provisioning Manager is installed on LIM1 (server 1) in a single or multiple server installation.
- Standalone
   This applies when MX-ONE Provisioning Manager is installed on any other server, including a MX-ONE Service Node that is not LIM1 (server 1).

In case MX-ONE Provisioning Manager shall co-exist on the same server as e.g. LIM2 (MX-ONE Service Node 2), the Service Node software must have been installed prior to MX-ONE Provisioning Manager.

# Installation Using mxone\_maintenance Script

It is recommended to install MX-ONE Provisioning Manager on a server that is part of the MX-ONE. Either it could be a server installed as Standalone Management Server, or on any of the LIM's.

The MX-ONE Provisioning Manager install binary is distributed with the MX-ONE package on the master LIM, and can easily be installed on selected server through the MX-ONE Maintenance Utility. Log-in as user **mxone\_admin**, and run the sudo -H /opt/mxone\_install/bin/mxone\_maintenance command and select **addon\_software** and follow the instructions on screen.

When another server than the master server is selected as target machine for the installation, the software will first be downloaded from the master server with the function rsync. To avoid interference with any possible live traffic, the bandwidth in this process is limited to 10 Mbit/s.

# **Prerequisites**

The prerequisites depends on the installation type.

# StandAlone Installation

The Operating System (OS) SLES12 needs to be installed and configured on the customer's server.

For information on how to install SLES12, see the installation instruction for *INSTALLING AND CONFIG-URING MIVOICE MX-ONE*.

Follow the instructions during the installation. When running  $net\_setup$  command, choose to configure the server for Other Server.

# **Coexistence Installations on Server 1**

The MX-ONE Service Node software must be installed. MX-ONE Provisioning Manager must have the same software version (for example, 7.0 SP0) as MX-ONE Service Node Manager and the MX-ONE Service Node.

For more information, see INSTALLING AND CONFIGURING MIVOICE MX-ONE.

# Considerations

When MX-ONE Provisioning Manager or MX-ONE Service Node Manager is installed a software package for configuration of the web server is also installed.

This configuration package provides a command – webserver\_config -that is used to configure the protocol (HTTP/HTTPS) the web server shall run. When HTTPS is chosen, it will also handle certificate management.

It is important to be aware that when MX-ONE Provisioning Manager and MX-ONE Service Node Manager co-exist on the same server, it is always the web server configuration that rules. That is, it is not possible to run one application in HTTP and the other in HTTPS on the same server.

When the web server is configured for HTTPS, it will do a redirect (302) to HTTPS on any call to HTTP.

If it is configured for HTTP, it will not reply on calls to HTTPS.

# **Preparations**

Before starting the installation, some preparations, described in this chapter, needs to be done.

# **Obtaining a Digital Certificate**

MX-ONE Provisioning Manager can be configured to use either standard HTTP or HTTPS. With HTTPS, it is necessary to configure a private key and a digital certificate, to be used in the system. The digital certificate can either be generated as a self-signed certificate after the installation or bought from a commercial certificate supplier.

In both cases the certificate is applied by using the <code>webserver\_config</code> command and then chooses to modify web server protocol + HTTPS.

# Installation

- 1. To start the installation of MX-ONE Provisioning Manager, log-in as user mxone\_admin.
- 2. Run the command sudo -H /opt/mxone\_install/bin/mxone\_maintenance and select option addon\_software and follow the instructions on screen.
- 3. During the installation a number of dialogue boxes will appear on the screen. Select **Yes** to continue the installation, or select **No** to exit the installation.
- 4. Wait until the software is installed.
- 5. Follow the progress according to on-screen instructions
- 6. Enter name, last name and user id for the System Setup Admin.
- 7. Enter a password for the System Setup Admin.
- 8. Confirm the password.
- 9. Enter Main Department Name, Main Department Location and Main Location Description.

**NOTE:** These settings can be changed later.

- 10. Select Yes to do a restart, select No to take the restart later.
- 11. To configure protocol (HTTP/HTTPS + certificate) run the webserver\_config command when the installation is complete.

# Accessing MX-ONE Provisioning Manager

If MX-ONE Provisioning Manager and MX-ONE Service Node Manager coexist on the same server, the default application to be accessed on the web server root is MX-ONE Provisioning Manager.

Pm can be accessed by only IP or <IP>/mp and <IP>/pm

Example, 192.168.100.50 or 192.168.100.50/mp or 192.168.100.50/pm

MX-ONE Service Node Manager can be accessed by adding *"/mts"* or *"/snm"* or *"/wbm"* at the end of the address, for example, 192.168.100.50/mts or 192.168.100.50/wbm or 192.168.100.50/snm

# **MX-ONE Provisioning Manager Start and Stop**

MX-ONE Provisioning Manager is running as an application under Jboss web server. To start/stop/restart the MX-ONE Provisioning Manager it is effectively the Jboss service that must be started/stopped/restarted. When this is done, other applications running under Jboss will also be affected. This concerns MX-ONE Service Node Manager and CSTAPhaseIII.

To restart the web server (Jboss) run the webserver\_config command and select Re-start webserver.

To check the status, start or stop Jboss, run the following commands:

- 1. systemctl status mxone\_jboss.service
- 2. systemctl start mxone\_jboss.service
- 3. systemctl stop mxone\_jboss.service

# Upgrade

When you run the installation file, it will automatically detect if there is an earlier version of MX-ONE Provisioning Manager installed and perform an upgrade. If the installation file is the same as the installed version, the installation/upgrade will stop.

Before starting the upgrade:

- 1. Go to the Scheduling task in MX-ONE Provisioning Manager and print all scheduled events. The scheduled events will not be kept during upgrade since the stored commands may not work any longer in the upgraded version.
- 2. Before performing an upgrade, create a backup of current database from a linux shell.
  - Run the mp\_configcommand and select Database backup. Press Enter.
  - When finished, copy the latest file from directory /var/opt/eri\_mp\_config to a safe storage. The dump files are named **mpManagerPostgres-Dump.<date+time>-<rpm-version>**.

This measure is only as a precaution in case something fails during the upgrade. In normal circumstances the data will automatically be restored.

**NOTE:** When PM and SNM are running on the same server, this backup should be done before upgrading the MX-ONE Service Node.

**3.** Log out from the MX-ONE Provisioning Manager Graphical User Interface before performing an upgrade.

Run the installation file as described in *Installation* and follow the on-screen instructions.

# Migrating 5.x or 6.x Manager Provisioning Data to 7.x PM

For more information, refer to the *MiVoice MX-ONE Upgrading or Updating MX-ONE 7.X - Installation Instruction* guide.

# Migrating from D.N.A. to MX-ONE Provisioning Manager

D.N.A. is not supported in MX-ONE 7.x. Migrating from D.N.A. to MX-ONE Provisioning Manager means that user and department data in MX-ONE, and the management of this data, is transferred from D.N.A. to MX-ONE Provisioning Manager.

# **Migration Scenarios**

A migration is performed according to one of following scenarios:

- Migration from D.N.A. directly to MX-ONE Provisioning Manager, as described in <u>Migrating from D.N.A. to MX-ONE Provisioning Manager on page 12</u> This scenario is used for environments where CMG is not included.
- Migration from D.N.A. to an environment including both MX-ONE Provisioning Manager and CMG, as described in *Migrating from D.N.A. to MX-ONE Provisioning Manager*.
- Migration from an environment including D.N.A's EMG (extension management) and CMG (user management) to an environment including MX-ONE Provisioning Manager and CMG.

# Migrating from D.N.A. to MX-ONE Provisioning Manager

**NOTE:** This migration scenario does not apply for environments including both MX-ONE Provisioning Manager and CMG.

Migration from D.N.A to MX-ONE Provisioning Manager comprises the following steps:

- 1. Exporting user and department data from D.N.A.
- 2. Backing up data in MX-ONE Provisioning Manager
- 3. Importing D.N.A. data to MX-ONE Provisioning Manager
- 4. Backing up data in MX-ONE Provisioning Manager (now including D.N.A. data).

### Exporting User and Department Data in D.N.A.

The following D.N.A. data is required when migrating from D.N.A. to MX-ONE Provisioning Manager:

- User data
- Department data
- A definition (.def) file, defining the user data structure in D.N.A.
- A definition (.def) file, defining the department data structure in D.N.A.

**NOTE:** Department names in MX-ONE Provisioning Manager must **not** contain the following characters: ", \*, ?, \, <>, ', and ,

Departments containing any of there characters must be renamed before exporting data from D.N.A.

Follow the steps below to export data from D.N.A:

- 1. On the D.N.A. server, open the **export.exe** application. The application is normally found in the DNA\_S\DMG\BIN folder.
- 2. Click Application and then Export.
- 3. In the **Export Data Status** dialog, select **Person File** and **Department File** and set the file names as desired. Unselect the other export options.
- 4. Click Apply.
- 5. Exit the application.
- 6. On the D.N.A. server, open the DNA\_S\DMG\BIN folder and move the following files to a USB memory or similar:
  - user.def
  - user.txt
  - dept.def
  - dept.txt

# Backing Up Data in MX-ONE Provisioning Manager

Before D.N.A. data is imported to MX-ONE Provisioning Manager, a data backup must be performed in MX-ONE Provisioning Manager by following the steps below:

- 1. In MX-ONE Provisioning Manager, go to the **Backup & Restore task** on the **System** tab.
- 2. Click Backup.

#### CHAPTER 2

### Importing D.N.A. Data in MX-ONE Provisioning Manager

After backing up data in MX-ONE Provisioning Manager, D.N.A data can be imported. Follow the steps below to import D.N.A. data:

- 1. In MX-ONE Provisioning Manager, go to the Import task on the System tab.
- 2. Click Import....
- 3. Select D.N.A. and click Next.
- 4. Select Department.
- 5. In the **Definition File [.def]** field of the **Department** section, specify the **dept.def** file created during the export in D.N.A.
- 6. In the **Data File [.txt]** field of the **Department** section, specify the **dept.txt** file created during the export in D.N.A.
- 7. Click **Next** and then **Apply**.
- 8. Click Import....
- 9. Select D.N.A. and click Next.
- 10. Select User.
- 11. In the **Definition File [.def]** field of the **User** section, specify the **user.def** file created during the export in D.N.A.
- 12. In the Data File [.txt] field of the User section, specify the user.txt file created during the export in D.N.A.
- 13. Click Next and then Apply.

The exported D.N.A. users and departments are now available in MX-ONE Provisioning Manager.

**14.** Perform a data backup in MX-ONE Provisioning Manager according to *Backing Up Data in MX-ONE Provisioning Manager*.

# Migrating from D.N.A. to MX-ONE PM in Environments

Migration from D.N.A to MX-ONE Provisioning Manager in environments including both MX-ONE Provisioning Manager and CMG comprises the following steps:

- 1. Exporting user and department data from D.N.A.
- 2. Importing D.N.A. data to CMG.
- 3. Backing up data in MX-ONE Provisioning Manager.
- 4. Adding CMG as a subsystem in MX-ONE Provisioning Manager.
- **5.** Verifying that the root department in MX-ONE Provisioning Manager corresponds to the root department in CMG.
- 6. Importing CMG data in MX-ONE Provisioning Manager.
- 7. Backing up data in MX-ONE Provisioning Manager.

## Exporting User and Department Data from D.N.A.

The following D.N.A. data is required when migrating from D.N.A. to MX-ONE Provisioning Manager and CMG:

- User data
- Department data
- A definition (.def) file, defining the user data structure in D.N.A.
- A definition (.def) file, defining the department data structure in D.N.A.

**NOTE:** Department names in MX-ONE Provisioning Manager must **not** contain the following characters: ", \*, ?, \, <>, ', and ,

Departments containing any of there characters must be renamed before exporting data from D.N.A.

For information on how to export data from D.N.A., see *Exporting User and Depart-ment Data in D.N.A.* on page 12

## Importing D.N.A. Data to CMG

When migrating D.N.A. data in an environment including MX-ONE Provisioning Manager and CMG, data must be imported in each system separately. MX-ONE Provisioning Manager contains functionality for importing CMG data, and it is recommended that D.N.A. data is imported to CMG first. By then importing the CMG data (now also containing D.N.A. data, if following this procedure) to MX-ONE Provisioning Manager, the CMG and MX-ONE Provisioning Manager databases will be identical (a prerequisite for environments using MX-ONE Provisioning Manager and CMG). For information on how to import D.N.A. data to CMG, see *CMG General Installation Guide*.

NOTE: After import, verify that the D.N.A. data is available in CMG.

### Downloading and Installing the CMG Export Registry File

Before exporting data from CMG, a registry file defining how to format CMG data so that it can be imported to MX-ONE Provisioning Manager must be installed on the CMG server. Follow the steps below to download the file using MX-ONE Provisioning Manager:

- 1. In MX-ONE Provisioning Manager, go to the **Data Management** task on the **System** tab and click **Import...**.
- 2. In the Import Source section, select CMG and click Next.
- 3. Click in the Download Registry File [.reg] section and save the file to a USB memory or similar. The



file name is CMG\_export\_setup.reg.

- 4. On the CMG server, create a backup of the registry. For information on how to back up a registry, refer to *Microsoft's* documentation.
- 5. Move the CMG\_export\_setup.reg file to the CMG server and install it by double-clicking it.
- 6. After successful installation of the registry file, delete the file.

## **Exporting Data from CMG**

The CMG application **Spman** is used for exporting data from CMG. The application extracts user data from the CMG database and stores it to an ASCII file with one row per user. The registry on the CMG server (updated in the previous chapter) defines the following parameters for the file:

- File name
- Data format
- Extracted fields
- Selected users
- Sort order

**NOTE:** Do not change any settings or the order of the settings in the export setup registry file, otherwise the import of the extracted data will fail.

Follow the steps below to export data from CMG:

- 1. Click Start, Programs, Mitel and then Spman.
- 2. Select Export\_MP.
- 3. On the Edit tab, select Enabled and click Save.

**NOTE:** On this tab, the registry settings installed earlier are displayed. The settings are installed as *HKEY\_LOCAL\_MACHINE\SOFTWARE\Netwise\Nice<dbid>\Programs\EXPORT\_MP*.

Program	EXPORT_MP		
Program path	export.exe		Save
Parameters	-n EXPORT_MP		
Wait	0		New
Max restarts	0		Delete
Start order	0		
Enabled			
Desktop	Г		Previou
State	Running		Next
Start time	08-05-06 11:09		
Errors	0		
Additional para	ameters		
Group	Name	Value	
Config	▼ FileSpec	MPExport.txt	•

Figure 2.1: Edit tab

4. On the Status tab, initiate the export by clicking Start.

atabase Ericsso	n 💌					
Program	Start time	Trace	Errors	State		Select <u>all</u>
BROADCAST		0	0	Disabled	-	Develophel
CMGVoiceSrv		0	0	Disabled		Deselect al
CmgVoiceSync		0	0	Disabled		Start
CTR		0	0	Disabled		
DBTOPBX	08-04-03 15:17	0	0	Running		Stop
DELIR	08-04-03 15:17	0	0	Running		<u>I</u> race
EXPDELTA		0	0	Disabled		
EXPDELTALDIF		0	0	Disabled		<u>R</u> efresh
EXPORT		0	0	Not running		
EXPORT_MP	08-05-06 11:09	0	0	Running		Exit
FLASH	08-04-03 15:17	0	1	Running		
FLEXSIM		0	0	Disabled		
FUTURE	08-04-03 15:17	0	0	Running		
IMPORT		0	0	Disabled		
IMPORTLDIF		0	0	Disabled		
IMPORTORG		0	0	Disabled		
IRCTONOTES		0	0	Disabled	-	

Figure 2.2: Status tab

 After approximately one minute, the state of EXPORT\_MP changes from Running to Not running, indicating that the export is finished. If state is not changed automatically, click Command and Refresh.

Normally, the export is only performed once. If it is necessary to redo the export, repeat the export procedure, starting from step 5 above.

The exported file **MPExport.txt** is stored in the CMG log directory, usually C:\NiceServ\log.

**NOTE:** It is not recommended to import more than 500 users at a time in MX-ONE Provisioning Manager. If the exported file contains more than 500 users, divide it into multiple files with a maximum of 500 users in each file.

### Backing Up Data in MX-ONE Provisioning Manager

Before CMG data (also containing D.N.A. data, if following this procedure) can be imported to MX-ONE Provisioning Manager, a data backup must be performed by following the steps below:

- 1. In MX-ONE Provisioning Manager, go to the **Backup and Restore** task on the **System** tab.
- 2. Click Backup.

#### CHAPTER 2

### Adding CMG as a Subsystem in MX-ONE Provisioning Manager

In environments comprising MX-ONE Provisioning Manager and CMG, MX-ONE Provisioning Manager is the single point of entry for managing user and extension data. To achieve this, CMG must be added as a subsytem in MX-ONE Provisioning Manager. This means that changes performed to a user in MX-ONE Provisioning Manager automatically applies to the user's settings in CMG.

Follow the steps below to add CMG as a subsystem in MX-ONE Provisioning Manager:

- 1. In Provisioning Manager, go to the Subsystem task on the System tab and click Add.
- 2. In the **Subsystem Type** field, select **CMG Server** and specify the settings of the CMG server.

### Creating Locations for CMG Customer Groups in MX-ONE PM

There must be a location created in MX-ONE Provisioning Manager for each CMG customer group. If a CMG customer group is not mapped to a location, a new location for the CMG customer group is created in MX-ONE Provisioning Manager during the import. Follow the steps below for each customer group in CMG:

- 1. In MX-ONE Provisioning Manager, go to the **Location** task on the **System** tab and click **Add**.
- 2. In the Location Name field, specify a name for the location.
- 3. In the **CMG Customer Group** field, specify the customer group in CMG to which the location will correspond.
- 4. Click Add.

#### Importing CMG Data in MX-ONE Provisioning Manager

When CMG is added as a subsystem in MX-ONE Provisioning Manager and locations that corresponds to the customer groups in CMG are created, CMG data can be imported to MX-ONE Provisioning Manager.

The CMG data does not include user ID fields. If a misc field contains the user ID you can map that field during import. If not, the exported CMG data can be manually edited and user ID data can be entered into one of the unused misc fields to be mapped during the import.

Follow the steps below to import CMG data:

- 1. In MX-ONE Provisioning Manager, go to **System** tab and **Data Management** tab. Then select task **Import**.
- 2. Click Import....
- 3. Select CMG and click Next.
- 4. In the Data File [.txt] field, select the MPExport.txt file created during the CMG export procedure.
- If the user data in CMG contains a misc field defining a mailbox number, this data can be mapped to the MX-ONE Provisioning Manager mailbox settings. To import the mailbox data, select Import Mailbox Info.
- 6. Click Next.
- 7. In the Map imported UDF(s) to MX-ONE Provisioning Manager UDF(s) section, specify how to map the adaptable fields in CMG (found below the Keywords section on the Main Form tab in CMG Directory Manager) with the User Defined Fields (UDFs) in MX-ONE Provisioning Manager.
  - NOTE: If importing mailbox info was selected in the previous step, do the mailbox mapping.

- If a misc field holds the user ID, do the user ID mapping.

- 8. Click Next.
- 9. In the **Map imported PBX ID(s) to Subsystem(s)** section, specify how to map PBX IDs in CMG with subsystems in MX-ONE Provisioning Manager.
- 10. Click Apply.
- 11. On the **Result** page, click **Done**.
- **12.** Verify that the imported CMG data is available in MX-ONE Provisioning Manager.
- **13.** Perform a data backup in MX-ONE Provisioning Manager according to *Backing Up Data in MX-ONE Provisioning Manager*.

**NOTE:** See *Important Post-Migration Considerations* on page 16 for important information on how to manage user data in environments including MX-ONE Provisioning Manager and CMG.

# Migrating to MX-ONE PM from Environments

Migration to MX-ONE Provisioning Manager from environments using D.N.A.'s Extension Manager (EMG) for extension management and CMG for user management follows the procedure described with the following exceptions:

 The procedure starts at *Registry File on page 15* Downloading and Installing the CMG Export

 The CMG data referred to in Manager on page 17 is already. Backing Up Data in MX-ONE Provisioning does already include D.N.A. data since user data

**NOTE:** See *Important Post-Migration Considerations on page 19* for important information on how to manage user data in environments including MX-ONE Provisioning Manager and CMG.

# **Backing Up Data in CMG**

Data backup in CMG is performed automatically, on a daily basis. To be able to restore CMG data in case of a failed import of D.N.A. data, it is recommended that the most recent backup is located and made available before importing data from D.N.A.

For information on how to access and restore data backup files in CMG, see CMG General Installation Guide.

# **Important Post-Migration Considerations**

After the migration of CMG and D.N.A. data, MX-ONE Provisioning Manager is the single point of entry for user and extension management in MX-ONE. When changing user and extension data in MX-ONE Provisioning Manager, the corresponding data in CMG is automatically updated accordingly. Changing user data in CMG will cause unsynchronized databases.

Import from CMG to MX-ONE Provisioning Manager should only be performed once, during the migration. If MX-ONE Provisioning Manager is used correctly (that is, the application is used for all user management in MX-ONE), there will be no need for additional imports of CMG data.

For more information on user and extension data in MX-ONE Provisioning Manager and its subsystems, see *MX-ONE Provisioning Manager, Description*.

# **Post Installation**

Figure 2.3: Post-Installation menu		
Provisioning Manager Post-Install Configuration		
This utility is for performing individual tasks in Provisioning Manager.		
You can use the UP/DOWN arrow keys to navigate and spacebar to select.		
Please choose your option!		
Database check         [] 0       Database backup         [] 0       Database restore         [] 0       Provisioning Manager Re-install         [] 0       Unlock user         [] 0       Set user password         [] 0       View user privileges		
< <mark>0K &gt;</mark> < Exit >		

To access the post install menu, log in as **mxone\_admin** and enter the following command:

sudo mp\_config

Select one of the options:

- Database check, to verify some basic but important settings in the database
- Database backup, to create a backup of the database
- Database restore, to choose from a list of backups and restore it to the database
- **MX-ONE Provisioning Manager Re-install**, to re-install current version of MX-ONE Provisioning Manager and then choose from a backup list which data to restore
- Unlock user, to unlock a user specified by user id
- Set user password, to set a new password for an existing user specified by user id
- View user privileges, to list the subset of privileges that is assigned to a user specified by user id

Additional configuration (common for the system) can be found through the command (webserver\_config); Run as root.

## Uninstallation

To uninstall MX-ONE Provisioning Manager, login as **mxone\_admin** and run the following command:

sudo mp\_uninstall

## Log Files

Log files are created automatically and can be found in directory /var/log/mxon-e\_pm/eri\_mp.

#### Installation/Upgrade:

- mp\_install.log
- mx-one\_pm\_rpm\_<version>-<release>.log

#### **Un-installation:**

- mp\_uninstall.log
- mx-one\_pm\_rpm\_<version>-<release>.log

Additional information can be found in log files for Webserver Configuration (directory /var/log/mxone/webserver):

- webserver\_config.log
- application\_log.log

Runtime information can be found in directory /opt/jboss/standalone/log:

server.log

## **Fault Recovery**

If the installation is unsuccessful, see *Fault Handling* for a solution.

## **Increasing Heap Memory Size in Jboss Configuration File**

Follow the steps below for increasing the heap memory size in Jboss configuration:

- 1. Login to Provisioning Manager server with root user credentials.
- 2. Go to path: cd /opt/jboss/bin/
- **3.** Edit **standalone.conf**file and change the options Xms512m and Xmx512m to the desired values. In the example below, options are changed to 2048m

JAVA\_OPTS="-Xms2048m -Xmx2048m -XX:MaxPermSize=256m -Djava.net.preferIPv4Stack=false -Djava.net.preferIPv6Addresses=true" JAVA\_OPTS="\$JAVA\_OPTS -Djboss.modules.system.pkgs=\$JBOSS\_MOD-ULES\_SYSTEM\_P-KGS -Djava.awt.headless=true" JAVA\_OPTS="\$JAVA\_OPTS -Djboss.modules.policy-permissions=true" JAVA\_OPTS="\$JAVA\_OPTS -Djboss.modules.policy-permissions=true"

4. Save the changes.

#### 5. Restart PM server.

**NOTE:** For restarting PM server, log in as **mxone\_admin** and run command: sudo webserver\_config and select restart web server.

# **MX-ONE Provisioning Manager Deployment**

## Introduction

MX-ONE Provisioning Manager is a web-based management tool for management of MX-ONE<sup>™</sup> extensions through a Graphical User Interface (GUI).

MX-ONE Service Node Manager is a web-based management tool used for configuration of the MX-ONE through a Graphical User Interface (GUI). MX-ONE Service Node Manager is also used for creation and updates of configuration files for the IP phones.

MX-ONE Service Node Manager must always be deployed on Service Node 1 (LIM1) in the MX-ONE.

The purpose with this document is to describe the alternatives available for deployment of MX-ONE Provisioning Manager and provide recommendations for different scenarios.

**NOTE:** Both MX-ONE Service Node Manager and MX-ONE Provisioning Manager must be deployed on Linux based servers.

## **MX-ONE PM Deployment Alternatives**

## General

MX-ONE Provisioning Manager can be deployed:

- on the same server as MX-ONE Service Node Manager
- on another MX-ONE Service Node
- on a separate, Linux based server

There are several factors considered before taking a decision such as:

- Company strategies
- System size
- Server type (s)
- · Networked or one stand-alone system

The user must follow the general guidelines when planning the deployment of the management applications in the MX-ONE system and/or network:

- Communication protocol used between MX-ONE Service Node Manager and MX-ONE Provisioning Manager is the only functional difference between deployment of MX-ONE Provisioning Manager on the same server or on a different server as MX-ONE Service Node Manager.
- Web services communication is used when the applications are deployed on different servers. This
  communication occurs in large systems with many users, which can result in longer response times
  (for example, requesting printouts of all extensions). The network stability/quality also has an impact
  on this communication, which is in an unstable network situation (means communication is disturbed
  or interrupted).

**CHAPTER 3** 

- MX-ONE Provisioning Manager's communication with MX-ONE is done through MX-ONE Service Node Manager, which means if MX-ONE Service Node Manager is not running; MX-ONE Provisioning Manager cannot access the MX-ONE system that MX-ONE Service Node Manager is running on. So, during network configuration, MX-ONE Provisioning Manager interfacing many MX-ONE systems is recommended to have MX-ONE Provisioning Manager on a separate server.
- Connection with the different MX-ONE Service Node Manager applications takes place by using of web services.
- MX-ONE Service Node Manager and MX-ONE Provisioning Manager must have the same SW version when deployed on the same server, which must be upgraded at the same time.
- When deployed on different servers, MX-ONE Provisioning Manager must have the same or higher SW version than MX-ONE Service Node Manager.

### MX-ONE SNM and PM on the same SN

This is the most common alternative and the recommended deployment for a 1 server (LIM) system.

The following are the industrial standard servers and virtualized server requirements for MX-ONE:

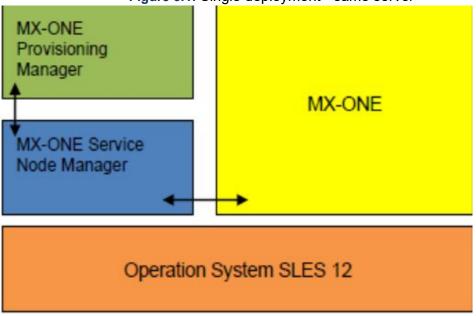


Figure 3.1: Single deployment - same server

Table 3.1: MX-ONE 7.0 - Server Requirements - Industrial Standard Servers (Sheet 1 of 2)

		Provisioning M	anager Standal	one		
	Physical Server (Bare metal)					
Number of Users	Memory (GB)	Number of CPUs	Disk (GB)	Application (GB)	Type of Server	
500	4	2	100	100	Provisioning Manager Standalone	

	Provisioning Manager Standalone							
	Physical Server (Bare metal)							
Number of Users	Memory (GB)	Number of CPUs	Disk (GB)	Application (GB)	Type of Server			
1000	4	2	100	100	Provisioning Manager Standalone			
2500	6	2	100	100	Provisioning Manager Standalone			
5000	6	4	100	100	Provisioning Manager Standalone			
7500	6	4	100	100	Provisioning Manager Standalone			
10000	8	4 100		100	Provisioning Manager Standalone			
15000	8	4	100	100	Provisioning Manager Standalone			
30000	12	6	100	100	Provisioning Manager Standalone			
50000	16	6	100	100	Provisioning Manager Standalone			
70000	20	6	100	100	Provisioning Manager Standalone			
100000	24	6	100	100	Provisioning Manager Standalone			

#### Table 3.1: MX-ONE 7.0 - Server Requirements - Industrial Standard Servers (Continued) (Sheet 2 of 2)

Provisioning Manager Standalone								
	Physical Server (Bare metal)							
Number of Users	Memory	Memory (GB) CPU				Disk (GB)	Application (GB)	
Number of managed users	Minim um (GB) require d Memor y	Reserv ation (GB)	Minimum number of vCPU required	Minimum MHZ required	Minimum MHZ reservatio n	Disk size (GB)	Type of Application	
500	4	2	2	1000	500	100	Provisioning Manager Standalone	
1000	4	2	2	1000	500	100	Provisioning Manager Standalone	
2500	6	2	2	1000	500	100	Provisioning Manager Standalone	
5000	6	3	4	3500	2000	100	Provisioning Manager Standalone	
7500	8	3	4	3500	2000	100	Provisioning Manager Standalone	
10000	8	4	4	3500	2000	100	Provisioning Manager Standalone	
15000	8	4	4	3500	2000	100	Provisioning Manager Standalone	
30000	12	6	6	4000	2000	100	Provisioning Manager Standalone	
50000	16	6	6	4000	2000	100	Provisioning Manager Standalone	

#### Table 3.2: MX-ONE 7.0 - Server Requirements - Industrial Standard Servers (Sheet 1 of 2)

			Provisioning	g Manager Star	ndalone		
			Physical	Server (Bare m	netal)		
Number of Users	Memory	(GB)	CPU			Disk (GB)	Application (GB)
Number of managed users	Minim um (GB) require d Memor y	Reserv ation (GB)	Minimum number of vCPU required	Minimum MHZ required	Minimum MHZ reservatio n	Disk size (GB)	Type of Application
70000	20	6	6	4000	2000	100	Provisioning Manager Standalone
100000	24	8	6	4000	2000	100	Provisioning Manager Standalone

Table 3.2: MX-ONE 7.0 - Server Requirements - Industrial Standard Servers (Continued) (Sheet 2 of 2)

It is mandatory to change the heap memory size in JBoss configuration for Provisioning Manager and Service Node Manager as mentioned below. The memory requirements are in addition to the memory required by Service Node.

- 2048 MB (2GB) or more recommended for up to 2000 users
- 4096 MB (4GB) or more recommended for more than 2000 users

NOTE: The default value of 512 MB in JBoss configuration support is up to 1000 users.

For instructions on how to change heap size, contact Mitel Support team or refer to *Installing MX-ONE Provisioning Manager* document or *NSTALLING AND CONFIGURING MIVOICE MX-ONE* I document.

Also, it is recommended to run Provisioning Manager on a standalone system for more than 2000 users.

#### **MX-ONE SNM and PM on different Service Nodes**

This alternative is recommended for a multi-server (LIM) system, that is more than one server and more than 2000 users using either with industrial standard servers or virtualized server. In this situation, the master LIM server has MX-ONE Service Node Manager installed and MX-ONE Provisioning Manager is placed on any of the LIM in the system. This is done to offload the master server.

This is recommended as an alternative during configurations, where it is foreseen that the processing in server one (master server) becomes heavy due to specific functionality/interfaces.

It is mandatory to change the heap memory size in JBoss configuration for Provisioning Manager and Service Node Manager as mentioned below:

• 4096 MB (4GB) for PM system (for more than 2000 users).Note! If a large number of users are managed by Provisioning Manager, you may need to increase the heap memory size to a higher value.

 4096 MB (4GB) for Service Node Manager (4GB). This memory requirement is on top of memory needed by Service Node.

For instructions on how to change heap size, contact Mitel Support team or refer to *Installing MX-ONE Provisioning Manager* document or *INSTALLING AND CONFIGURING MIVOICE MX-ONE* document. **NOTE:** This deployment mode is that, even if MX-ONE Service Node Manager is the MX-ONE Provisioning Manager communication link to the MX-ONE Service Node, it is the server that MX-ONE Provisioning Manager is deployed on that absorbs the Java CPU load.

The communication between MX-ONE Service Node Manager and MX-ONE Provisioning Manager takes place through web services (with or without security enabled).

#### **MX-ONE PM on Separate Server**

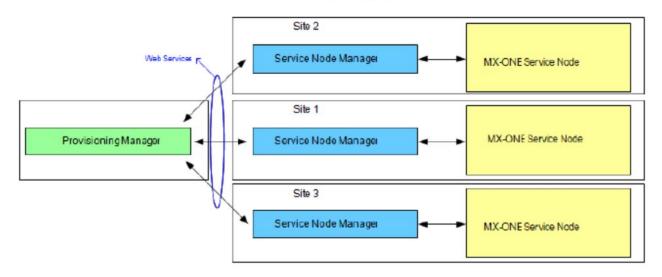
In a network where there may be several MX-ONE systems, networked together, it may be advantageous to place the MX-ONE Provisioning Manager on its own server, independent of any MX-ONE system. This is the recommended alternative for a networked set-up as MX-ONE Provisioning Manager can access all operational MX-ONE systems.

By placing the MX-ONE Provisioning Manager on a separate server, user can avoid loss of communication to all other MX-ONE systems; which is unavoidable during upgrading of the MX-ONE system where MX-ONE Provisioning Manager typically resides.

The server that MX-ONE Provisioning Manager is deployed on should be equipped with minimum 4 GB of RAM.

The communication between MX-ONE Service Node Manager and MX-ONE Provisioning Manager takes place through web services (with or without security enabled).

Figure 3.2: Communication between MX-ONE Node Manager and Provisioning Manager



Multi Deployment

# **MX-ONE Provisioning Manager, User** Instructions

## Introduction

This section discusses MX-ONE Provisioning Manager.

### Scope

The user guide contains:

- A workflow describing in which order to add data into PM
- A description of the navigation and the user interface in PM
- An overview of how to perform actions in PM
- Additional information for some tasks
- PM system messages and error handling

## **Target Group**

This document is intended for users of MX-ONE Provisioning Manager and support personnel.

#### **Internet Browser Settings**

There are a few settings and aspects that needs to be considered to optimize function and performance:

- Javascript must be enabled in the browser in order to use PM.
- The browser must be configured to refresh pages on every visit. For information about browser configuration, see help and documentation specific for your browser.
- Installing many plug-ins in the browser may affect the rendering performance of the browser and may lead to longer lead time to display the web pages. PM does not require any browser plug-ins.

## **Target Group**

This document is intended for users of MX-ONE Provisioning Manager and support personnel.

## **Internet Browser Settings**

There are a few settings and aspects that needs to be considered to optimize function and performance:

Javascript must be enabled in the browser in order to use PM.

- The browser must be configured to refresh pages on every visit. For information about browser configuration, see help and documentation specific for your browser.
- Installing many plug-ins in the browser may affect the rendering performance of the browser and may lead to longer lead time to display the web pages. PM does not require any browser plug-ins.

## **MX-ONE Provisioning Manager Overview**

MX-ONE Provisioning Manager is a management tool for MX-ONE that is used to configure users and assign services to the users. It is also used to configure administrators with different access privileges for both MX-ONE and PM.

Subsystems can be connected to PM. A subsystem is a component of MX-ONE, for example, a MX-ONE. Any combination of subsystems is allowed. The subsystems provide services to the users.

For more information about PM, see the description for MX-ONE PROVISIONING MANAGER.

MX-ONE Provisioning Manager can be connected to MS Active Directory. User changes in AD can automatically trigger changes in PM and its subsystems. For more information, see the document MX-ONE PROVISIONING MANAGER INTEGRATION WITH MS ACTIVE DIRECTORY.

MX-ONE Provisioning Manager is part of the MX-ONE Manager concept that consists of several operation and maintenance applications providing management functions for MX-ONE. For more information about PM in MX-ONE, see the system description for MIVOICE MX-ONE.

#### **System Requirements**

MX-ONE Provisioning Manager can be accessed from anywhere using a commercially available browser. The browser requirements are:

- Microsoft Internet Explorer 8 (or later versions)
- Mozilla Firefox 18 (or later versions)
- Google Chrome (latest version)
- Microsoft Edge 80.0.361.48 (Official build) (64-bit)

Both HTTP (TCP Port 80) and HTTPS (TCP Port 443) are supported. If HTTPS is used, it must be configured. For higher security, it is recommended to use a commercial digital certificate issued by a commercial Certification Authority (CA). For more information about PM security, see the description for MX-ONE PROVISIONING MANAGER.

#### Key Features of MX-ONE Provisioning Manager

The key features of MX-ONE Provisioning Manager are:

- Location access restriction
- · Import and export functions of user and department data
- Assignment of services to users
- Support of the following phone types:
- Analog phones
- CAS phones

#### CHAPTER 4

- Fax
- Digital phones
- IP phones
- Cordless phones (DECT)
- Mobile phones/remote extensions.
- Backup functions
- MS Active Directory integration
- Comparison of PM data and subsystem data
- End user interface
- Efficiency enhancing features
- Web Service interface for external applications
- Configuration of Least Cost Routing for mobile extensions
- Assignment of function keys for digital and IP phones
- Configuration of personal number lists
- Configuration of parallel ringing
- Configuration of group membership

For more information about key features, see the description for MX-ONE PROVI-SIONING MANAGER.

## **Preferred Language**

The language used in MX-ONE Provisioning Manager can be set per user in the User task under the Advanced settings. The default language is English.

The sorting of the text columns in PM are by default done after the servers default language (en-US). To sort after another language, the preferred language setting must be set in the web browser.

## **Getting Started**

There are two ways to set up MX-ONE Provisioning Manager.

- Using the Wizard for Express and Express SAAS installation. A single page of entry fields helps you to quickly set up the system. This is possible since the system is predefined.
- Manual set up for all other installation setups. You are forwarded to the start page where you can
  access any task in the system to perform your configuration. See the Manual Workflow When Getting
  Started section below for further details.

## Manual Workflow When Getting Started

After installing MX-ONE Provisioning Manager it is recommended to add data into the system, for example to add departments, administrators, subsystems and so on, in the following order:

- 1. Optionally add additional locations in the Location task.
- 2. Optionally modify User Defined Fields (UDFs) for users and departments in the UDF Mapping task.
- 3. Optionally add additional departments in the Departments task. Alternatively the Import task can be used.

- 4. Optionally add or modify security profiles in the Security Profiles task.
- 5. Optionally add users to promote to administrators with different security profiles. Use the User and Administrator tasks.
- 6. Register subsystems
- 7. Add users and configure services such as extensions and mailboxes for the users using the User task. Alternatively the Import task can be used.

**NOTE:** To quickly find the location in the menu for the different tasks, a tip is to use the site map available at the top of MX-ONE Provisioning Manager.

**NOTE:** After installation it is recommended to create an extra super user to keep as backup if something happens to the original super user account, for example if the password is lost, otherwise the whole system must be reinstalled.

#### Integrating With MITEL CMG

The following settings are needed to get the integration with CMG in place:

- 1. The CMG Server shall be registered in the Subsystem task. Note the setting for CMG Department Structure.
- 2. Each registered MX-ONE (subsystem task) shall be mapped to a "CMG PBX ID" which is the CMG's own setting for the same MX-ONE.
- **3.** Each registered location (Location task) shall be mapped to a "CMG Customer Group" which is the CMG's own corresponding geographical or logical group number.
- 4. Users and departments can be imported from CMG in a migration scenario. The UDF (User Defined Fields) fields in PM can be defined during the import proce-dure.
- 5. The UDF field mapping to the CMG "Miscellaneous" fields can be managed in the UDF Mapping task when a CMG subsystem has been registered.
- 6. Make sure that the CMG Connection task in MX-ONE Service Node has been configured to set up the telephony connection between the MX-ONE and CMG Server.

When the above settings are in place, operations in the User task and renaming or changing parent department task will update the CMG.

Note: To open up the communication between the MX-ONE Provisioning Manager and the CMG Server, the AnA and CWI interfaces on the CMG Server must be enabled and activated and access given to the CMG user that was entered when registering CMG in the PM Subsystem task.

Note: In PM, you can create a department structure, and populate this department structure in CMG during PM/CMG synchronization. To do this, you need to make a change in the config file on the CMG server, for which you must have administrator rights.

Default path:

C:\ inetpub \ wwwroot \ CMGUserInformationService

Note that If you use Notepad or Notepad++ to change in the file, then you must start them with "run as administrator" or similar.

The default values are mentioned as below:

<add key="CreateOrg" value="False"/>

<add key="DeleteOrg" value="False"/>

You must change to:

<add key="CreateOrg" value="True"/>

<add key="DeleteOrg" value="True"/>

To make the parameter change to take effect, either you need to stop and start the application pool in IIS, that is running the application "CMGUserInformationService" or perform a iisrestin cmd.

Note: If CMG version is 8.2 and CMG speech is installed, then CMG speech shall have web services interface enabled and following files should be configured.

In CMGUserInformationService under Application Settings "SpeechProvisionin-gEnabled" parameter should be set to TRUE.

..\Aastra\Aastra Speech Service\SpeechServiceConfig.xml the Provisioning Port should be set to 8006

#### Integration With MiCollab Advanced Messaging

The following settings are needed to get the integration with Mitel MiCollab Advanced Messaging (AM) in place:

• The MiCollab AM Server shall be registered in the Subsystem task.

When the above configuration is in place the MiCollab AM mailboxes can be configured either through the User task or directory in the Mailbox task.

Note:Operations in the Mailbox task will not update PM user accounts that are tied to the targeted mailbox

Note: To open up the communication between the PM and the Mitel MiCollab AM Server, the web services interface on the Mitel MiCollab AM Server must be enabled and activated.

Note:The Mitel MiCollab AM shall NOT be set to use the "Windows login credentials", because PM will not be able to login into Mitel MiCollab AM in that case.

Note: The user account defined in MiCollab AM, which PM will use for its communication with MiCollab AM, shall have local admin rights in MiCollab AM.

#### Integration With MS Active Directory

Please see the document MX-ONE PROVISIONING MANAGER INTEGRATION WITH MS ACTIVE DIRECTORY for detailed information on how to update MX-ONE automatically from AD.

#### Integration With SIP-DECT OMM

MX-ONE Provisioning Manager integrates with the SIP DECT system through the OMM, which is its point of management. An OMM is defined as a subsystem. One OMM is connected to one MX-ONE Service Node. Reversely, an MX-ONE Service Node is connected to one OMM. A resiliency OMM is invisible to the PM, and cannot be separately administrated.

Once Manager Provisioning has the definition of an OMM, it can configure an end users' SIP-DECT service in it, and connect this service as an IP Terminal to a single- or multi-terminal Extension in the MX-ONE Service Node.

Please see the document "SIP-DECT OM SYSTEM MANUAL; INSTALLATION, ADMINISTRATION AND MAINTENANCE" for information on how to set up the OMM for use with PM.

#### Integration With MiCollab Server

Please see the MiCollab Platform Integration Guide document for detailed information on how to integrate PM with MiCollab Server.

## **Using MX-ONE Provisioning Manager**

In MX-ONE Provisioning Manager (PM) there is a number of configuration areas, for example, Users and System. Each configuration area contains a number of configuration tasks, for example, Departments and Subsystem. The configuration tasks are used to set up users, administrators, and their services.

This section describes the user interface and navigation in PM. How to use each task is explained in the online help, see Using the Help.

For information about troubleshooting, see FAULT HANDLING OF MX-ONE PROVI-SIONING MANAGER.

#### Logging In and Logging Out

Browse to the login screen of MX-ONE Provisioning Manager. Enter User Id and password provided by the administrator to log in to the application, the User Id and password are case sensitive. 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 the privilege Auto Unlock, for example the System Setup Admin User, will be automatically unlocked every 20 minutes time interval.

Click Logout in the upper right corner to log out from PM. If the browser window is closed, the user is automatically logged out.

The application has a time limit after which an inactive user is automatically logged out. The time limit is 45 minutes by default, the time left before automatic logout is indicated in the browser status bar (lower left corner).

To be enable to see this indicator, the browser must be configured for allowing status bar updates using Java Script.

For more information, see Enabling the Automatic Logout Indicator.

#### Navigating in MX-ONE Provisioning Manager

The user interface is divided into menu tabs and submenus containing different configuration tasks. For most of the tasks it is possible to view, add, change or remove configuration items. How to perform different actions is found in chapter 4, Actions.

Figure 4.1: MX-ONE Provisioning Manager User Interface

DI Mitel Provisioning Manager	Logged in as: Alacarte About User Guide Site Map Logout
Users Services Administrators System Logs Own Settings A	
Extension Available Extensions Individual Diversion Mailbox B	
Extension - Add - Step 1 / 2	Shortouts : Common Category 💙 Go Help
K- Back Next >> Apply Cancel	
MX-ONE Service Node:	Help Extension An extension is an internet phone line attached to a PIX. A user can have several extensions, for example, one extension for fixed telephony and one for mobile telephony. The following types of extensions can be managed: • DF (EIP, H323, IP-DECT, SIP-DECT, SIP-Remote) • Digital • Hole • Digital • Hole • Apale • Cols • ADN • DECT • Virtual • Nubi-Terminal This also possible to configure the
<- Back Next -> Apply Cancel	

#### Table 4.1: User interface items

Item	Description
A	Main menu
В	Submenu
C	Work area
D	Help frame

**NOTE:** Do not use the Back and Forward buttons in the browser. Using these buttons will result in an error message. Reload the page to go back to MX-ONE Provisioning Manager. Note:

#### Icons, Symbols and other Graphical Elements

The following icons and symbols are used in MX-ONE Provisioning Manager:

Table 4.2: Icons and Symbols in MX-ONE Provisioning Manager (Sheet 1 of 4)

Symbol	Function	Description
?	Help	Displays information about the property and how to configure it.

#### Table 4.2: Icons and Symbols in MX-ONE Provisioning Manager (Continued) (Sheet 2 of 4)

Symbol	Function	Description
0	Change	Change the properties for an existing configuration item.
Q	View Details	View the details of a configuration item.
×	Remove	Remove the configuration item.
	Add new using this as template	Add a new configuration item using an existing item as a template.
\$	Create template from this	Create a template with the values in the existing configuration item.
Y	Filter	Display or hide the fields used to filter the list.
\$ \$ \$ \$	Sort the list	Sort the list in ascending or descending order. The arrow pointing in both directions indicates that the column is unsorted.
*	Mandatory	It is mandatory to set a value for this property.
4	Undo changes	Restore the value to the previously saved value
Ð	Edit field	Enable the field for editing.
8	Information	Information exclamation mark followed by system information.

#### Table 4.2: Icons and Symbols in MX-ONE Provisioning Manager (Continued) (Sheet 3 of 4)

Symbol	Function	Description
6	Restore	Restore the system to a previous state.
3	Backup	Keeps the Backup of the current system state.
<b>(</b> ]	Download	Download a template in .xml format.
e f	Unlock	Unlock a locked user.
•	Run	Run a selected batch operation.
*	Multi terminal conversion	Conversion of single terminal (Generic extension) to multi terminal.
۲	Activate	Activate the set personal number list, that is, change status from Set to Active.
۲	Deactivate	Deactivate the active personal number list, that is, change status from Active to Set.
Θ	Not Set	The status of the personal number list is Not Set that is, the list has no defined call sequences.
•	Set	The status of the personal number list is Set that is, the list has defined call sequences but it is not active.

Table 4.2: Icons and Symbols in MX-ONE Provisioning Manager (Continued) (Sheet 4 of 4)

Symbol	Function	Description
٠	Active	The status of the personal number list is Active, that is, the list deflects incoming calls according to the defined call sequences.

#### Using the Help

There are several levels of Help in MX-ONE Provisioning Manager:

- User Guide: This user guide, which is found in the upper right corner of the application.
- Help: Online help for a specific task that provides information needed to complete the task. The help is displayed in a pop-up window or in the Help frame.
- Online context help that is displayed in a pop-up window for a specific property. The context help

describes the property's usage, options and if special conditions must be considered.

#### **Basic or Advanced Settings**

Property settings that are not often used and not mandatory are grouped in advanced settings for a task. Some fields in advanced settings have default values. The advanced settings are displayed by clicking Advanced. Basic settings are displayed by clicking Basic.

#### **Enabling the Automatic Logout Indicator**

MX-ONE Provisioning Manager comprises a function for displaying the remaining time until an automatic logout due to inactivity is performed. The information is displayed in the status bar of the browser.

Figure 4.2: Automatic logout indicator

29 minutes left to log out due to inactivity.

To be able to see this information, the browser must be configured for allowing status bar updates using Java Script. For information on how to enable this function in the browser, see the browser documentation.

## **Actions**

This section describes the actions that can be performed in the different tasks. Most of the actions can be performed at different stages, for example from a result screen or from a list view.

	Y	User Id	00	Last Name	90	First Name	40	Extension / Telephony System	90	Department(s)	40	Import from	4	Customer	40
		John		Roy		Dave				Company01					
	1	Micheal		Goud		Smith				Company01					
Change F	Rem	ove Pri	int	Compare	Vie	w									

#### Figure 4.3: List view

#### **Self Services**

The Forgot your password link on the login page of the GUI, makes it possible for users to get a new password. This is useful if the user has forgotten the password or if the user's account has been locked.

The following steps must be done to get a new password:

- 1. Click on the Forgot your password link. The Forgot Password screen is opened.
- 2. Enter a valid user id and press Submit.
- 3. A confirmation message are shown and a new password has been sent to the user's e-mail address.

**NOTE:** The Forgot your password link is only shown when a mail server is connected to the system.

### **Adding Data**

Data can be added to a new configuration item in the following ways:

- Click Add .... System default values are displayed for the new configuration item. To create a configuration item without using a template, the value <No Template> must be selected in the Using Template drop-down list before clicking the button. To create a configuration item using a template, see 4.10.3 Using a Template to Create a Configuration Item on page 19.
- 2. From a result screen or a view details screen, click Add from this.... The previously added configuration item is used as a template.
- **3.** From a list view, click (Add new using this as template). The selected configuration item is used as

a template.

Some configuration tasks have predefined values and can only be changed.

**NOTE:** When a user is added in the User task, it is automatically assigned the security profile End User. An end user can be promoted to administrator by assigning the user a different security profile and defining access to departments and locations in the Administrator task.

### **Viewing Data**

Configuration items can be viewed in the following ways:

- For some tasks the list view is displayed by clicking View. The list displays the existing configuration items with a subset of the property values or all property values.
- From a list view, click (View details). The details of the configuration item are displayed. Click on the

arrows to view the previous or the next configuration item.

• From a list view, select one or more configuration items, by clicking their check boxes, and then click View. The details of the selected configuration items are displayed simultaneously.

Data for selected configuration items can also be compared, see Comparing data.

#### **Filtering Data in List Views**

In some tasks, for example the User task, it is possible to filter the list in the list view to find specific configuration items. To display or hide the fields to enter the search criteria in, click (Filter).

To filter the list, enter the search criteria in one or more fields and click Filter. Wildcards can be used in the search criteria, a question mark (?) to replace one character or an asterisk (\*) to replace zero or more characters.

#### **Sorting Listviews**

**CHAPTER 4** 

The list in the listview can be sorted by clicking the arrows displayed for the columns:

in ascending order

(Sort descending): the column is sorted in ascending order, clicking it sorts the list by the items in that

column in descending order

• (Sort ascending): the column is sorted in descending order, clicking it sorts the list by the items in that

₽

column in ascending order

## **Comparing Data**

Configuration item properties can be compared with the compare function. The compare function is available in list views.

Perform the following steps to compare two configuration items:

- 1. Select two items to compare in the list.
- 2. Click Compare.

A new screen with the result of the comparison is displayed. Property values that differ in the comparison are highlighted. The property values can be changed by clicking one of the Change <item> ... buttons.

User	Value	Value
User Id	aastra	John
First Name	Dave	Smith
Last Name	Roy	Rachel
Security Profile	Super Uper	End Uper
Department(s)		
Department(s)	AdminDept; aastra	AdminDept; aastra
Preferences		
Use Last Selection	No	Yes
Language	English	English
Service Summa		
Property	Value	Value
Extensions		
Mailboxes		

#### **Searching for Users**

In the User task list view and when adding an administrator, it is possible to search for particular users. In the field, enter All to view a list of all users, User Id, first name, last name, a combination of last name and first name (in that order), extension number or department and click View or Search. Searching for users by only entering the first part of the name is possible. To search on first name only, enter space and then first name. Wildcards can be used, a question mark (?) to replace one character or an asterisk (\*) to replace zero or more characters.

### **Changing Data**

Configuration items can be changed in the following ways:

- From a list view, click (Change). The configuration item is opened and the set values can be edited.
- From a list view, select one or more configuration items and click Change.... Makes it possible to change values for all selected configuration items at the same time. If changing values for more than one configuration item, (Change) enables the field.

⇒

• From a result screen, click Change This.... The configuration item is opened and the set values can be edited.

To restore the previously saved value in a field, that is to undo the

change, click (Undo Change). Click Apply to save and apply the changes.

 $\not \sim$ 

#### **Removing Data**

Configuration items can be removed in the following ways:

• From a list view, click (Remove).

#### • From a list view, select one or more configuration items and click Remove.

• From a result screen, click Remove This.

A pop-up confirmation window is displayed before a configuration item is removed.

### **Printing Data**

Configuration data can be printed in the following ways:

- From a list view, click Print.... Prints the properties of selected configuration items.
- From a list view, click the Print All link. Prints the properties of all existing configuration items.
- From a view details screen, click the Print link. Prints the properties of the configuration item.

Clicking Print..., Print All or Print opens a pop-up window that displays the print preview.

#### Example:

**Printing Security Profile** 

- 1. Go to the Administrators tab and then Security Profile.
- 2. Select items to print.

Note:Select less then ten (10) items.

- 3. Click the Print link.
- 4. A pop-up window opens that displays the print preview.
- 5. Click Print to open the browser print dialog box, make desired selections and print the page.

### **Swapping Equipment Positions**

		Extension 🔩	Server / Equipment Position 🛛 🍫	Extension Type 🛛 🗛	TelephonySystem 🔌
Q	🗙 🖹 🗞 👍	3050	1	IP	WBM85, version 6.1 SP1
90	🗙 🗈 🗞 👍	3051	1	IP	WBM85, version 6.1 SP1
Q /	🗶 🗈 🗞 👍	3052	1	IP	WBM85, version 6.1 SP1
Q /	🗙 🗈 🗞 👍	3053	1	IP	WBM85, version 6.1 SP1

Figure 4: List-view, including the Swap button

- To swap two Equipment Positions, perform the following steps:
- 1. Select two extensions of the same type from the list.
- 2. Click on Swap.

## **Handling Templates**

A template is a set of predefined values that can be used when a new configuration item is added. Templates are used to simplify the process of adding many configuration items with similar property values. Only property values that can be identical for several configuration items can be set in the template. Property values set in templates will not be set in MX-ONE.

Click the Manage Templates link in a task to display the list view with the existing templates for that task. In the list view, the templates are displayed with the defined name, the type, the user that created it, and the date when it was created, for example,

Digital extension\_DigitalExtension (by jsmith, 15/02/08)

#### Creating a Template for a Configuration Item

There are two ways to create a template:

- Create a new template, that is, a template with no predefined values:
  - a. Click the Manage Templates link.
  - **b.** Click Add New... and enter property values in the configuration task where applicable.
  - c. Enter a template name and click Apply to save the template.
- Create a template based on an existing configuration item:
  - a. Click in the list view



b. Enter a template name and click Apply to save the template.

NOTE: Creating a template will not alter any data in MX-ONE.

#### Uploading or Downloading a Template

Templates can be created in one system and transferred to another. To upload a template, click Upload.... To download a template, click (Download). Templates are saved in .xml format.



#### Using a Template to Create a Configuration Item

To use a template to create a configuration item, perform the following:

**1.** Select a template from the list.

Add Using Template: <defa< th=""><th>ult template&gt;</th><th>▼</th><th>Manage Templates</th></defa<>	ult template>	▼	Manage Templates
	ult template>		
Telephony System:	nplate_WBM85_IPExtensio	n (by alacarte, 10/.	2//15)
Extension Type:	IP	•	
Enter Extension Number(s):	All		
	Example: * or 1000 or 1000-1050	or 1000,1500-1700,2	000 or 100*
Enter Equipment Position:			
	Example: 1-0-40-00, 1A-0-40-00		

- 2. Click Add New... and enter property values for the configuration item where applicable.
- 3. Click Apply to save the new configuration item.

### **Using a Multistep Button**

Multistep buttons are 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.

1. To make a detour from task A to task B to edit the values in the drop-down list, click Edit....

	② Location:	Swedan 💌 Edit
2.	Click Add New to add a new configuration iter	n, click (Change) 🥖
	to edit an existing one, or click (Remove) to re	move an existing one. 💢
3.	Click Continue or <- Back to return to task A.	
?	) Location:	Swedan V Edit India Swedan

### **Using Shortcuts**

In the Add and Change pages of the Extension task there is a shortcut dropdown at the top that quickly will take you to the selected task in MX-ONE to which the managed extension belongs. You will get automatically logged in and navigated to the selected task.

### **Using Backup & Restore**

To avoid loosing system data it is recommended to back up system data regularly. Then, if data has been accidentally deleted or corrupted, it is possible to restore the system to the state it was in when the backup was made. All data except subsystem data is backed up. The data is stored on the server that MX-ONE Provisioning Manager (PM) is installed on.

The system can store an unlimited number of backup directories. Each backup directory is identified by a time stamp and the system release version.

When restoring the system, the backup directory must have the same system release version as the installed version of PM. That is, if PM 1.2 is installed it is not possible to use backup directories with version 1.0 or 1.1. Backup directories can still be used to restore the system when a service pack for PM has been installed. That is, if PM 1.0.2 has been installed, backup directories with system release version 1.0, 1.0.1, and 1.0.2 can be used.

All stored backup directories are displayed in a list, including those with system release versions older than the installed version of Provisioning Manager The icon (Restore) is only displayed for the backup

directories that can be used to restore the system.

The process of saving system data during a backup and the process of restoring data during a restore may take a few minutes.

Note: It is not possible to alter system data during a backup or restore.

A backup or restore is performed in the following way:

- 1. Go to the System tab and then Backup & Restore.
- 2. Click Backup to start a backup or click (Restore) to restore the system.

This backup o	only backs up the internal data	abase of	Drovicio						
	and the state of the		PLOVISIO	ning	Manager. To backup the su	ubsyst	ems, please o	jo to t	e subsystem task in Provisioning Manag
								,	,,
ackup Uplo	ad								
Backup Uplo	au								
	Backup with Timestamp		Version	<b>₽</b> ŵ	Last Restore Timestamp	♦	Description	<b>₽</b>	
B> / ¥ (j)		•	Version 5.1_SP1	\$	Last Restore Timestamp	\$	Description	♦	
© / × ₪ ▷ / × ₪		6		<b>∲</b> ∂	Last Restore Timestamp	\$ <sub>\$</sub>	Description	<b>&amp;</b> ç	

**R**adi

## Subsystem Backup

Enables to take the backup of MiVoice MX-ONE subsystem and Service Node Manager data.

The icon (Restore) is only displayed for the backup directories, which is used to restore the system.

The process of saving system data during a backup and the process of restoring data during a restore may take a few minutes.

**NOTE:** It is not possible to alter system data during a backup or restore.

The backup of the Subsystem is performed in the following way:

1. Go to the System tab> Subsystem.

.

- 2. Click Backup icon start a backup of the system. The following Scheduling page is displayed to schedule the backup.
- 3. Select the Enable Scheduling check box to start the schedule backup. Immediate backup of the subsystem is triggered if the check box is not selected.

9	Enable Scheduling: Description:			
	Date Time			
1	Start Date:	*	30 May 2017	
1	Start Time:		18:49	
	Recurrence			
3	Enable Recurrence:			
Ð	End Date:		Date	30 May 2018
			Occurrences None	
3	Recurrence:		Every day	
			Every weekday	
			Weekly	Mon Tue Wed Thu Fri Sat Sun
	Notification			
3	Email Address:			

The created backup files are stored in the /var/opt/eri\_sn folder on the MiVoice MX-ONE and are used when restoring the MiVoice MX-ONE database. You can restore MiVoice MX-ONE and Service Node Manager using the Backup and Restore task in Service Node Manager.

## **Using Compare with Subsystem**

Data inconsistencies can also be caused by subsystem data being modified directly in MX-ONE. Examples:

- extensions are added or removed in MX-ONE but not in MX-ONE Provisioning Manager
- mailboxes are added or removed on the Messaging Server but not in MX-ONE Provisioning Manager
- one of the extensions associated to a user is deleted in MX-ONE while the user's profile in MX-ONE Provisioning Manager is unchanged.

The Compare with Subsystem task is used to compare the PM data with the subsystem data to find data inconsistencies. The result is displayed in a list. Based on the list, the administrator decides what to add or remove in the system, using the corresponding tasks, to synchronize PM and subsystem data.

- 1. Go to the System tab and then Data Management.
- 2. Select which subsystem to compare the PM data with, and maximum number of rows to be displayed per result page. Click View.
- 3.

Cor	npare with Subsy	stem		
Ad	4			
_		_		
	Log Date and Time 🔌	Subsystem Name 😽	Subsystem Type 🛛 🍕	Difference(s)
×	2017/05/30 17:59:08	Abhishek	TelephonyServer	<u>0</u>

4. Click on a post in the Differences column to view the result.

#### Importing Data to MX-ONE Provisioning Manager

The import function in MX-ONE Provisioning Manager is used to add users and departments to the system in two scenarios:

 When migrating existing users and departments from D.N.A or CMG to MX-ONE Provisioning Manager.

Note: For detailed information on how to migrate to MX-ONE Provisioning Manager from D.N.A. and CMG, see Installing MX-ONE Provisioning Manager (9/1531-ANF 901 15).

When adding new users and departments.

#### Importing from D.N.A. and CMG

This is only to be used in when initially setting MX-ONE Provisioning Manager. For details, see Installing MX-ONE Provisioning Manager (9/1531-ANF 901 15).

#### Importing from CSV

User and department data can be imported from CSV files, where CSV is the common acronym for Comma Separated Values. This typically allows for batch input data to conveniently be edited with spreadsheet software. Templates and examples can be downloaded from the CSV import web pages. There is a CSV import option (option CSV file) that can very flexibly process and import much data for each user record. It allows you to connect a column in a CSV to one of many attributes of an PM user. For more information and step by step instructions, see MX-ONE Provisioning Manager Online help.

## **Exporting Data from MX-ONE Provisioning Manager**

Data in MX-ONE Provisioning Manager can be exported for call accounting purposes or for usage in, for example, CMG or other PM installations.

Follow the steps below to export data from PM:

- 1. In MX-ONE Provisioning Manager, click System, Data Managementand then Export. The Export Data page is displayed.
- 2. Click Export....
- 3. Select an export type and click Next.
- 4. In step 2/2, select the data to include in the export, then click Next.
- 5. For exports using CMG data format, specify a definition file (this file is required for correct format of the exported data). Then click Apply to initiate export.
- 6. On the Result page, click Done.

#### **Exporting Data for CMG**

**NOTE:** You may export user data from MX-ONE Provisioning Manager and import it to the CMG if you want to transfer data without enabling the automatic integration between PM and the CMG

The purpose of exporting data in CMG format is if you want to restore CMG with PM data after loosing all CMG data without having backed up CMG.

Normally when operating in PM, CMG will automatically be updated. To synchronize PM with CMG, use the Compare with Subsystem task to find the differences and then update the systems with your corrections.

Data exported for CMG is stored using CSV format. The following PM data is included when exporting data for CMG:

- Department data
- User data.

A user can be associated with several extensions in PM, but only one extension in CMG. For users associated with more than one extension in PM, the export file will contain a separate record for each extension in PM.

For correct export file format, definition files for department and user data are required when exporting data for CMG.

#### **Exporting General Data**

The purpose of exporting data in XML format is if you want to post process MX-ONE Provisioning Manager data in another system.

Data exported as general data is stored using XML format. The following MX-ONE Provisioning Manager data is included when exporting general data:

- Complete department data
- Complete user data
- System data: administrators, security profiles, locations, and subsystems.

### **Exporting Call Accounting Data**

The purpose of exporting data in CAAPI format is if you want to reuse post processing tools as used together with D.N.A. The format of CAAPI is the same as it was for D.N.A. For a more extensive export, please use the XML export format instead.

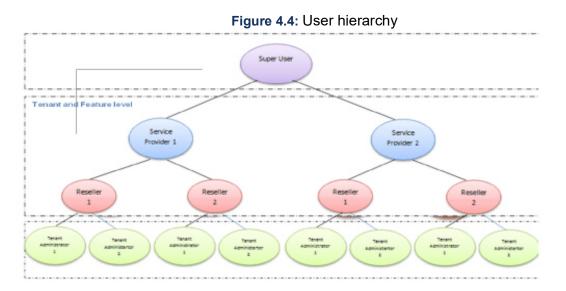
Call accounting data such as account code data can be exported from MX-ONE Provisioning Manager. The following data files are created when exporting call accounting data:

- Account codes
- Authorization codes
- Cost centers
- Departments
- Extensions
- Voice Line Service.

**NOTE:** To get the cost center data into the COSTCEN.DAT file you need to set the UDF Field Type to "COST CENTER" for the applicable UDF in the UDF Mapping task.

The exported files are stored in a .zip file, available for download on the first page of the Export Data task.

## **Tenant and Feature Configuration**



### **Create a Service Provider**

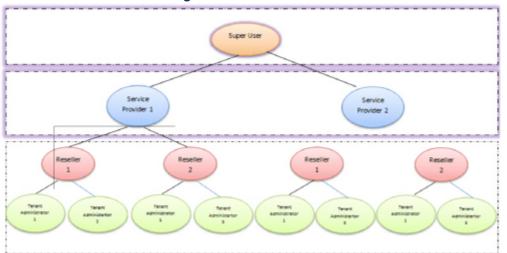


Figure 4.5: Create Service Provider

1. Use the user created in the MX-ONE Provisioning Manager setup, i.e. System Setup Admin, to login to the application.

🕅 Mitel	
Provisioning Manager	
	Mitel
Version : 6.1 SP1	Login
© 2001-2016 Mitel Networks Corporation	

2. Go to Users -> User -> Add a new User.

🕅 Mitel 🕴 Pro	visioning Manager		Logged in as: Mitel About User Guide S	te Vap Logout
Users Services	Administrators System Logs	Own Settings		
User Departments	UDF Mapping Unlock			
User - Add - Step User	1 / 2 // Cent	() Last Name: •	Servicep	
() Uper id: •	Servicep		in any	-
Password: Email Address:	••••••	<ul> <li>Confirm Password:</li> <li>SMS:</li> </ul>		-
Atemate First Names:		Iterate Last Names:		-
() Kaywords: () Departmenti():	Goldting Department(s): Location(s): Company(21)/WHI (Jens: Location(s): Company(21)/WHI (Jensited); Location(s): Company(21)/WHI (Jensited); Jens: witho	<ul> <li>Companyill: Lo</li> </ul>	main	1
to a first second second	t in Selected Department(s) list is primary departme		No. 6 Court	
Profestances	um peretura Departmentis) est la primary departme			
Use Last Selection:	8			
Provisioning Manager Lang	guage: Brylish 💌			

- 3. Check the result.
- 4. Go to Administrators -> Administrator.
- 5. Select the Security Profile "Service Provider" and promote the user to Service Provider.

🕅 Mitel 🛛	Provisioning Manager Lagged in as	Mittal About User Guide Sile Map Logout
Users Senices Administrator Sec	Administrators System Logs Own Settings unity Profiles	
Administrator -	Add	-
Bepartment:     Constanting     Security Profile:     Access to     Department(s):	Bervices -, Company-01     Services -, Company-01     Services -, Company-01     Services -, Company-01     Services -, Company-01     Location(b):     Location(b):     Company-011 (Location(1)     Company-011 (Location(2)     Company-011     Company-011     Company-011     Company-01     Co	Help Administrators have access to tasks used to manage users, services, subsystems and so on. An administrator is a prometer of the administrator can access tagende on the access prelegies included in the administrator's security profile.
Access to Subsystem in Location(s):	V e- V	Administratory can peuter action an

- 6. Check the result.
- 7. Repeat the earlier operations in order to create new Service Provider.

### **Create a Reseller**

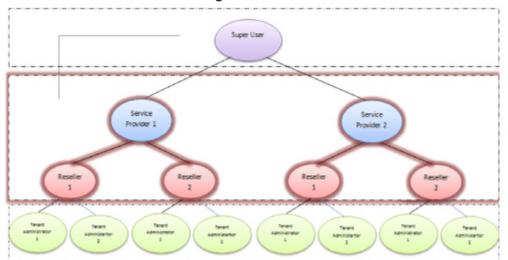


Figure 4.6: Create Reseller

1. Logon with one of the Service provider Credentials.

🛤 Mitel		
Provisioning Manager		
		Servicep
		******
Version : 6.1 SP1	×	Login
© 2001-2016 Mitel Networks Corporation		

2. Go to Users -> User -> Add a new User.

Mitel Prov	visioni	ing Manager		Logged in as: Servicep	About User Guide	Site Map	Logest
Users Services	Administr	rators System Ov	un Settings				
User Departments	Unio	ch					
User - Add - Step 3 User • lock (red - Step 3 (App) () Prot Name	_	ai	🕐 Last Name:	Papsler			
	Receiver					_	
Password:			Confirm Paseword:     O SMS:			_	
Alternate First Names:			Alternate Last Names				
3 Keywords:							
① Department(s):		Eviating Department(a): Location(a) Company(1)/VEM Users(Location(a) Company(1)/VEM Users(2): Location Company(1)/VEM Users(2): Location Company(1)/VEM Users(2): Location	40 Company()	esetwert(n): Location(n):	Realize Realize		
Note: The first department	in Selecter	d Department(s) list is primary depart	timent				
Use Last Selection:     Provisioning Manager Lang	uege:	English 💌					

- 3. Check the result.
- 4. Go to Administrators -> Administrator.
- 5. Select the Security Profile Reseller and promote the user to Reseller.

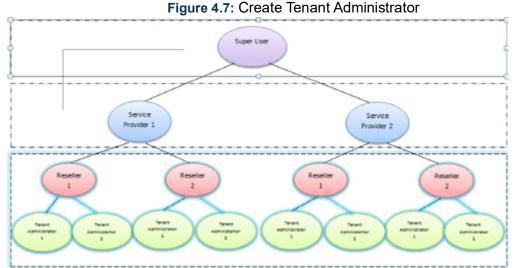
ers Services	Administrators	System	Own Settings					
ninistrator								
Administrator -	Add							
Apply Cancel								_
<ul> <li>User Name(x), Extension Number, Department:</li> </ul>	* Reselier	(sect.)					Help	
Security Profile:	<ul> <li>Reseller - Reselle</li> <li>Reseller</li> </ul>	<ul> <li>Reselver, Company</li> </ul>	91			Administrator		
Amess to Departmentiol:	* Existing Departmen Location(s):	4(x).		Selected Department(s), Location(s);		Administrators have to manage users, se and so on. An admin promoted user with	ervices, subeystem ristrator is a	18
	CompanyII1; Locatio CompanyII1WIM U CompanyII1WIM U	whic Location()] whilest, Location()	department: Location(1)			profile. What the ad- access depends on t included in the admir profile.	ministrator can the access privilege	21.9
	Comparison (come of	and a feature in the second			Here Doort	Administrators can n	wver assign an	
Access to Subsystem in Lacation(S):	nd • Ni ·					access privilege to a administrator that th easigned themselve only assign a securit user or administrator assigned to them, or privileges.	hey have not been a. Administrators of by profile to an end or with the privilege	d d
						The following seven predefined:	security profiles an	

- 6. Check the result.
- 7. Repeat the earlier operations in order to create another Reseller.

NOTE: One Reseller data cannot be seen by other resellers.

Parent can view all the child's data

#### **Create a Tenant Administrator**



- 1. Logon with one of the Reseller Credentials.
- 2. Create the tenants and the respective number series.

🔀 Mitel 🕴	Provisioning Man	ager				Logged in as: Reseller	About	User Guide	Site Map	Logout
Users Services	Administrators	System	Logs Tenant	Own Setti	ngs					
Tenant Configuration	Feature Level Mapping									
Tenant Configur Apply Cancel	ation - Add									Help
Testat Configurable 0 Telephony System: 0 Customer Hame: 0 Actorner Hame: 0 Actorner Hame: 0 Donan Name: 0 Donan Name: 0 Bestict Terminal Ragi 0 Restict Terminal Ragi 0 Restict Terminal Ragi 0 Excepton for Daling 0 Restict Terminal Ragi 0 Directory Numbers: 10 Common Abbrevietled 10 Enable Number Dala a Institate Subscribers	stration from Foreign IP domai ormat: Numbers: even Customers: Numbers: nd Initiate Subscribers:	192 168 28 11     DEFAULT •     DEFAULT		Feature level basic •	Dialing Privileges Internal • Internal •	End May Device Type Mills (462) -	To s form clici This thro deta On 1 Nun Sub	nant config see help informant and options the <sup>10</sup> Help is is the first scruen you be contained to the scruen you be contained to the scruen you be contained to the scruen be contained to the scruent scruent you have a scruent be scruent you have a scruent have a scruent you have a scruent you have a scruent have a scruent you have a scruent you have a scruent have a scruent you have a scruent	for a specific p for a specific p ion. een that will gu ant Configurati add the Custor Name and Initia ustomer Number me mbers	oe, property, ide you ion mer ate er:
			1.	basic • basic •	Internal • Internal •	Mitel 6863i • Mitel 6863i •				
Apply Cancel										

3. Configure feature levels.

Reseller can provide alias names for the feature level licenses defined in MX-ONE.

🛪 Mitel	Provisioning	a Manager			Logged in a	Logged in as: Reseller		User Guide	Site Map	Legent	
ters Sené	ces Administrato	ra System	Tenant	Own Settings							
mani Configuratio	n Peature Level	Hassing									
Feature Lev	vel Mapping									н	
Feature Level	Mapping										
(B BASIC	Gold										
BASIC     BASIC     BORDLESS     BON     BURRDENCY	Gold Bilver Brance energency	1									
BAGEC  CORDLASS  CONDLASS	Gold Bilver Bronze	L	ł								

4. Go to User -> Add a new User.

Tenant created by the reseller in the tenant configuration page will appear in the User page.

🗙 Mitel 🕴 Pr	rovisioning Manager		Logged in as: Reseller About User Guide S	ite Map Logo
bera Services	Administrators System Tena	ant Own Settings		
ber Departments	Unlock			
User - Add - Step User - Not - Not - A	1 / 3 spoty Cancel			
First Name	Tedmin	(B Last Name -	(1998) (B)	
UserId: Password:	Tadmin	Customer:     Confirm Password:     B    Execution	Pitel w	-
Password:     Password:     Password:				-
Alternate First Names:		Alternate Last Names:		-
Keywords:				
③ Department(s):	<ul> <li>Existing Department(s): Location(s):</li> </ul>		artment(s); Location(s):	
	Company Cylline Terry, Cocosoto Company Cylline Terry, Technical Company Cylline Terry Statistics Company Cylline Terry Statistics		Restances Restances	
I Note: The First department	ent in Selected Department(s) list is primary departm		The second	
Preferences				
O Use Last Selection:	2			
Provisioning Manager La	anguage: Baglah M			

- 5. Check the result.
- 6. Go to Administrators -> Administrator.

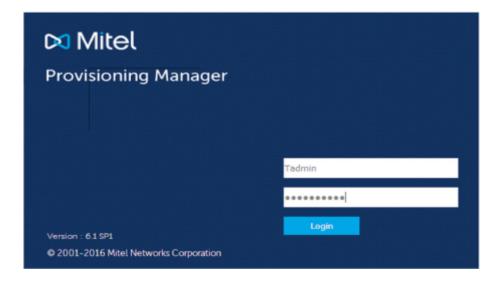
Select the Security Profile as Tenant Administrator and promote the User as Tenant Administrator

ers Ser	vices	Administrators	System	Tenant	Own Settings						
ministrator											
Administra	ator - Ad	bb									
Apply Cent	ei .										
<ul> <li>User Name) Butension R Department</li> </ul>	anbec	Tadne	- Inert					-	1400	,	
(b) Security Proj	Mar.	Tadmin , Tadmin 1     Tenent Administrator		1				Administ			
Access to Department	(4)+	Boisting Departmen Location(c): Compeny01: Location Compeny02:W0M Up Compeny02:W0M Up Compeny02:W0M Up	tiel. 61. ers: Location01 ers/best: Location01	t depertment: Loc	ation01	Selected Geostmentis), Location(x):	Meetin	to manage of and selen. A promoted up profile, toha access depe	aters, service in administra- ser with an a title administration inds on the	seeigned securi	e Ry
Access to Its In Location()		Location01				*	Mara Sant	assigned the only assign user or adm	ege to a use or that they i emperves. As a security pr inistrator will		an I
								The followin predefined.	-	unity profiles an	

- 7. Check the result.
- 8. Repeat the earlier operations to create another Tenant Administrator.

#### **Create a Tenant**

1. Login with one of the Tenant Administrator Credentials.



2. Go to Users -> User -> Add a new User.

Company010VBH Users: Location01 Company010VBH Usersided: Location0			
ol			
	Last Name:     A Customer:	Triever	
	Conten Password:	Pitel	
	3 949		
	Alternate Last Names:		
Company01/WWH Usersidest: Location01	Compandia La		
(C) Id Department(s) fist is primary department (2)	2	Berta Verkim	
	Company(1) WHI Users: Location(1) Company(1) WHI Users(bet) Location(1) Company(1) WHI Users(bet) Jikers without all Department(2) But is primary department	Abernate Last Harres:      Distring Department(a): (cestion(a):     Company(1)(WH) (sees: (cestion(a):     Company(1)(WH) (sees: (cestion(a):     Company(1)(WH) (sees: (cestion(a):	Abenata Last Hames:      Desertment(b): Location(s)     Gregorithe(Location(s))     Gregorithe(Location(s))

3. Configure the tenant.

Tenant Configuration page is used to create the number series for the single customer.

🕅 Mitel 🛛	Provisioning	Manage	er			Log	iged in as: Tenantadmin	About	User Guide	Site Map	Logout
Users Service:	System	Logs	Tenant	Own Settings							
Tenant Configuration											
Tenant Config Apply Cancel	juration - Add										Help
Common Abbrevia     Clastomer Humber     Customer Humber     Customer Humber     Customer Humber     Common Kamer     Denain Owner:     Partetict Terminal     Enable Short User     Derectory Number     Cammon Abbrevia	: : Doformat: ing Numbers: between Customers: ::	• P domeins:	192.168.28.112 80 cut600 DEFAULT • Ø Ø Ø 10 Edit 6001-6002 6002 6002-6011					To s form click This thro deta On t Num Sub:	ee help informal at and options the <sup>(17)</sup> Help ic is the first scre ugh adding Ten ils. his screen you : ber, Customer f	en that will guide ant Configuration add the Customer lame and Initiate stomer Number: mber me abers	ierty,
⑦ Enable Number Da Initiate Subscrit	ta and Initiate Subscribers eers		Ø Number Range	Server 1 * 1 * 1 *	Feature level basic • basic • basic • basic •	Dialing Privileges Internal • Internal • Internal •	End User Device Type Mitel 68631 • Mitel 68631 • Mitel 68631 • Mitel 68631 •				

4. Logout the Tenant Administrator login and logon with Tenant Viewer [End User] Credentials.

▶ Mitel Provisioning Manager	
Version : 61 SP1 © 2001-2016 Mitel Networks Corporation	Tviewer ••••••••••• Login

# Setup a New MX-ONE PM to Monitor Different Sites

The MX-ONE Provisioning Manager Admin users shall be given either the cloud or CPE rights.

PM in cloud mode allows Service Providers and Reseller to setup systems that are using feature level model.

PM in CPE model is the same as in the previous versions of PM, except that a new user needs to be created to manage the system.

The new user hierarchy is composed by several levels and they are divided basically in the two types of MX-ONE business models, Cloud or CPE (á la carte). A main user is created during the installation of PM and this user is used to create new users and assign the current service profile that fits the system type.

For example, a customer that is running MX-ONE in CPE license model will assign a user as AlaCarte Service Provider.

Figure 4.8: User Hierarchy

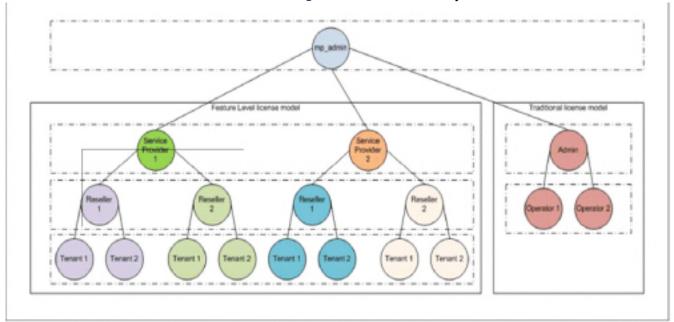
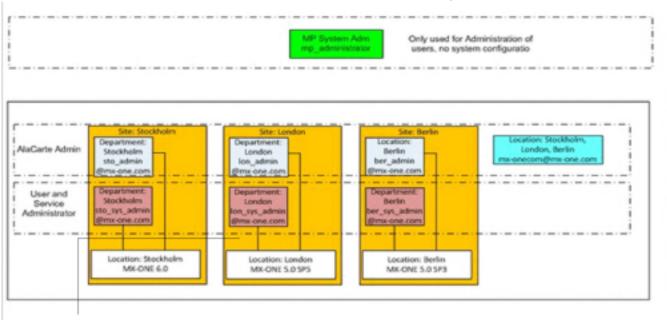


Figure 4.9: User hierarchy



# **CPE Mode Setup**

Assumptions:

- New PM
- 3 sites
- · Users local in the site only see information of their own site

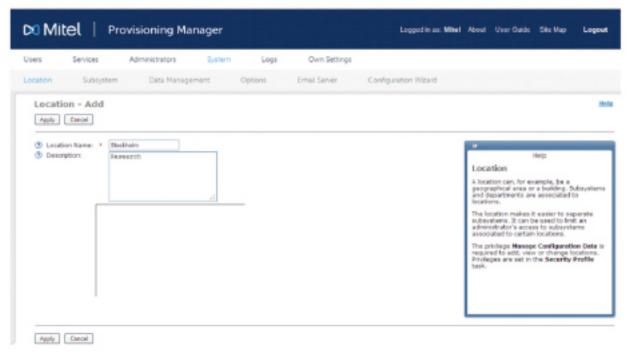
- A corporate admin, can see information from all 3 sites
- 1. Use the user created in the MX-ONE Provisioning Manager setup, i.e. System Setup Admin User, to login to the application.

Figure 4.10: Login page

🖂 Mitel	
Provisioning Manager	
	Mitel
	•••••
Version : 6.1 SP1	Login
© 2001-2016 Mitel Networks Corporation	

2. Go to System, Location and define the locations.





3. Check the result.

#### 4. Go to Users, Departments and define the Departments.

Repeated for each location.

Users	Services	Administrators	System Logs	Own Settings		
lser	Departments	UDF Mapping	Unlock			
Add Rafin	artments	Coloren	<ul> <li>Department Name:</li> <li>Parent Department:</li> <li>Eccation:</li> <li>Description:</li> </ul>	Niteri Iscattoreta V		
			Apply			

**NOTE:** The Department Name can now hold up to 64 alphanumerical and special characters both. But, the characters such as ", \*, ?, \, < and > are not allowed.

1. Check the result.

🕅 Mi	itel   Pr	rovisioning Man	ager			Logged in as: Midel	About	User Guide	Site Map	Lagout
Users	Services	Administrators	System	Logs	Own Settings					
User	Departments	UDF Mapping	Unlock							
Depa	rtments									Hele
	oply operation au pertments : IR	accessful for:								_
	Remove Expand	Cultapor								
Refresh	/Synchronize									
0 (m)	itel	4 Pains Paine	(D) Par	partment Name: rent Departmenti	HR Milel W					
	101		(1) Los (1) Des	sation:	Stochheim 💌					
				7						
			-144							

2. Go to Users, Users and add a new user, select the correct department.

🛤 Mitel   Pro	visioning Manager		Logged in as: Mitel	About Uner Guide	Sile Map Logout
Users Services	Administrators System Logs	Own Settings			
User Departments	UDF Mapping Unlock				
User - Add - Step User	er Censel	(B) Last Name: •	(all sends		
<ul> <li>First Name:</li> <li>User 1d:</li> </ul>	Alacarte Alacarte	(p) Last Name:	Alacarte		
<ul> <li>Pasaword:</li> <li>Graal Address:</li> </ul>	•••••	Confirm Passworth     Ø SMS:			
<ul> <li>Alternate First Names:</li> </ul>		Alternate Last Names:			_
(3) Keywards:					
(bepartment(s):	Enipting Department(b): Location(b):     Pron/All; Stockholm:	>	meent(i): Location(ii):	Here is a	
Note: The first department Professions	t in Selected Department(s) list is primary department	R			
O Use Last Selection:					
Provisioning Manager Land	quage: English w				

3. Check the result.

4. Go to Administrator Menu, Administrator and add the create user to a service profile.

DI Mitel Provisioning Manager	Logged in as: <b>Wite</b> l About User Guide	Ste Map Lagout
Users Services Administrators System Logs Own Settings		
Administrator Security Profiles		
Administrator           Image: The second sec		Poliet.AM media

5. Select the Security Profile, Access to Departments and Access to Subsystems in Locations.

Mitel   Provisioning Ma	nager Logged = as: N	Hell About User-Guide Sticklep Legout
isers Services Administrators	System Logs Own Settings	
dministrator Security Profiles		
Administrator - Add		-
🛞 User Nameta), Entension Number, Department:	* Alexente	нер
Security Profile	* AlaCarla Service Previder 🖌 Vievs Bill	Administrator
() Access to Department(3):	Existing Department(i), Location(ii), Alter(M), Studialm , Material (M), Studialm , C	Administration flow access to taking used to memory over the events information and except users with an assigned exceptor previously user with an assigned exceptor prefile. What the administrator can arenes observed on the acress provideges included in the administrator's security prefile.
Access to Subsystems in Location(s):	Advances of A Standholm	Administrators can never assign an access privilege to a user or administrator that their have not been assigned themselves, administrators can enty assign a security profile to an end user or administrators with the privileges assigned to these, or a subset of those privileges.
		The following seven security profiles are predefined

6. Check the result.

🖂 Mil	tel	Provisioning M	anager			Logged in an: Mitel	About	User Guide	Site Map	Logout
Users	Senioes	Administrators	System	Logs	Own Settings					
Administrato		Security Profiles								
Admin	istrator								Rd	int.All Hele
[ A69 ]										
		User Di 🍬 First Name 🕈								
82		Macarte Macarte	Macarte	AlaCarte Bervi Bystem Betup						
Chang	e. Ser	eve Print Compare	View							

7. Logout Administrator and do logon with new user.

8. Add the subsystem and select the location, if the setup is correct, only one appears.

rs Services Adminis	rators System Logs Own Settings	
riton Subsystem De	ta Management Options Email Server Conf	iguration Wizard Batch Operation
Subsystem - Add		
B Subsystem Type: B Use WTTPS:	Telephany Bystem	14 Help
Bubayaten Name	Bandhalm - HK-DAB	Subwystern
B version:	6.1 SP1 W	Missice Mx-ONE comprises a number of
3 12 Address	192.165.25.30	components, such as CM3, OneBax, MMC, MiCollab Server/SIP DECT Henager
D PDC:	194	and Hilvoice Mil-CAB. By adding the servers on which the components run as
<ul> <li>User to in Subsystem:</li> <li>Password in Subsystem:</li> </ul>	Prised	subsystems in Provisioning Manager
Confirm Password in Subsystem:		user accounts and services related to the subsystems can be managed using
Tarminal Password		Provisioning Manager as 5 single coint of entry, beveral subsystems can be
Confirm Terminal Password		installed on the same server, including the server on which Provisioning
B IP Phone Server:	Enter Hansel URL M	Hanager run.
B Domain Folder:	*	When adding a subsystem, Provisioning Manager is provided with user
D Location:	Loosienii) - Cat	oreceivants trust are valid for togging on to the subsystem. These andwardshi are used, in the background, by Prevensioning Managar when server-missiony with the subsystem. This accommended that an

- 9. Check the result.
- 10. Check the result by clicking the subsystem link (Stockholm MX-ONE).

lsers	Services	Administrators	System	Logs	Own Settings					
ocation	Subsystem	Data Manag	ement	Options	Email Server	Configuration Wigard	Batch	Operation		
Subsys	netern								int All	Hall
Add										

11. Access the subsystem that you created on the previous slide and logout.

🛤 Mitel	Service No	de Manager				Logged in as: Alacarte	About	Uter Guide	Site Map	Logout
Initial Setup	Number Analysis	Telephony	Senices	System	Toois	Logs				
Welcome										
This application has For user settings p	ndies the system setting issue use the "Mytics P	as for the MiVolce MiLL In-Chill Provisioning M	INE Service Node. tanager' application	n.						

12. Repeat the operations for all users and sub-systems

Check if everything is correct and that the 3 users cannot see the others systems.

- 13. Using the "local admin" account create a new user and select the correct department
- 14. Check the result.
- 15. Select the Security Profile, Access to Departments and Access to Subsystems in Locations
- 16. Check the result.

# **End User Profile Settings to Monitor Group Data**

Log in to PM with system setup admin privileges, change the End user profile, and assign "End user group service role" to monitor group handling for end users.

Figure 4.12:	Change scr	een for End	user security	profile

Mitel Provisioni	ing Manager				Logged in as: Mitel About	User Guide Site Map	Logout
sers Services Administr	rators System Lo	gs Own Settings					
dministrator Security Profiles							
Security Profile - Change	- End User						He
⑦ Security Profile Name: *	End User						
<ul> <li>Description:</li> </ul>	Access to end user self service web interface						
Privileges							
<ul> <li>Privileges</li> <li>(?) End user self service:</li> </ul>		⑦ End user group service:	✓				
<ul> <li>Manage configuration data:</li> </ul>		<ul> <li>Manage user data:</li> </ul>					
<ul> <li>View user data:</li> </ul>		⑦ Manage service data:					
<ul> <li>View service data:</li> </ul>		⑦ Manage administrators:					
View administrators:		⑦ Manage security profiles:					
<ul> <li>View security profiles:</li> </ul>		Import/Export user data:		団			
Auto unlock:		⑦ Manage UDF data:		X			
③ SNM: Manage advanced feature:		③ SNM: Command line interface:					
③ SNM: Manage extension data:		⑦ View subsystems:					
⑦ Tenant configuration data:		⑦ AlaCarte:					
⑦ Feature level configuration data:		⑦ View logs:					
⑦ Manage individual diversion:		⑦ Manage available extensions:					
⑦ Manage Batch Operation:		③ SNM: View Logs:					
③ SNM: Manage Secure Data:		③ SNM: Backup:					
③ SNM: IP Phone Configuration:		⑦ Manage Secure Data:					
⑦ Manage Featurebased System:							

Log in to PM with end user privilege. The features under group setup heading shown in the figure below, can be configured by the end user.

Mitel Provision	ing Manager				Logged in as: Mitel About User Gu	ide Site Map
ers Services Administ	rators System Log	gs Own Settings				
ninistrator Security Profiles						
Security Profile - Change	- End User					
Apply Cancel	End ober					
Appiy Cancer						
<ul> <li>Security Profile Name: *</li> <li>Description:</li> </ul>	End User Access to end user self service web interface					
Privileges						
② End user self service:		② End user group service:	<b>V</b>			
⑦ Manage configuration data:		⑦ Manage user data:				
View user data:		⑦ Manage service data:				
⑦ View service data:		⑦ Manage administrators:				
⑦ View administrators:		⑦ Manage security profiles:				
⑦ View security profiles:		⑦ Import/Export user data:		X		
Auto unlock:		⑦ Manage UDF data:		8		
③ SNM: Manage advanced feature:		③ SNM: Command line interface:				
SNM: Manage extension data:		View subsystems:				
⑦ Tenant configuration data:		⑦ AlaCarte:				
⑦ Feature level configuration data:		View logs:				
⑦ Manage individual diversion:		⑦ Manage available extensions:				
⑦ Manage Batch Operation:		③ SNM: View Logs:				
③ SNM: Manage Secure Data:		③ SNM: Backup:				
③ SNM: IP Phone Configuration:		⑦ Manage Secure Data:				
⑦ Manage Featurebased System:						

# System and Error Messages

MX-ONE Provisioning Manager provides system messages and error messages directly or when a configuration item is submitted. An icon is displayed together with the system information.

Figure 4.14: Error messages



Figure 4.15: Information messages

Session has expired! Please login again

Figure 4.16: Acknowledge messages

Restore operation successful for:
 Backup with Timestamp: 2012-05-02 21:19:47

This message type can be displayed for procedures including several sub-procedures, where one or more sub-procedures might be non-successful. Rollbacks are performed for non-successful sub-procedures

	Figure 4.17: Other messages				
🖌 Cha	Change operation partly successful for:				
• User	Id: John				
X	hange oper	ration failed for:			
		Reason: Not initiated or not supported	Field: Extension / Telephony Syster		

For certain operations a pop-up window is displayed, please see the following example for invalid template name.

#### Figure 4.18: Pop-up message



### Logs

MX-ONE Provisioning Manager provides three logs with different information level:

- Audit trail: Information about all changes made by a user in the system
- Event Log: System log information useful for fault tracing
- Security Log: Information about successful and unsuccessful login attempts

Log files are created every day even if no data is logged. Logs older than 90 days are overwritten.

#### Changing the Log Level

If not enough or too much information is displayed in the logs in the Logs task, the wrong level for the logging is set in the configuration file jboss-log4j.xml. The configuration file is stored on the server that MX-ONE Provisioning Manager is installed on.

The following log levels are available:

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

To change the log level, follow these steps:

- 1. Go to opt/jboss/server/default/conf and open the file jboss-log4j.xml.
- 2. Edit the log level in the following row: <category name="se.ericsson.ebc.mp"><priority value="INFO" class="se.ericsson.ebc.emtsn.util.log.XLevelTrace"/> <appender-ref ref="MP"><category>
- 3. Save the file. After approximately one minute the new log level configuration is applied.

# **Post-Installation Configuration Tool**

To start the tool, enter one of the following commands in a shell connected to the server:

- If logged in as root, enter the command mp\_config.
- If logged in as eri\_sn\_admin, enter the command sudo -H mp\_config.

# **MX-ONE Provisioning Manager Interface with WebSEAL**

### General

The Provisioning Manager is used to manage and administer the Mitel MX-ONE communication system. This enables you to connect the IBM WebSEAL to the Provisioning Manager for having a centralized access management.

### **Requirements**

IBM Tivoli Access Manager WebSEAL can be used for SSO authentication to log on to applications. The purpose is to register with the PM via WebSEAL.

# WebSEAL

WebSEAL is a high-performance, multi-threaded web server that applies a fine-grained security policy to the Tivoli Access Manager protected Web object area. WebSEAL can provide SSO solutions and incorporate resources from a back-end web application server into its security policy.

To get more information on IBM Tivoli Access Manager and WebSEAL, click the following link:

https://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1134-01/en\_US/HTML/amweb41\_admin04.htm

### **Connection to the Provisioning Manager**

WebSEAL connects to the PM with the establishment of a junction. A junction enables WebSEAL to provide the services (PM) used to the client protected.

To get more information on IBM Tivoli Access Manager and WebSEAL, click the following link:

https://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1359-00/en\_US/HTML/am51\_web-seal\_guide16.htm

To create the junction for the PM, use the following values from the table in WebSEAL.

Name of the Junction	/mp
Junction Type	Transparent path
Scripting Support	No
Back-end Server	
Server Type	Apache
Connection Type	Mutual ssl
Host-name and IP	Host-name and IP of the PM
Port	443
Transfer Parameters	
iv-user	Yes
LTPA2-Token	No

Host name and IP refer to the service to be protected (PM). The IV-User Header is used as transfer parameter for the service PM. The service (PM) evaluates the IV user header and determines the login data from this.

### PM webserver\_configuration for login via WebSEAL

For protection against misuse, the FQDN of the WebSEAL server is stored in the PM. The configuration is done by webserver\_config tool.

To login via WebSEAL, do the following:

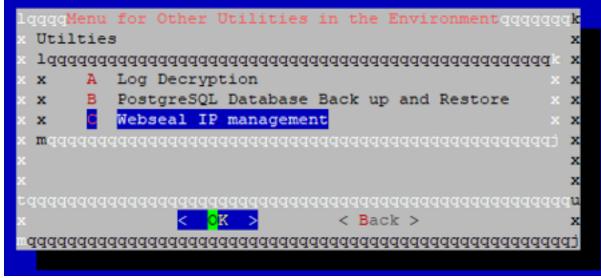
1. Enter the command sudo -H webserver\_config. The following screen appears.

Figure 4.19: Other Utilities

MX-ONE Provisioning Manager (PM) Configuration - webserv qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq	
	qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
	nfigure web server x
	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
x x	A Configure web protocol to http or https. x x B Configure AD authentication. x x
· · · · · · · · · · · · · · · · · · ·	C Root Certificate Management
x	D Check Configuration
A A A A A A A A A A A A A A A A A A A	E Collect Diagnosis
x x	F Re-start webserver (Application PM) x
× ×	G Change TLS Level for HITPS x
× x	H Enable or Disable of Encryption of Environment x
x x	I Redundancy x
x x	J Package Management x x
× ×	K Heap Memory Management x
x x	L Other Utilities x x
	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
	X
	*
	aqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
aa	999999999999999999999999999999999999999

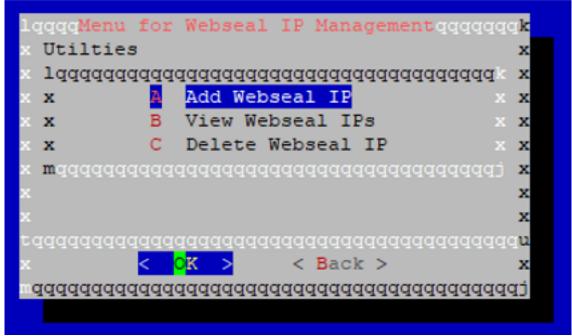
2. Select J for Other Utilities and Click OK. The following screen appears.

#### Figure 4.20: WebSEAL IP Management

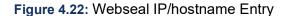


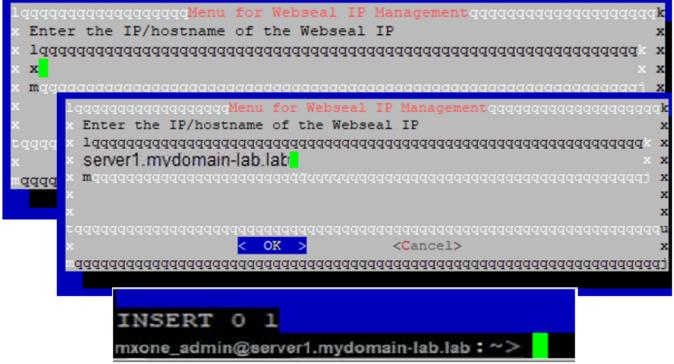
3. Select (C) for Webseal IP management. Click OK. The following screen appears.

Figure 4.21: Add WebSEAL IP



4. Select (A) to enter the address of Add Webseal IP and click OK. The following subsequent screen appears.



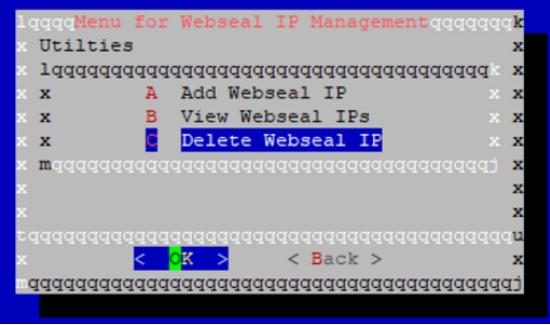


5. Enter the required IP address or the FQDN details.

The webserver\_config tool acknowledges the entry with **INSERT 0 1**, the tool webserver\_config is closed. A check for validity of the entered values does not take place.

6. Click OK. The following screen appears.





- 7. Select (C) Delete WebSEAL IP to delete the existing configuration IP details.
- 8. Click OK. The following screen appears acknowledging that the deletion takes place without inquiry.

Figure 4.24: Delete Input



The webserver\_config tool acknowledges the input with DELETE 1, the tool webserver\_config is closed.

### **Registration via WebSEAL**

To log in to the PM via WebSEAL, do the following:

1. Open the Corporate WebSEAL URL in a browser. The Corporate log in page will be displayed. The use must type the credentials.

After successful authentication, if the user is known in PM, the login takes place. The PM only allows login via the IV user header if the FQDN of the WebSEAL server is stored in the PM.

🔀 Mi	tel   P	rovisioning Ma	nager			Logged in as:	About	User Guide	Site Map	Logout
Users	Services	Administrators	System	Logs	Own Settings					
Welco This appli		user settings for the MiVoi	ce MX-ONE.							

## Figure 4.25: PM Welcome Page after Successful WebSEAL Registration

# **MX-ONE Provisioning Manager integration** with **MS Active Directory**

# Introduction

The purpose with this document is to describe the integration between Provisioning Manager (PM) and Microsoft Active Directory, (AD) in MX-ONE 7.0.

When a user is added, changed or removed in the AD by the system administrator, PM will be automatically notified to update the MX-ONE System accordingly. PM can be set to only handle user accounts in PM and CMG, or to also handle extensions and mailboxes in the MX-ONE System and MiCollab Advanced Messaging (AM) servers.

The integration with AD is a one way communication. AD notifies and passes data to PM. PM does not operate on AD. There are no schema changes or extensions/additions required in AD. AD is the master except for extensions.

Extensions can be added and updated but removal of extensions can only be done from PM for a specific user.

Only default fields in AD will be used by PM to create, update and remove user accounts. Additional AD fields can be mapped as User Defined Fields (UDF) in PM and hence extend the number of fields to import.

A PM template can be assigned to one of 4 telephony fields in AD so as to enable IP extensions to be created for a user according to the rules defined in the associated template. See AD - PM Field Mapping for more details.

Multiple IP templates can be used to extend the number of MiVoice MX-ONE for one AD server.

An optional way to determine which MiVoice MX-ONE the extensions are created in is to use the Telephony System Mapping.

Only IP extensions can be created and managed from AD since the other extension types requires additional data that don't have corresponding fields in the default setup of AD, such as equipment positions, IPEI numbers etc. To handle IP extensions, IP extension templates and Multi terminals templates need to be defined in PM and configured in the AD task in PM, please see the PM Active Directory configuration section below.

The figure below shows the connections between AD/PM and MiVoice MX-ONE/MiCollab AM/CMG

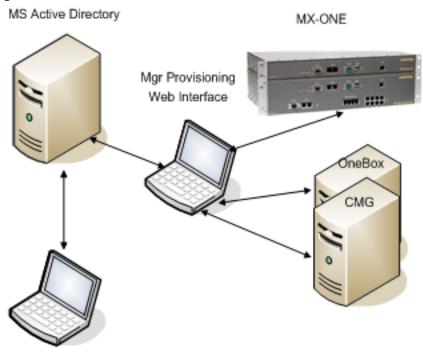


Figure 5.1: Connections between AD/PM and MiVoice MX-ONE/MiCollab AM/CMG

IT Admin User Management

### Scope

The document describes the following:

- AD Integration setup
- Functionality
- Limitations

# **Target Groups**

This document is intended as an overview of the Provisioning Manager integration possibilities with Microsoft Active Directory and is targeted towards the system administrators of both the MiVoice MX-ONE and the Microsoft Active Directory system.

# **Functionality**

# Overview

There are two modes of integration:

- Manually triggered synchronization
- Automatic notification

The manual synchronization is used to initially move all existing AD users to PM, or to update PM if there has been a malfunction in the AD – PM connection.

The automatic notification is the normal mode of operation. When AD is updated PM gets notified and will act according to its setup.

In the PM User task, you can see if a user has been created from AD or through PM locally.

In the PM Active Directory task, you define the connection to AD, rules for operations and which parts of AD to synchronize with.

The search domains and IP number templates can be configured from the Active Directory task by selecting the **Configure Domains** tab.

The online help provides details to the **input** fields as well as a general overview.

Certain tasks need to be done in a specific order for the AD integration to work correctly. The recommended work flow to set up AD is as follows:

- 1. Create user in AD. See Active Directory Connection Setup for more details.
- 2. Create IP extension templates in the PM Extension task to be used when creating IP extensions, if automatic creation of extensions is desired in the Telephony System.
- 3. Ensure that the number series are set up in the Telephony System through Service Node Manager.
- 4. Configure the PM Active Directory task. See Active Directory Connection Setup and PM Active Directory Task for more details.
- 5. Execute a manual synchronization on each defined Search Domain.
- 6. Activate the automatic notification function for each Search Domain.
- 7. To find information about the synchronization, see the audit trail log and the event log. The logs will be automatically updated in case of an event from AD. It is therefore strongly recommended to frequently read the logs.

# **Active Directory Connection Setup**

A user must be created in AD that is a member of Administrators and Domain Users. This user with its password shall be entered in the AD task together with the AD IP address and port to set up the AD connection.

AD can be organized to group its users in different domains defined by their distinguished names, usually according to geographical locations. In PM they are referred to as Search Domains, i.e. the AD areas where PM shall be updated from. In PM you can define multiple Search Domains and manually synchronize them individually as well as enable and disable the automatic notification function.

Each AD domain can be configured to support multiple MX-ONE systems.

# AD – PM Field Mapping

AD fields to be used in PM for setting up extensions:

#### Table 5.1: General User Information with fixed mapping

AD FIELD	PM FIELD
Given-Name (givenName)	First Name
Surname (sn)	Last Name
SAM-Account-Name (sAMAccountName)	User Id

Table 5.2: AD Number Field information mapped to a specific field in a PM Template

AD FIELD	PM FIELD
Telephone-Number (telephoneNumber)	Extension data based on selected template
Telephone-Number-Other (otherTelePhone)	Extension data based on selected template
Phone-IP-Primary (ipPhone)	Extension data based on selected template
Phone-Ip-Other (otherIpPhone	Extension data based on selected template

Table 5.3: AD Number Field information mapped to a specific field in a PM Template (Sheet 1 of 2)

AD FIELD	AD ATTRIBUTES
Initials	Initials
Display Name	displayName
Description	description
Office Location	location
Web Page Address	wWWHomePage
Web Page Address (Others)	url
Street	streetAddress
Post Office Box	postOfficeBox
City	I [Locality-Name]
State/Province	st
ZIP/Postal Code	postalCode
Country	C [Country-Name]
User Logon Name	userPrincipalName
Phone Number (Others)	otherPhoneNumber
Account is Disabled	UserAccountDisabled

	1
User Must Password Change at Next Logon	Pwd-Last-Set **
User Cannot Change Password	UserAccountControl
Account Never Expires	UserDontExpirePassword
Account Expires (Use same data format as server)	accountExpires
Profile Path	profilePath
Logon Script	scriptPath
Title	title
Department	department
Company	company
Manager	manager
Fax	facsimileTelephoneNumber
Fax (Others)	otherFacsimileTelephoneNumber
IP Phone Number	ipPhone
IP Phone Number (Others)	otherlpPhone
Room Number	roomNumber
Secretary	secretary
Assistant Name	assistantName
Mobile Number	mobile
Mobile Number (Others)	otherMobile
Notes	info
Employee ID	employeeID
Employee Number	employeeNumber
Home Phone Number	homePhoneNumber
Home Phone Number (Others)	otherhomePhoneNumber
Telephone Number	telephoneNumber

#### Table 5.3: AD Number Field information mapped to a specific field in a PM Template (Continued) (Sheet

The above table indicates that up to four different AD number fields can be associated to the same template or each of the four AD number fields could be used with different templates. In most situations, only one PM template is used and it is associated to 'Telephone-Number' field in AD. The other three AD number fields would be optional fields used to define additional numbers to the primary number for that user.

Associating a different template to any of the other AD number fields can be used to differentiate between users in different MX-ONE systems in the same PM. In this case, then only the corresponding AD number

fields associated to a given template must be filled in. If you fill in two AD number fields associated to different templates, this would result in creating extensions for the same user in two different systems.

A PM template dictates the detailed settings for the extension when creating it in the MX-ONE Service Node. The number entered in an AD number field will be attributed the settings from the mapped template when PM then creates the extension in the MX-ONE Service Node.

An optional way to determine which Telephony System the extensions are created in is to use the Telephony System Mapping which will overwrite the Telephony System specified by the template with the mapped system.

The received AD record will be mapped to the Telephony System matching the **Active Directory Values** of the selected **Active Directory Field**.

Rules must be set in PM for how the AD synchronization shall be handled when changes are done in AD and one of the following situations occurs:

- An extension defined for a user already exists in PM.
- · An existing user changes extension numbers.
- A user is deleted in AD.
- Users are configured with shared extensions in PM.

Refer to the PM Active Directory task online help for setting up the synchronization rules.

The AD fields will not provide any information about the creation of a mailbox, therefore the same number as for the extension will be used to set up a mailbox.

If no template has been mapped to an AD number field, no extension or mailbox will be created, even if the AD number field is filled in.

Below are some screens shots showing the *"Active Directory Users and Computers"* GUI, which is used to administer the AD, and the available AD fields for a standard AD installation.

Proper	ties	
	ns Remote control T	)ial-in   Object   Securi erminal Services Profile   CO   Telephones   Organizati
<u>F</u> irst name:	<u></u>	Initials:
Last name:		
Di <u>s</u> play name:		
Description:		
Offi <u>c</u> e:		
<u>T</u> elephone number:		<u>O</u> ther
E- <u>m</u> ail:		
<u>W</u> eb page:		Othe <u>r</u>
	ОК	Cancel Apply

#### Figure 5.2: Active Directory Users and Computers GUI - 1

Figure 5.3: Active Directory Users and Computers GUI - 2

Pro	operties ? X
· · · ·	icates MemberOf Dial-in Object Security essions Remote control Terminal Services Profile COM+ Iress Account Profile Telephones Organization
Telephone nu	imbers
Ho <u>m</u> e:	
<u>P</u> ager:	O <u>t</u> her
Mo <u>b</u> ile:	Other
<u>F</u> ax:	Other
<u>I</u> P phone:	Other
Notes:	
Notes:	
	OK Cancel Apply

### **PM Active Directory Task**

The set-up required in PM is done in the Active Directory task found a level below the System tab and Data Management sub tab.

Fill first in the **IP Address**, **Port**, **User Name** and **Password** to the AD server. Change the rest of the fields according to your preferences.

Email notification of connection failure to AD can be configured.

NOTE: PM Email Server task needs to be configured first.

#### Figure 5.4: Provisioning Manager

lsers Services	Administrators System	Lo	gs Own Settings	
Location Subsy	stem Data Management O	ptions	Email Server Configuration Wizard	
Compare with Subsystem	Active Directory Server - Ch	ando		
lackup & Restore	and the second	ange		
	Apply			
Scheduling				
Active Directory	Server Configure Domains			
	General Settings			
	③ IP Address:		172.17.11.100	
	⑦ Port :		389	
	User Name:		WBMlaastra	
	③ Password:			
	⑦ Confirm Password:			
	Notification			
	(1) Email Address:			
	Rules			
	⑦ Create Default Password:		8	
	① Automatically Remove Users:		8	
	③ Scan for Removed Users Interval [m]:		30	
	Extension Handling  () Extension/Mailbox Handling:		Try assign otherwise create new extension/mailbox *	
	Extension Number Length:		Try assign orienvise create new extension matters *	
	Mailbox Handling		r	
	( OneBox Server:		OneBox, version 5.0 *	
	() Create Mailbox:		2	
	Class Of Service:		None *	
	() UDF Mapping:		Edit	
	Remove Active Directory Server Confi	uration		
	Remove Configuration			

Select the **Configure Domains** tab and add a new Search Domain.

Fill in the Search Domains, the easiest way is to copy the **distinguishedName** field in the AD server.

It can be selected if a received telephone number shall be made into extensions and mailboxes and how and when to assign them to the received user. New extensions will use the selected extension template. The mailboxes will get the same number as the extensions. The IP Extension Templates are defined in the PM Extension task.

An optional way to determine which MX-ONE the extensions are created in is to use the **Telephony System Mapping**.

Select the **Active Directory** field that will be used when mapping the MX-ONE used when creating an extension. The mapped MX-ONE will overwrite the system read from the templates.

Enter the **Active Directory Values** that will be used then mapping the MX-ONE towards the received Active Directory record

Users Services	Administrators System Log	s Own Settings
Location Subsy	stem Data Management Options	Email Server Configuration Wizard
Compare with Subsystem	Multistep - Previous task	
Backup & Restore	- Back Active Directory Server - Change Cont	figure Domains
Scheduling Active Directory	Domain Configuration - Change - ( Apply Cancel	OU=Hej,OU=WBM Users,DC=wbm,DC=oamgorup
	⑦ Search Domains:       *         ⑦ Description:	OU=Hej,OU=WBM Users,DC=wbm,DC=oamgorup
	<ul> <li>Select Location :</li> <li>Select parent department for AD deparments : Extension Templates</li> </ul>	Globen    Globen
	⑦ Template for Telephone Numbers:	MyTemplate_WBM85_IPExtension ▼
	⑦ Template for Other Telephone Numbers:	None
	⑦ Template for IP Phones:	None
	⑦ Template for Other IP Phones:	None
	Telephony System Mapping	None
	<ul> <li>? Active Directory Field:</li> <li>? Telephony System</li> </ul>	None   Active Directory Values
	WBM85:	
	WBM60:	
	Apply Cancel	

Figure 5.5: Active Directory Values

Synchronization is done when performing an initial setup of PM, to quickly port all users from Active Directory to PM. The manual synchronization can be used in case of a connection failure to AD and it is required to get the systems back in synch. The manual synchronization is triggered by clicking on the **Refresh** icon for the desired Search Domain as shown in the picture below.

The **Automatic notification** option is used when a change in AD shall be automatically transferred to PM. The notification is enabled or disabled by clicking the **Activate/Deactivate** icon for the desired Search Domain.

Users Services	Administrators Syste	m Logs	Own Settings		
Location Subsyste	em Data Management	Options	Email Server	Configuration Wizard	Batch Operation
Compare with Subsystem	Active Directory Server	- Change			
Backup & Restore	Apply				
Import					
Export	Server Configure Domains				
Scheduling	Create				
Active Directory	Add				
	Search Doma	ins	Desci	iption	
	🔍 🥖 💢 🖲 🦑 OU=Sweden,OU=				
	🔍 🥖 💥 🐵 🖑 OU=ucl_demo,OU=WBM Users,DC=wbm,DC=oamgorup				

#### Figure 5.6: Enabling/disabling automatic notification

Users will be sent and updated to CMG if a CMG system is registered. When users are added, users will be placed in the same department that they belong to in AD. If the department does not exist, it will be

automatically created. For PM to be able to add user to CMG, the directory must map the Organization Unit structure. You must manually create it in CMG before synchronization. If you remove a department from AD, then it reflects Department in PM as **User without Department**. If you rename the department, then the same gets reflected in PM after the sync between AD to PM.

When user gets moved between departments in AD, it gets reflected in PM after the sync is done between the AD and PM.

# **Extension Handling Details**

If the extension already exists, an option in the PM Active Directory task will decide if the request shall fail or if it shall assign the existing extension as a shared extension to the new user. By the term fail, it is meant that the extension part of the request will not go through. The user as such will still be added.

As Active Directory only automatic sends notifications for user additions and changes, not for removal of users, Provisioning Manager will have to check for removed users with a specified interval.

If PM is set to not remove extensions when a user is removed in AD, then, potentially, shared extension setting must be set to enable the user to be assigned to already existing extensions. The same logic applies for mailboxes.

If a user is removed from AD, the PM setting for removing or keeping mailboxes must be adhered to. If the user has been assigned with extensions, these extensions will not be removed.

The phone numbers listed in AD may be listed in international format. They will be cut to the specified number length when used to add a new extension. Non-digit characters will also be stripped. If the number is not a number, then no action shall be made.

Example of numbers:

+46 8 56867074

+46 8 568 xxxxx

+1 905-760-1234

+46 (0)8 1234567

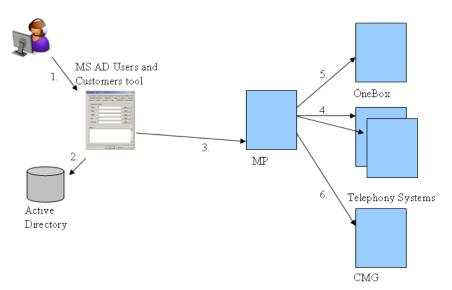
**NOTE:** AD administrator must have the master list for extension numbers and is responsible for the allocation of numbers as no list of available numbers will be available in the AD Users and Computers tool.

There is an option to add *"Other"* numbers for each telephony field, that is, additional numbers, in the AD GUI. Because these are not tagged separately, it will not be possible to handle them separately and they will therefore become additional numbers of the same extension type and based on the same template.

# Name Handling

A changed name will be propagated to all extensions associated with the user, assuming it is not a shared extension. In the case of a shared extension, the name will be added to this extension on CMG and MiCollab Advanced Messaging, but will not be changed or added in MX-ONE Service Node. If the name is too long for the name field for the extensions, it will be truncated.

# **Execution Flow**



The execution flow is as follows:

- 1. The AD administrator logs on to the Active Directory Users and Computers tool.
- 2. The administrator configures the users and submits the request. The standard AD settings are stored in AD.
- **3.** The data is sent through notification to PM where a predefined template is mapped to the submitted phone numbers. The user is created or modified.
- 4. PM sends a web services request to the selected MX-ONE to configure extensions.
- 5. PM sends a web services request to the selected MiCollab AM to configure a mailbox.
- 6. PM sends a web services request to the CMG to configure/modify a user.

# Limitations

The following limitations apply:

- In a system with legacy extensions, these extensions will not be automatically provisioned from AD. Only the user will be set up in PM providing that no template has been mapped to the AD number fields. If a template has been defined, IP extensions will be created.
- PM supports provisioning of maximum 75000 users from AD.
- If a CMG is connected to Provisioning Manager, Active Directory cannot have a user with the same *"last name"* and *"first name"* due to CMG that don't have an unique id (like user id). If Provisioning Manager doesn't have any CMG connected, it will work with same name but with different user id.
- Only four AD number fields can be mapped to PM IP extension templates. This means up to 4 templates can be used to create IP extensions, each mapped to a specific AD number field. In this case, only AD number fields associated to the same template should be filled in for a given user. Filling in 2 AD number fields that are associated to different templates for the same user will result in creating 2 different IP extensions for this user. A template contains detailed settings as well as in which Telephony System the IP extension shall be created in. That means that you can create IP extensions with the same settings in four different systems, or four different types of IP extensions in the same Telephony System or a combination thereof.

- Number handling is not included in PM; this will have to be handled by the MX-ONE administrator.
- Only 1 AD is currently supported.

**NOTE:** For very large systems (for example, above 15000 users) with multiple servers in the same logical system, the AD synchronization with PM and the subsequent creation/update of users/extensions in the MX-ONE system and its associated applications can be taken anywhere from a few hours up to a day or longer.

**NOTE:** There is a limitation in AD, it allows only to have five subscriptions for automatic change notifications. AD synchronization in PM does not work with more than five active domains. If you activate more than five domains (green icon), the automatic synchronization will not work anymore.

# **Additional Info**

For larger systems with many users, there will be a lot of notifications coming from AD to PM. Every computer login that a user performs triggers an update of AD and thereby a notification to PM. This will most likely not have an impact on the network performance, but it is worth mentioning.

**NOTE:** It is **NOT** recommended to use the System Setup Admin for Active Directory synchronization, as the users created by System Setup Admin during AD sync are not visible to other administrators.

# **AD** Authentication, Description

# Introduction

# **Description of AD Authentication**

AD authentication refers to the possibility to configure Provisioning Manager (PM) to authenticate user passwords in Active Directory (AD) instead of in the PM user database.

The concept is not a true "Single Sign On", but it will be possible to log in to PM and Service Node Manager (SNM) with the same user name/alias and password as when logging in to the corporate or department domain, as defined in AD.

When the PM server is configured for AD authentication, it will still be possible to log in with currently stored passwords in PM user database. This implies that if the AD server for some reason is out of service users who know the PM specific passwords will be able to continue working as normal.

AD authentication is only available when the PM web server is running in SSL mode. It is also required that SNM sub systems configured for PM authentication shall run in SSL mode.

# Prerequisites

- The authentication towards AD is performed over protocol LDAPS. The AD server must therefore be enabled for LDAPS.
- AD authentication is implemented with LDAP authentication method 'Simple authentication' (see: http://msdn.microsoft.com/en-us/library/cc223499.aspx). As this requires that the user password is sent in clear text, AD authentication is only allowed when the entire web server PM is running on is configured for SSL (HTTPS).
- The AD server must be configured for SSL on the LDAP(S) interface.
- An SNM defined as subsystem for PM configured for AD authentication will also use the AD authentication feature when it is configured for PM authentication method (that is, not *"Linux"*). See Scenario 2: SNM Login for more details.
- Subsystems configured with PM authentication method must also be configured for SSL.
- Subsystems not configured for SSL must use Linux authentication method. That is, all users that need access must be provided with an own Linux account. Note that this is a high security risk if users get used to log in with AD credentials. See *Scenario 3: SNM Login over HTTP* for more details.
- Auto-login in SNM is disabled when you select click on subsystem in PM. Instead the user needs to be authenticated again, but as long as the SNM server is configured for SSL and PM authentication method, the same user name and password as for the domain (and PM login) will be used.
- All users that should be able to log in to PM and SNM must still be defined as users in the PM database. However, the password associated with each user is not in use as long as AD authentication is enabled.

• The user name or alias used when logging in to PM or SNM with AD authentication must match the one defined and stored in the PM database.

#### Example:

A user is defined as jdoe in PM and as jdoe@mydomain.com in AD.

The "Principal DNS Suffix" is configured as mydomain.com.

PM server will build the complete User-Principal-Name as jdoe@mydomain.com and it is possible to log in to PM with jdoe, only.

The login name or alias must have a perfect match in the PM database to read validate the users' privileges, even if the password is validated in AD.

See Configure AD Authentication for more details.

### **Supported AD versions**

- Windows Server 2008 R2 (64 bit)
- Windows Server 2012 (64 bit)

# Security

### Secure Socket Layer (SSL)

The server, on which PM is installed, needs to be configured for SSL (HTTPS). End users will be using HTTPS when accessing the application web page. The same applies for web services between PM and SNM. Also the AD communication with LDAP shall be encrypted over SSL.To configure SSL/HTTPS, use the webserver config command. See *Configuration* for more details.

### Certificates

The use of certificates is all about trust. We need to be able to trust the other party we connect to and communicate with. Due to this, two different kinds of certificates are required when running AD authentication:

- Server Certificate: As a server to run the web application over HTTPS
- Root Certificate: As a client when we connect to the AD server.

#### **Server Certificate**

The server certificate is used for the purpose of other (clients) to trust the PM when connecting over HTTPS. This could either be a self-signed certificate or a certificate signed by a Certificate Authority (CA). See *Configure Web Protocol* for more details.

#### **Root Certificate**

PM and SNM are running as Java driven applications under Jboss.

When connecting to an AD server over SSL, it is required that the Java application can verify the AD server as a trustful source. To make this functioning, a proper certificate must be imported and stored in the Java trust store.

The certificate could be the AD server's own server certificate that is distributed when connecting to it over SSL. This will work perfectly as long as the AD connection is defined as a fixed host name or IP address representing the AD server.

However, in a more complex environment, it is more common that the AD connection is made through a broadcast through the domain controller or by addressing a sub domain or even the entire domain. In this situation, it would be inconvenient to store the server certificates for all possible transfer servers the connection will need to verify as trustworthy. Instead, a proper root certificate that can verify the signature on each server's server certificate should be imported. See *Certificate Management for AD Authentication* for more details.

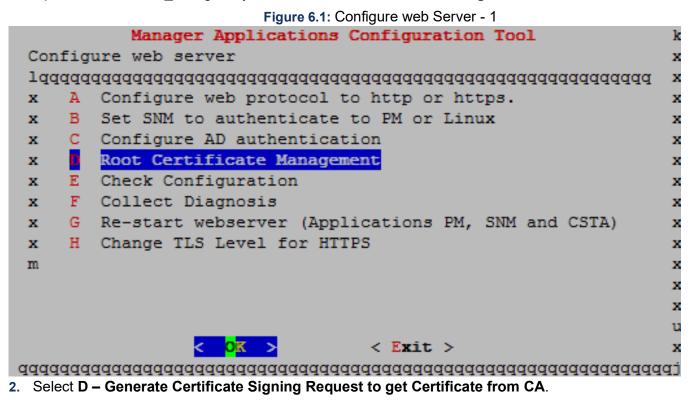
# Generating Certificate Signing Request (CSR) and Creating Keystore

This section explains how to use the webserver\_config utility to generate the Certificate Signing Request (CSR).

Once you receive the Signed Certificate from the Certificate Authority, the section also describes how to create the Keystore.

#### **Creating Certificate by Signing Request File**

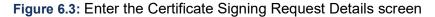
1. Open the webserver\_config utility. Select **D** - Root Certificate Management.



```
Figure 6.2: Configure web Server - 2
```

Roo	t C	ertificate Management
ldd	ddd	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
х	A	Load uploaded Root Certificate into Java truststore
х	в	Download Server Certificate by connecting to trusted host
х	С	Search loaded Certificates by alias
х		Generate Certificate Signing Request to get Certificate From CA
x m	Е	Creating Key Store By using CA Signed Certificate
		< OK > < Back >

3. Fill in the below form with the below details:



Press also Considirente Circular Demote Describe	x
Enter the Certificate Signing Request Details lagagagagagagagagagagagagagagagagagagag	X
xCountry Name (2 letter code) [AU]:	
X	
xState or Province Name (full name) [Some-State]:	x
x	x
xLocality Name (eg, city) []:	Stockholm x
x	x
xOrganization Name (eg, company) [Internet Widgits Pty Ltd]:	Mitel X
x	x
xCommon Name (eg, YOUR name) []:	pmsnm.common.com X
x	x
xSAN - DNS Names Ex: [pm.common.com,snm.common.com] :	pm.common.com, snm.common.com
x	x
xSAN - IP Adresses Ex: [192.168.1.1,192.168.1.2] :	192.168.26.1,192.168.26.2 x
x	
x	
	0
	Ŷ
< <mark>0 x &gt;</mark>	<cancel> x</cancel>
444444444444444444444444444444444444444	444444444444444444444444444444444444444

NOTE: Common Name is like Domain Name which we want to display in the Certificate.

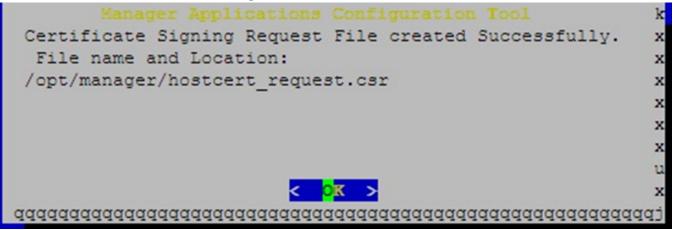
In the above screenshot *"pmsnm.common.mitel.com"* is common name, which can be anything based on the organization.

#### Figure 6.4: Example of Common Name field

MiVoice N	X-ONE Provisio × 🔽 📭 MiVoice MX-ONE Service I × 🗖 MiVoice MX-ONE Provisio ×
← ⇒ C <sup>i</sup>	د المعالية://192.168.26.194/mp/
	Certificate
	General Details Certification Path
	Certification path
	Image pmsnm.common.mitel.com
- (	CANL DNC Nemon Subject Alternate DNC Nemon

- a. SAN DNS Names: Subject Alternate DNS Names
- **b.** Ex: pm.common.com,snm.common.com
- c. SAN IP Addresses: Subject Alternate IP Addresses. Ex: 192.168.2.1, 192.168.2.3
- d. After you have filled the form click **OK**. The system will generate the Certificate Signing Request (CSR) File and locate it at /opt/manager/hostcert\_request.csr.
- 4. You must copy this file to the local system and share it with Certificate Authority (CA) for them to provide the Signed Certificate.

Figure 6.5: Successful creation of CSR file



#### Creating the Key Store by using Signed Certificate

Once you receive the Signed Certificate from the Certificate Authority, you must copy that certificate to the server where you want to enable the HTTPS.

1. Open webserver\_config utility.

```
Figure 6.6: Creating the Key Store - 1
```

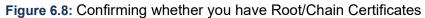


- 3. Then select the path of the Signed Certificate in the system.
- 4. Press TAB to move between Directories, Files and Buttons sections
- 5. Press **Space** and select the Directory and Files

Manager Applications	Configuration Tool	k
Directories	Files	x
laaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	144444444444444444444444444444444444444	x
x <mark>.</mark>	xcertnew.cer	x
x	xcertnew2.cert	x
x	xcommon_response.cer	x
x	xcommon response der.cer	x
x	xpmsnm common response.cer	x
x	xroot der.cer	x
x	xroot der.cer.tmp	x
х	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
х	x	x
x	x	x
х	x	x
x	x	x
m	m	x
144444444444444444444444444444444444444	144444444444444444444444444444444444444	x
x/home/eri_sn_admin/TestCert	ts/certnew2.cert	x
m		x
		u
< OK >	<cancel></cancel>	x
199999999999999999999999999999999999999	1aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	qj

Figure 6.7: Selecting the directory and files

6. Confirm whether you have any Root / Chain Certificates available with our CA Signed Certificate







Certificate	×
General Details Certification Path	
Certification path	
GeoTrust Global CA	1
Google Internet Authority G2	
When you open the certificate like above, here "GeoTrust Global CA" is a Root Certificate, Internet Authority G2" is Chain / Intermediate Certificate, "*.google.com" is a Signed Certific These Root and Signed Certificates will be provided by the Certificate Authority or can be dow	cate.
from their sites. If there is only Root Certificate, you can use that file directly and ignore the below section of marga all these Root and Chain Certificates into ano file.	otherwise
merge all these Root and Chain Certificates into one file When you open these Root / Chain Certificates in the notepad, the content might look like BEGIN CERTIFICATE	below:

-----END CERTIFICATE-----

7. Merge the content like below in the file First Root Certificate, then Chain Certificate:

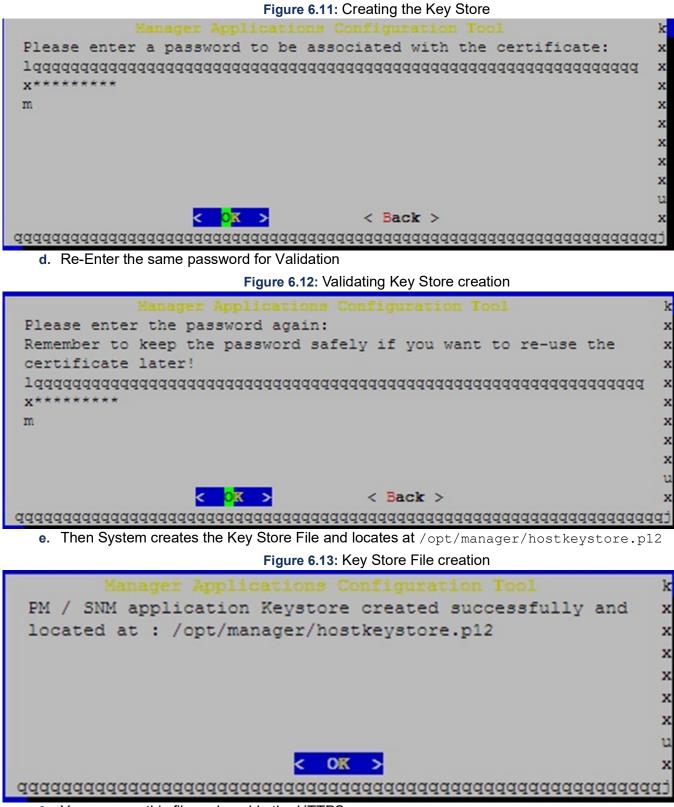
-----BEGIN CERTIFICATE-----Root Certificate Information -----END CERTIFICATE----------BEGIN CERTIFICATE-----Chain Certificate Information

- 8. Select the Root / Chain Certificate file:
  - a. Select TAB to move between Directories, Files and Buttons sections
  - b. Press **Space** and select the Directory and Files.

Figure 6.10: Selecting the Root / Chain Certificate file

5		
Manager Applications	Configuration Tool	k
Directories	Files	x
Jaadaadaadaadaadaadaadaadaadaa	Jaadaadaadaadaadaadaadaa	x
x <mark>.</mark>	xcertnew.cer	x
x	xcertnew2.cert	x
x	xcommon_response.cer	x
x	xcommon_response_der.cer	x
x	xpmsnm_common_response.cer	x
x	xroot_der.cer	x
x	xroot_der.cer.tmp	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
x	x	x
m	m	x
Jaadaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	144444444444444444444444444444444444444	x
x/home/eri_sn_admin/TestCert	ts/root_der.cer	x
m		x
		u
< OK >	<cancel></cancel>	x
c. Enter the password to create the Key Sto		qj

c. Enter the password to create the Key Store



f. You can use this file and enable the HTTPS.

Webserver\_config ? Configure web protocol to enable HTTP or HTTPS? Change to HTTPS / Keep HTTPS? Certificate is uploaded to file System? select the created Key Store file from /opt/manag-er/hostkeystore.pl2.

# Importing Certificates for PM and SNM

Follow the steps below to generate and import certificates for PM and SNM by using local Windows Server as Certificate Authority.

- 1. Generate certificate requests by using IIS for PM and SNM.
- 2. Upload the certificate request to "certsrv" application.
- 3. Issue the certificates by using Microsoft Management Console (MMC).
- 4. Download the Issued certificates from "certsrv" application.
- 5. Complete the certificate request by using IIS.
- 6. Generate the PFX files for PM and SNM with private key to use as a keystore.
- 7. Follow below steps to enable SSL for PM and SNM applications.
  - a. Open Webserver\_config utility
  - b. Select Configure web protocol to HTTPS
  - c. Select Change to HTTPS
  - d. Select Certificate is uploaded to file system
  - e. Select the "PFX" file which was generated in Step 6.
- 8. Follow below steps to exchange the certificates between PM, SNM, AD and CMG
  - a. Open Webserver config utility
  - b. Select Root Certificate Management
  - c. Select Load Upload Root Certificate into Java truststore.
  - d. Select the certificate of other system and provide the alias name. For example, if you are executing above steps in PM, then you must select the certificate of SNM that you have downloaded from Step 4
  - e. In case if the Other system is AD or CMG, then you must get the AD or CMG certificates from AD or CMG servers by using Microsoft Management Console (MMC) tool.
  - f. Importing the certificate of PM/SNM, AD and or CMG is applicable for Co-Existing system (PM/SNM are in same server) also.
  - g. You can import the certificate by connecting to other system directly by selecting webserver\_config > Root Certificate Management> Download Certificate by connecting to trusted host > Enter the Other Server Name / IP, Port and alias names.
- **9.** At AD or CMG side, have to import the server Certificate of PM by using Microsoft Management Console (MMC) tool to the *"trusted people"* section.
- **10.** Import the Root Certificate of PM to AD or CMG by using Microsoft Management Console (MMC) tool to *"trusted Certificate Authority"* Section.

**NOTE:** Certificates that is generated in the steps above is a self-signed certificate using Microsoft IIS and there are also other ways of doing that. It is recommended to use the company's certificate.

# Users

There are two types of users that shall be considered in PM.

The first user type is *"end user"* which is the user that logs on to PM and/or SNM web page. This user may have different levels of privileges, from a *"plain"* end user in PM up to an administrator defined as *"Super User"*.

The second user type is *"service account"* which is the account used when PM and SNM communicate in the background through web services. This account is set up as any *"end user"* account and should be provided with enough privileges to serve all actions needed to be performed (independently of who is performing them).

The *"service account"* is the user defined as "User ID in Subsystem" when adding SNM as subsystem in PM. Whenever an action that requires access to SNM is performed in PM this account's privileges are checked.

See example of how 'end user' versus 'service account' is used: Scenario 4: PM Login + use case 'Add Extension'.

# Configuration

All configuration of AD authentication is done through the configuration utility for the web server, which is provided with each installation of PM or SNM. It is only when PM is installed that the configuration of AD authentication is available.

All necessary configuration scripts are available through the following command:

webserver\_config.

# **Configure Web Protocol**

To set the server in SSL mode, choose to configure the web server protocol and then choose HTTPS.

In SSL mode the PM server must have its own server certificate. This may be a self-signed root certificate, or a properly signed certificate from a Certification Authority (CA). The latter will be considered as 'safe' for visitors of the PM web as long as the CA's root certificate is included in the clients' browser. All modern web browsers are provided with a subset of root certificates from trusted CA's.

A self-signed certificate is from a technical point of view like a signed certificate from a CA. The main, but important, difference is that the self-signed certificate cannot be verified as trustworthy by other servers or clients. The clients web browser will show a warning when the page is visited.

If a server certificate is to be imported to the PM server, it must first be uploaded to the Linux file system. Use any kind of SFTP (Secure File Transfer Protocol) client, like e.g. WinSCP to connect and upload the certificate file. The certificate should be in the format PKCS#12.

#### Configuring Web from HTTP to HTTPS with Self-Signed Certificate

Follow the procedure below to configure the Web portal from HTTP to HTTPS with Self-Signed Certificate:

- 1. As root, or with sudo privileges, run the webserver\_config command.
- 2. Select Configure web protocol to http or https.

#### 3. Select [CHANGE TO/KEEP] HTTPS.

- 4. Confirm the next two windows by pressing the **Type** key.
- 5. Select Create a self-signed certificate.
- 6. Type the password to be associated with the certificate.

**NOTE:** This step is required in case the certificate shall be re-used later on.

- 7. Re-type the password.
- 8. Accept a restart of the web server. The configuration will not take effect before a restart of the web server is done.

#### **Configuring from HTTP to HTTPS with Uploaded Server Certificate**

Follow the procedure below to configure the Web portal from HTTP to HTTPS with uploaded server Certificate:

- 1. As root, or with sudo privileges, run the webserver\_config command.
- 2. Select Configure web protocol to http or https.
- 3. Select [CHANGE TO/KEEP] HTTPS.
- 4. Confirm the next two dialogs by pressing the **Type** key.
- 5. Select Certificate is uploaded to file system.
- 6. Use the Up/Down key, and Enter on the keyboard, to navigate to your certificate file, mark it and press **Enter**.
- 7. Accept that it is the correct file to be used.
- 8. Provide the password associated with the certificate.

**NOTE:** If an incorrect password is used, the certificate will not function.

**9.** Accept a restart of the web server. The configuration will not take effect before a restart of the web server is done.

#### Turning SSL off and back on again

When the server has been configured in SSL mode, it means a server certificate already is available. In case the SSL is turned off and should be turned on again, the configuration script will identify the previously used certificate which could be re-used.

The procedure looks exactly like the one for an uploaded server certificate, with the difference that you already at step 5 can choose to re-use the found certificate instead.

As for the case with the uploaded server certificate, it is an absolute must that the password matches the one associated with the certificate.

#### **Configure SNM authentication method**

The SNM authentication method refers to in which way a user that logs in to SNM is authenticated. It could be either of *"Linux authentication"* or *"PM authentication"*.

For Linux authentication it is required that the user has a Linux account. This is to be created according to standard Linux procedures via command or using mxone\_maintenance utitily. Log-in as user mxone\_admin, and key the command sudo -H /opt/mxone\_install/bin/mxone\_maintenance and select option user and follow the instructions on screen.

For PM authentication, SNM will instead send a (SOAP) request to the configured PM server to verify user credentials and privileges (authenticate and authorize).

**NOTE:** If the SNM server is not running SSL (HTTPS) and PM is configured for AD authentication, the SNM authentication method must be set to Linux authentication. This means that administrators that need to log in to SNM must be provided with a separate Linux account. This account will not be authenticated towards AD. Note that this is a security risk if users get used to log in with AD credentials. See further *Scenario 3: SNM Login over HTTP*.

If PM and SNM are running on the same server, that is, MX-ONE Service Node 1 (LIM 1), the SNM authentication method will automatically be set to PM authentication method as soon as AD authentication is enabled.

To set PM authentication method when PM is running on a standalone server, log in to the SNM server and do the following:

- 1. As root, or with sudo privileges, run the webserver\_config command.
- 2. Select Set SNM to authenticate to PM or Linux.
- 3. Select [CHANGE TO/KEEP] PM authentication.
- 4. Enter the required information in fields in the window.
- 5. Accept a restart of the web server. The configuration will not take effect before a restart of the web server is done.

#### **Certificate Management for AD Authentication**

This topic provides information on how to obtain and manage root certificates for AD authentication.

#### **Root Certificate or Signed Server Certificate**

To import a root certificate or a server certificate from another server that should be trusted.

Do as follows:

- 1. Connect to the Linux server with a SFTP client such as WinSCP and upload the root certificate to the file system.
- 2. As root, or with sudo privileges, run command webserver\_config.
- 3. Select Root certificate management.
- 4. Select Load uploaded Root Certificate into Java trust store.
- 5. Use the Up/Down on the keyboard, to navigate through the file system and find the uploaded certificate.
- 6. Select the certificate file and press Enter.
- 7. Select Yes, and press Enter.
- 8. Assign an alias (as identifier) to the certificate. This will be the only way to easily search and when applicable delete the certificate from trust store.

#### 9. Press Enter

**10.** Confirm (on command line) with yes or y, to trust the certificate.

#### **Alternative to Root Certificates**

It is for practical reasons not usual to have properly signed root certificates in lab environments, but it might still be necessary to verify AD authentication functionality. As long as the AD server can be directly accessed through either IP address or host name the following procedure can be used.

Do as follows:

- 1. As root, or with sudo privileges, run the webserver config command.
- 2. Select Root certificate management.
- 3. Select Download Server Certificate by connecting to trusted host.
- 4. Type server IP address or host name.
- 5. Type SSL port (commonly used is 636 for LDAPS).
- 6. Type an alias (as identifier) to the certificate. This will be the only way to easily search and when applicable delete the certificate from trust store.
- 7. Press Enter.
- 8. Follow the progress on the screen. If the connection takes very long time, e.g. because of faulty inserted IP address, you may have to press ctrl-c to interrupt. In that case the process needs to be started over again.
- Repeat the steps from Step 3 to Step 8 for PM/SNM machine also, to download the certificate of PM/SNM local certificate to Java Trust Store.
- **10.** Confirm (on command line) with yes or y to accept the certificate.

#### Search and Delete root certificates

There might be good reasons for finding root certificates in the Java trust store. If e.g. a certificate was trusted added by mistake or if in general find out what's already stored. All certificates in trust store are identified through a unique alias.

To search Java trust store and optionally delete a certificate, perform the following steps:

- 1. As root, or with sudo privileges, run the webserver config command.
- 2. Select Root certificate management
- 3. Select Search loaded Certificates by alias.
- 4. Type the full or partial alias or all to view all stored certificates. All aliases are in lower case.
- 5. If any hits a result list appears.
- 6. To view details, select View and press Type.
- 7. To go back, press Type.
- 8. To delete a certificate from trust store, select **Delete**and press **Type**.
- 9. To confirm deletion, select Yes and press Type, or select No.

# **Configure AD Authentication**

The following must be considered before AD authentication is configured:

- How shall the AD server be addressed:
  - IP address
  - Host name
  - Domain name
- Which port number is applicable for LDAPS on the AD server (default is 636)
- Is there a need to define the Base Context DN (Distinguished Name) for AD? This is equal to defining in which part of the AD the user shall be sought. Example:

CN=Users,DC=mysubdomain,DC=mydomain,DC=org

To search the entire AD, leave the field blank.

**NOTE:** Base Context DN must have a perfect match, and it cannot be verified by any means by the PM configuration tool.

- How the user credentials shall be typed:
  - a useralias only
  - useralias@domain (also commonly known as User-Principal-Name)
- All users belong to the same domain, ourdomain.com.
- The AD server uses User-Principal-Name when authorizing users, i.e. by default the user e-mail address, e.g. jdoe@ourdomain.com.
- In the AD authentication configuration, define the Principal DN suffix as ourdomain.com.
- The users will now use the alias only, e.g. jdoe when logging in to PM.

**NOTE:** If a user tries to login with jdoe@ourdomain.com, it will still be suffixed and the entire string jdoe@ourdomain.com@ourdomain.com will be sent to AD. The login will fail. The same applies if there are users with different domain names in their User-Principal-Name.

- Type the Principal DN suffix.
- Do never Type the character @. It will automatically be appended.

Do as follows:

- As root, or with sudo privileges, run the webserver config command.
- Select Configure AD authentication.
- If AD authentication already is configured, you will be asked if you'd like to turn it off, select No.
- Type host name, IP address or domain name to address the AD server.
- Type the port for LDAPS on the AD server (default 636).
- Type the Base Context DN, if desired (leave blank if not).
- Type the Principal DN suffix.
- Acknowledge restart of the web server. The configuration will not take effect before a restart of the web server is done.

NOTE: If the server not is configured for SSL/HTTPS, the AD configuration wizard will be interrupted.

# **AD** Authentication Maintenance

This topic provides information on the managing the AD authentication settings.

### **Modifying AD Authentication Configuration**

To modify any settings in the AD authentication configuration, such as AD server host name and port or Principal DN suffix, the procedure is basically the same as when activating it the first time.

Do as follows:

- 1. As root, or with sudo privileges, run the webserver config command.
- 2. Select Configure AD authentication.
- 3. On question Do you want to turn AD authentication off?, select No.
- 4. Modify applicable settings.
- 5. Accept restart of the web server. The modified configuration will not take effect before a restart of the web server is finished.

# **Turning AD Authentication Off**

The AD authentication service can be temporarily or permanently turned off. In any case the previous settings are saved in case the service should be turned on again later.

Do as follows:

- 1. As root, or with sudo privileges, run the webserver config command.
- 2. Select Configure AD authentication.
- 3. On question Do you want to turn AD authentication off? select Yes.
- 4. Accept restart of the web server. The modified configuration will not take effect before a restart of the web server is done.

### **Turning AD Authentication Back on**

An already existing configuration of AD authentication service can be turned back on. The procedure to do this is exactly the same as when configuring AD authentication the first time, with the difference that the fields are pre-filled with previous settings. If applicable, modify the settings.

The modified configuration will not take effect before a restart of the web server is finished.

# **AD** Authentication Scenarios

AD authentication is performed on the server where PM is installed. If no PM is in use in the MX-ONE system, only Linux accounts can be used to access SNM.

For each login attempt it is checked whether the user is:

- 1. Authenticated a match between user alias and Typed password is found.
- 2. Authorized the authenticated user has enough privileges.

At each login attempt it is first checked if the user can be authenticated in the PM user database. If not, an AD authentication attempt is made and if this is successful the user is authorized from PM user database.

Through this sequence it will always be possible to log in with an administrative service account in PM also if for some reason the connectivity with the AD server is lost. It is also possible to log in with a password stored in PM user database or a password connected to the user account in AD.

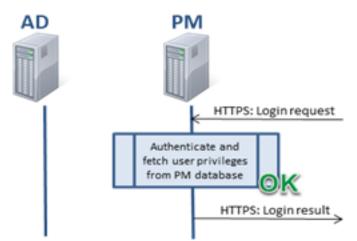
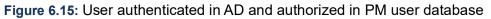
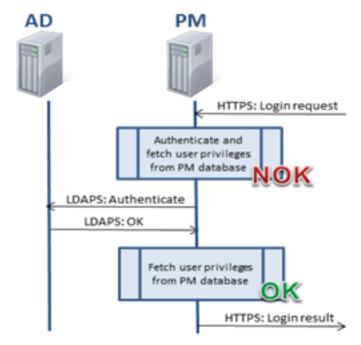
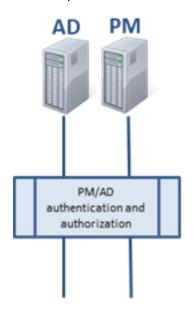


Figure 6.14: User authenticated and authorized in PM user database

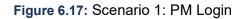


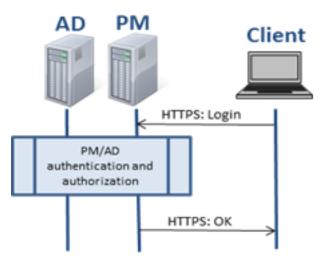




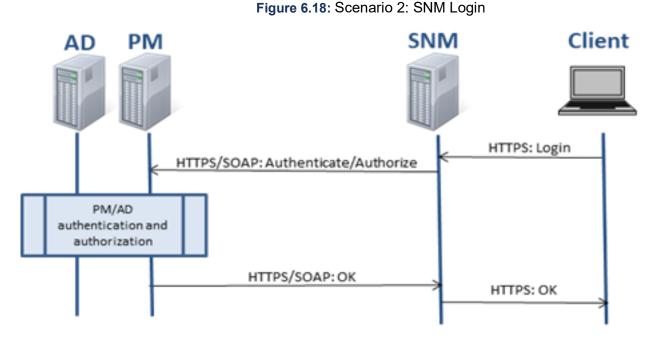
#### Figure 6.16: The examples above are in the following scenarios referred to as

# Scenario 1: PM Login





### Scenario 2: SNM Login



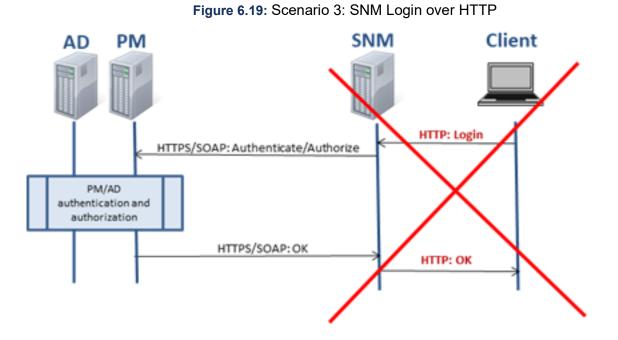
# Scenario 3: SNM Login over HTTP

Warning! This scenario shall be avoided!

- 1. PM server is configured for AD authentication.
- 2. SNM server is configured for PM authentication.
- 3. SNM server is not configured for SSL.

There is no built in mechanisms to control that SNM systems have been configured to use an PM as authentication server. Therefore it is important that the system administrator makes sure to configure all involved components in the network homogeneously.

The risk is that users get used to log in with AD credentials which basically requires SSL. If the user now connects directly to an SNM system without SSL, it is highly possible that the user still types AD credentials and the user alias and password may be exposed in the network.



### Scenario 4: PM Login + use case 'Add Extension'

A user that logs in to PM will get the privileges he/she is entitled according to the configuration. However, when executing things that requires access to the connected subsystem (SNM server) another account will be used for authentication in the background web services involved. This is referred to as the subsystem "service account".

The service account is the one defined when the subsystem was created. It is a separate account and should not be mixed up with normal accounts. The privileges for the service account must be set "high enough" to serve all end users and administrators.

- **NOTE:** Despite that the "service account" is configured with privileges on a high level, it will not enable any extra features for the logged in PM user.
- It is recommended that the "service account" is created for PM authentication only, and not as an AD
  user account. Implicit actions in the PM application that require use of the subsystem "service account"
  will render a lot of authentication requests. It is therefore more efficient to avoid AD authentication.

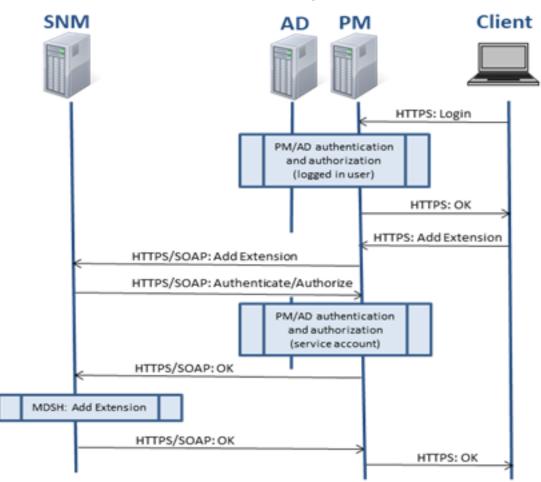
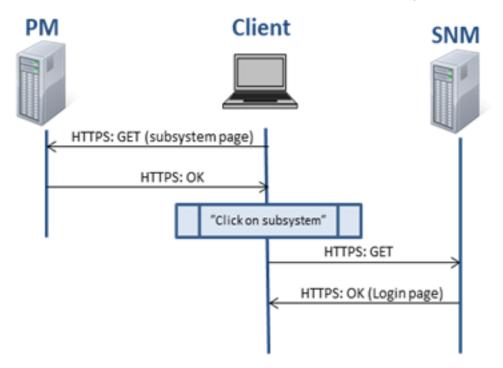


Figure 6.20: Scenario 4: PM Login + use case 'Add Extension'

### Scenario 5: In PM "click on subsystem"

PM holds a list of connected "subsystems". It is possible to click on the hyper links to log in to each subsystem. This may result in an automatic log in depending on the configuration.

The behavior for click on subsystem of type SNM is changed when using AD authentication. The automatic login is disabled. Instead the login page for the SNM will be launched. If the SNM server is configured for PM authentication, the same credentials can be used as when logging in to PM.



#### Figure 6.21: Scenario 5: In PM "click on subsystem"

# Fault Cases / Exceptions

Table	6.1: Fault	Cases /	Exceptions
-------	------------	---------	------------

Fault / Exception	Resulting in	Comments
Server is configured for HTTP (no SSL)	AD authentication will be automatically disabled	Administrator will be notified during the configuration
Wrong password is used in existing or uploaded server certificate	SSL traffic will not work Not possible to even load the web page	The reason will be seen in Jboss server.log as: Error starting endpointjava.io.IOException: failed to decrypt safe contents entry
Root certificate for AD server or (when applicable) domain is missing	All communication over LDAPS with AD server will fail Not possible to log in	The reason will be seen in Jboss server.log as: Message: Exception caught during login: Password Incorrect/Password Required

# **Configuration of AD LDS, User Guide**

# Introduction

# General Introduction to AD LDS in MiVoice MX-ONE 6.x

Active Directory Lightweight Directory Services (AD LDS) role, is formerly known as Active Directory Application Mode (ADAM). Any user can provide directory services for directory-enabled applications without incurring the overhead of domains and forests and the requirements of a single schema throughout a forest.

It is a Lightweight Directory Access Protocol (LDAP) directory service that provides data storage and retrieval support for directory-enabled applications, without the dependencies that are required for the Active Directory Domain Services (AD DS). You can run multiple instances of AD LDS concurrently on a single computer, with an independently managed schema for each AD LDS instance.

# About this guide

This guide describes the processes for setting up AD LDS and getting it running. You can use the procedures in this guide to configure AD LDS on servers that are running the Windows Server® 2012 operating system.

# Requirements

Before you start using the procedures in this guide, do the following:

- 1. Check the availability of at least one test computer on which you can install AD LDS.
- 2. Log on to Windows Server 2008 with an administrator account.

# Steps for Getting Started with AD LDS

The following sections provide step-by-step instructions for setting up AD LDS. These sections provide both graphical user interface (GUI) and command-line methods for configuration setup of AD LDS.

- 1. Enabling AD LDS in Windows Server
- 2. Creating AD LDS Instance
- 3. Restarting the AD LDS Instance
- 4. Creating an Admin User in AD LDS
- 5. Checking User authentication
- 6. Adding Attributes to UserProxyFull Class
- 7. Editing UserProxyFull Object Class as User Object class

- 8. Modifying MS-AdamSyncConf File
- 9. Synchronizing Users from Active Directory to AD LDS Instance
- 10. Checking Synchronized Users in ADLDS
- 11. Enabling LDAPS (SSL) for AD LDS
- 12. Using AD LDS as a User repository in Provisioning Manager (PM) Application
- 13. Uninstalling of AD LDS Instance and AD LDS Roles from Server

**NOTE:** To maximize your chances of successfully completing the objectives of this guide, it is important that you follow the steps in this guide in the order in which they are presented.

# Prerequisite

AD LDS server should be a part of Active Directory Domain, so that users can login into AD LDS server using their respective User IDs and Passwords from active directory. User display name and User ID must be same in Active Directory created for all users.

### **Enabling AD LDS in Windows Server**

If any of the organization wants to use AD LDS as a proxy to AD Server, then they can follow this document to enable AD LDS as a proxy server.

To enable AD LDS in Window Server, do the following:

- 1. Click Start, and then click Server Manager. You can do this from Task Bar or from Start/ Administrative Tools menu.
- 2. Select the Server Manager> Add Roles and Features. Click Next. The following screen appears.

<b>B</b>	Add Roles and Features Wizard
Before you begin	DESTINATION SERVER WIN-I5QI9N3LK72.mxone.local
Before You Begin Installation Type	This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
Server Selection Server Roles	To remove roles, role services, or features: Start the Remove Roles and Features Wizard
Features Confirmation Results	Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, close the wizard,
	complete the steps, and then run the wizard again. To continue, click Next.
	Skip this page by default
	< Previous Next > Install Cancel

3. ChooseRole-based or feature-based installation. Click Next.

L	Add Roles and F	eatures Wizard	_ 🗆 🗙
Select installation	i type		ESTINATION SERVER 9N3LK72.mxone.local
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	<ul> <li>machine, or on an offline virtual ha</li> <li>Role-based or feature-based in Configure a single server by add</li> <li>Remote Desktop Services inst</li> </ul>	nstallation ing roles, role services, and features. allation Virtual Desktop Infrastructure (VDI) to create a	
		< Previous Next > In	stall Cancel

#### 4. Select Idapstest server from the server pool. Click Next

<b>a</b>	Add	Roles and Features V	Vizard	_ <b>□</b> ×
Select destination	server			DESTINATION SERVER WIN-I5QI9N3LK72.mxone.local
Before You Begin Installation Type Server Selection Server Roles	<ul> <li>Select a server fi</li> <li>Select a virtual h</li> </ul>	rom the server pool	to install roles and features.	
Features Confirmation	Server Pool			
Results	Name Idapstest	IP Address 10.5.0.4	Operating System Microsoft Windows Server	2012 R2 Datacenter
	Add Servers comma	rvers that are running Win	dows Server 2012, and that ha fline servers and newly-added	
		< Pre	vious Next >	Install Cancel

5. Mark Active Directory Lightweight Directory Services from the list of roles and click Next.

<b>7</b>	Add Roles and Features Wizard	_ <b>D</b> ×
E Select server roles Before You Begin Installation Type Server Selection Server Roles Features AD LDS Confirmation Results	Select one or more roles to install on the selected server.  Roles  Active Directory Certificate Services  Active Directory Federation Services  Active Directory Lightweight Directory Services  Active Directory Rights Management Services  Application Server	DESTINATION SERVER WIN-ISQ(INJLK72.muone.local Description Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure of Active Directory Domain Services. Multiple instances of AD LDS can exist on a single server, each of which can have its own schema.
Results	Application Server     DHCP Server     DNS Server     Fax Server     Fax Server     Network Policy and Access Services     Print and Document Services     Remote Access     Remote Desktop Services     ✓	which can have its own schema.

#### 6. From the list of features, choose nothing - just click Next \_ х 冾 Add Roles and Features Wizard Select features DESTINATION SERVER WIN-I5QI9N3LK72.mxone.local Select one or more features to install on the selected server. Before You Begin Installation Type Features Description Server Selection .NET Framework 3.5 combines the $\land$ $\triangleright$ .NET Framework 3.5 Features (1 of 3 installed) power of the .NET Framework 2.0 Server Roles .NET Framework 4.5 Features (2 of 7 installed) $\triangleright$ APIs with new technologies for Features ≣ building applications that offer Background Intelligent Transfer Service (BITS) appealing user interfaces, protect AD LDS BitLocker Drive Encryption (Installed) your customers' personal identity BitLocker Network Unlock Confirmation information, enable seamless and BranchCache secure communication, and provide the ability to model a range of Client for NFS business processes. Data Center Bridging Direct Play Enhanced Storage (Installed) Failover Clustering Group Policy Management IIS Hostable Web Core Ink and Handwriting Services ~ - - -Ш > < Previous Next > Install Cancel

#### 7. click Next.

#### х b Add Roles and Features Wizard DESTINATION SERVER Active Directory Lightweight Directory Services (AD LDS) WIN-I5QI9N3LK72.mxone.local Organizations that have applications which require a directory for storing application data can use Before You Begin Active Directory Lightweight Directory Services (AD LDS) as the data store. AD LDS runs as a non-Installation Type operating-system service, and, as such, it does not require deployment on a domain controller. Running as a non-operating-system service allows multiple instances of AD LDS to run concurrently on a single Server Selection server, and each instance can be configured independently for servicing multiple applications. Server Roles Things to note: Features AD LDS After installing AD LDS, instances of AD LDS can be created by launching the AD LDS Setup Wizard from the Advanced Tools section of the AD LDS home page. Confirmation · Before removing the AD LDS role, you must use Programs and Features in Control Panel to remove all previously installed AD LDS instances. < Previous Next > Install Cancel

#### 8. Click Install to start installation.

<b>B</b>	Add Roles and Features Wizard	-		x
Confirm installation	on selections	TINATIO I3LK72.m		
Before You Begin	To install the following roles, role services, or features on selected server, click Install.			
Installation Type	Restart the destination server automatically if required			
Server Selection	Optional features (such as administration tools) might be displayed on this page because			
Server Roles	been selected automatically. If you do not want to install these optional features, click Pr their check boxes.	evious	to cle	ar
Features				
AD LDS	Active Directory Lightweight Directory Services			
Confirmation	Remote Server Administration Tools Role Administration Tools			
Results	AD DS and AD LDS Tools AD LDS Snap-Ins and Command-Line Tools			
	Specify an alternate source path			
	< Previous Next > Install	C	ancel	

#### 9. Once installation is complete, click **Close**.

2	Add Roles and Features Wizard
Installation progre	DESTINATION SERVER WIN-I5QI9N3LK72.mxone.local
Before You Begin	View installation progress
Installation Type	Feature installation
Server Selection	
Server Roles	Configuration required. Installation succeeded on WIN-15QI9N3LK72.mxone.local.
Features	Active Directory Lightweight Directory Services
AD LDS	To create a new AD LDS instance on this server, run the Active Directory Lightweight Directory
Confirmation	Services Setup Wizard. For more information, see http://go.microsoft.com/fwlink/?Linkld=224861. Run the Active Directory Lightweight Directory Services Setup Wizard
Results	.NET Framework 3.5 Features
	.NET Framework 3.5 (includes .NET 2.0 and 3.0)
	Remote Server Administration Tools Role Administration Tools
	AD DS and AD LDS Tools
	AD LDS Snap-Ins and Command-Line Tools
	You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details. Export configuration settings
	< <u>P</u> revious <u>N</u> ext > Close Cancel

**10. NOTE:** AD LDS Role is successfully set up. Create a new AD LDS Instance as "Instance1" using the wizard.

Active Directory L	ightweight Directory Services Setup Wizard	x
	Welcome to the Active Directory Directory Securices         Setup Wizard         This wizard helps you install Microsoft Active Directory Lightweight Directory Services (AD LDS).         AD LDS is a powerful directory service that is easy to install and deploy. It provides a dedicated data store for applications, and can be configured and managed independently.         To continue, click Next.	
	< Back Next > Cancel Help	

11. Click the Run the Active Directory Lightweight Directory Services Setup Wizard shown in the above screen. And then click Close.

**NOTE:** This entire procedure implemented and documented based on Windows 2012 edition.

# **Creating AD LDS Instance**

- 1. Open Server Manager.
- 2. In the Console tree, select Roles> select Active Directory Lightweight Directory Services from Roles Summary section.

L	Add Roles and Features Wizard	_ <b>D</b> ×
Select server roles Before You Begin Installation Type Server Selection Server Roles Features AD LDS Confirmation Results	Add Roles and Features Wizard         Select one or more roles to install on the selected server.         Roles         Active Directory Certificate Services         Active Directory Domain Services         Active Directory Federation Services         Active Directory Rights Management Services         Active Directory Rights Management Services         DHCP Server         DNS Server         Fax Server         Wetwork Policy and Access Services         Print and Document Services	DESTINATION SERVER WIN-ISQI9N3LK72.mxone.local Description Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure of Active Directory Domain Services. Multiple instances of AD LDS can exist on a single server, each of which can have its own schema.
	Remote Access  Remote Desktop Services	
	< Previous Next	> Install Cancel

- 3. Click Next> Next...until the AD LDS Role is successfully setup. Refer the step 10 and 11 of Enabling AD LDS in Windows Server.
- 4. Select A unique instance displayed in the **Setup Options**. Click **Next**.

0	Active Directory Lightweight Directory Services Setup Wizard
Se	etup Options An AD LDS instance is created each time AD LDS is installed.
	You can create a unique instance, or you can install a replica of an existing instance.
	Select the type of instance you want to install.
	A unique instance
	This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.
	○ A replica of an existing instance
	This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.
	< Back Next > Cancel Help

5. Enter the Instance name and Description. Click Next.

Active Directory Lightweight Directory Services Setup Wizard
Instance Name The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.
Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended. Instance name:
Instance1 Example: Addressbook1
Description: AD LDS instance
The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter. AD LDS service display name: instance1
AD LDS service name: ADAM_instance1           < Back

- Enter the LDAP port number and LDAPS SSL port number that should be accessed from other applications to AD LDS; Or,
- 7. Click Next and continue with default ports.

**NOTE:** If you are installing AD LDS in the same server where Active Directory is installed, then it changes the port series from 50000. Otherwise, it gives default LDAP/s port such as 389, 636.

	Active Directory Lightweight Directory Services Setup Wizard
Po	orts Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.
	The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below. If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.
	LDAP port number: SOUDD SSL port number: 50001
	< <u>B</u> ack <u>N</u> ext > Cancel Help

8. Select Yes, create and application directory partition and enter the Partition name. Click Next.

Active Directory Lightweight Directory Services Setup Wizard
Application Directory Partition An application directory partition stores application-specific data.
Do you want to create an application directory partition for this instance of AD LDS?
No, do not create an application directory partition Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.
<ul> <li>Yes, create an application directory partition</li> </ul>
Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name: CN=Partition1,DC=Woodgrove,DC=COM
Partition name:
DC=wbmusersadldsdomain,dc=com
< Back Next > Cancel Help

Э.	Using the default values for storage location of ADLDS files. Click <b>Next</b> .			
Ě	Active Directory Lightweight Directory Services Setup Wizard			
	File Locations You can specify a location for each type of file associated with this instance of AD LDS.			
	Specify the locations to store files associated with AD LDS.			
	Data files:			
	C:\Program Files\Microsoft ADAM\instance1\data Browse			
	Data recovery files:			
	C:\Program Files\Microsoft ADAM\instance1\data Browse			
-				
	< <u>B</u> ack <u>N</u> ext > Cancel Help			

10. Choose Network service account for running the AD LDS Service. Х Active Directory Lightweight Directory Services Setup Wizard Service Account Selection AD LDS performs operations using the permissions associated with the account you select. Set up AD LDS to perform operations using the permissions associated with the following account. Network service account AD LDS has the permissions of the default Windows service account. O This account: AD LDS service has the permissions of the selected account. User name: Ω Browse .... Password: Cancel < <u>B</u>ack <u>N</u>ext > Help

**11.** You will receive a prompt warning about data replication. Since you are using a single LDAP Server, click **Yes**.

🔄 Ac	tive Directory Lightweight Directory Services Setup Wizard 🔽		
You have selected a system service account for this Active Directory Lightweight Directory Services instance. Because this computer is not a member of a domain, this instance will not be able to replicate data with AD LDS instance on other computers while using this service account. Do you want to continue?			
	Yes No		

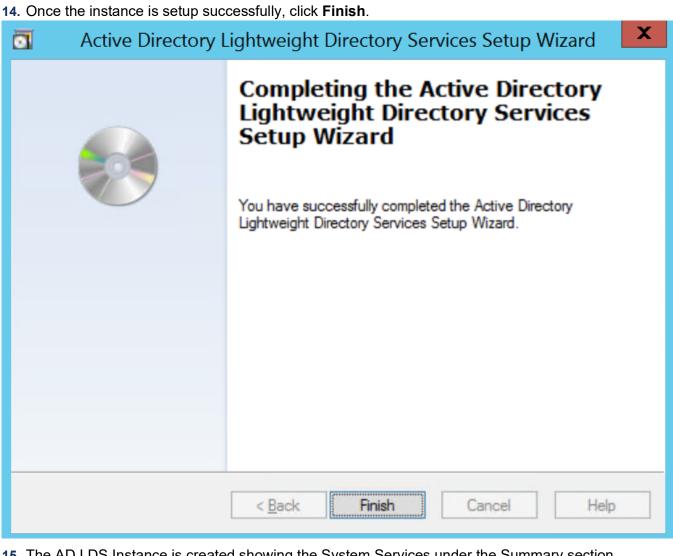
**12.** Select the below 3 LDF files from the Importing LDIF Files window.

The sector of th	X
File Locations You can specify a location for each type of file associated with this instance of AD LDS.	
Specify the locations to store files associated with AD LDS.	
Data files: C:\Program Files\Microsoft ADAM\instance1\data Browse	]
Dgta recovery files:	_
C:\Program Files\Microsoft ADAM\instance1\data Browse	]
< <u>B</u> ack <u>N</u> ext > Cancel He	lp

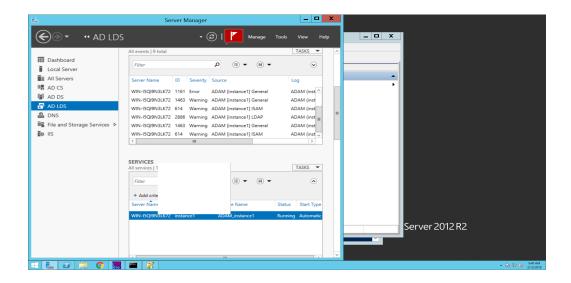
- a. MS-InetOrgPerson.LDF
- b. MS-User.LDF
- c. MS-UserProxyFull.LDF

13. Verify that all the selections are right and then Click <b>Next</b> to comministaliation.	
Active Directory Lightweight Directory Services Setup Wiza	ard X
<b>Ready to Install</b> The AD LDS Setup Wizard is ready to install AD LDS with the following configuration.	
Before continuing, review and confirm your selections.	
Selections:	
Install a unique instance of AD LDS.	^
Instance name: instance1 Computers will connect to this instance of AD LDS using the following ports: LDAP port: 50000 SSL port: 50001	=
AD LDS replication will use Negotiate authentication.	
Store AD LDS data files in the following location:	~
To change your selections, click Back. To install AD LDS, click Next.	
< <u>B</u> ack <u>N</u> ext > Cancel	Help

Ö	Active Directory Lightweight Directory Services Setup Wizard
	Installing AD LDS The AD LDS Setup Wizard is installing AD LDS.
	Installing AD LDS
	Please wait while the wizard completes the following steps.
	Importing LDIF file MS-ADAM-Upgrade-2.ldf
;	
	< <u>B</u> ack <u>N</u> ext > Cancel Help



15. The AD LDS Instance is created showing the System Services under the Summary section.

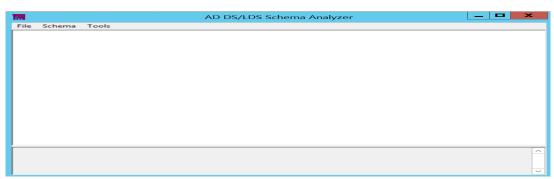


# Creating the Custom LDF File to suit for AD LDS Setup

1. Open Command Prompt and then Go to C:\Windows\ADAM.



2. Execute ADSchemaAnalyzer.exe that displays a new window AD DS / LDS Schema Analyzer.



3. In Schema Analyzer window, go to File Menu and then select Load Target Schema.



- 4. In Load Target Schemadialog box, provide the following details:
  - a. Server[:port]: [Give IP address of Active Directory Server]: [Active Directory port]
  - b. Username: [Username to connect to Active Directory]
  - c. Password: [Password of above username of Active Directory]
  - d. Domain: [Domain of Active Directory which contains above user]

Load targ	get schema 📃 🗖 🗙
1	
Server[:port]	10.211.159.143
<u>U</u> sername	administrator
Password	
<u>D</u> omain	mxone
Bind type	
Server type	
Auto	
AD DS/LDS	S
C Generic (s	ubschemaSubentry)
Load LDIF	Ok Cancel

**NOTE:** If you do not provide port number after server IP/DNS Name, it takes default LDAP port that is 389.

- 5. Click Ok.
- AD DS/LDS Schema Analyzer screen shows the following folder structure. Once it is connected to Active Directory Server.

1998	AD DS/LDS Schema Analyzer	_	-	×
File Schema Tools				
🗈 🧰 Classes				
Attributes     Property sets				
in the party sets				
Validating schema Schema is ok.				~
Processing dependencies Loaded schema: 1472 attributes, 264 classes, 80				
Loaded schema: 14/2 attributes, 264 classes, 80	property sets.			

7. Go to File Menu and then select Load base schema.

🕌 AD D5/LD5 Schema Analyzei	×
File Schema Tools	
Load target schema Ctrl+T	
Load base schema Ctrl+B	
create tour file Ctri+t	
Exit	

- 8. The Load base schema dialog box appears to enter the following details:
  - a. Server[:Port]: [Give IP address of AD LDS]:[AD LDS port]
  - b. Username: [Administrator Username of the local server]
  - c. Password: [Password of Administrator]
  - d. Domain: [Domain of Active Directory which contains above user]

11	AD DS/LDS Schema Analyzer	DX
File Schema To	pols	
	Load hase schema – 🗖 🗙	
Validating schema		

- 9. Click Ok.
- 10. Go to Schema Menu and then select Mark all non-present elements as included.

1000		AD DS/LDS Scho	ema Analyzer	• ×
File	Schema	Tools		
8.0		e present elements w present elements		
	Mar	k all non-present elements as included		
-				
4				
4				
4				

- 11. Click Ok.
- 12. Go to File Menu and then select Create LDIF file.

									 		_
			AD DS/L	LDS Sche	ema An	alyzer		L	 -	>	<
File	Schema Tools										
	Load target schema	Ctrl+T									
	Load base schema	Ctrl+B									
	Create LDIF file	Ctrl+L									
	Exit										
			1								
ade	d schema: 1472 attributes. 2	264 classes, 80	property sets								

- **13.** In the File Dialog box provide the path of LDIF file to store.
- 14. By default, it shows C:\Windows\ADAM Path.
- **15.** Enter name of the file and click **Save**.
- **16.** Open Command Prompt and then Go to C:\Windows\System32.
- **17.** Execute the following 3 commands as mentioned below:
  - ldifde -i -u -f [Path of LDIF File which is created by using Schema Analyzer]
     -s [IP address of AD LDS]: [Port of AD LDS] -b [Administrator Username of the local server ] [Domain of Active Directory which contains above user] [Password of Administrator] -j . -c "cn=Configuration,dc=X" #configurationNaming-Context

For example,

ldifde -i -u -f c:\windows\adam\ADLDSSyncProxy3\_129.ldf -s
192.168.26.129:50000 -b administrator pmsnmdomain XXXXXXXXXXX -j .
-c "cn=Configuration,dc=X" #configurationNamingContext



ldifde -i -f c:\windows\adam\MS-AdamSyncMetadata.ldf -s [IP address of AD LDS]:[Port of AD LDS] -b [Administrator Username of the local server ] [Domain of Active Directory which contains above user] [Password of Administrator] -c CN=Configuration,DC=X #ConfigurationNamingContext

For example,ldifde -i -f c:\windows\adam\MS-AdamSyncMetadata.ldf -s
192.168.26.129:50000 -b administrator pmsnmdomain XXXXXXXXXXX -c
CN=Configuration,DC=X #ConfigurationNamingContext



ldifde -i -f c:\windows\adam\MS-adamschemaw2k8.ldf -s [IP address of AD LDS]:[Port of AD LDS] -b [Administrator Username of the local server ] [Domain of Active Directory which contains above user] [Password of Administrator] -c CN=Configuration,DC=X#ConfigurationNamingContext

For example,ldifde -i -f c:\windows\adam\MS-adamschemaw2k8.ldf -s
192.168.26.129:50000 -b administrator pmsnmdomain XXXXXXXXXX -c
CN=Configuration,DC=X#ConfigurationNamingContext

C:\Users\Administrator>cd c:\Windows\System32	
c:\Windows\System32>ldifde -i -f c:\Windows\ADAM\MS-AdamSyncMetadata.LDF -s 10.2 11.159.143:50000 -b administrator mxone Mitel0123 -c CN=Configuration,DC=X #Conf igurationNamingContext	6
Connecting to "10.211.159.143:50000" Logging in as "administrator" in domain "mxone" using SSPI	
Importing directory from file "c:\Windows\ADAM\MS-AdamSyncMetadata.LDF"	1
Loading entries	
1208 entries modified successfully.	
The command has completed successfully	
c:\Windows\System32>	1

## **Restarting the AD LDS Instance**

- 1. Select Server Manager > Roles > Active Directory Lightweight Directory Services.
- 2. Check for **System Services** section that is displayed in the right side pane.

	Server Manager		
) 🔿 🗧 📢 AD LDS	- 🗭   🗾 Manage To	pols View Help	
	All events   9 total		
Dashboard Local Server	Filter P (B) • (B) •	•	
All Servers	Server Name ID Severity Source	Log	
AD CS	WIN-I5QI9N3LK72 1161 Error ADAM [instance1] General	ADAM (inst ^	
AD DS	WIN-I5QI9N3LK72 1463 Warning ADAM [instance1] General	ADAM (inst	
AD LDS	WIN-I5QI9N3LK72 614 Warning ADAM [instance1] ISAM	ADAM (inst	
DNS	WIN-I5QI9N3LK72 2886 Warning ADAM [instance1] LDAP	ADAM (inst	
ile and Storage Services ▷	WIN-I5QI9N3LK72 1463 Warning ADAM [instance1] General	ADAM (inst	
IS	WIN-I5QI9N3LK72 614 Warning ADAM [instance1] ISAM	ADAM (inst 🗸	
	SERVICES All services 1 Start Services	TASKS 💌	
	Stop Services           Filter         Restart Services	$\odot$	
	+ Add crite Pause Services Resume Services Server Name Services	Status Start Type	
	Сору		
	WIN-I5QI9N3LK72 instance1 ADAM_instance1 R	tunning Automatic	
		Server 2012 R2	

3. Select the AD LDS Instance Name and right click on the AD LDS instance, select **Restart/Stop – Start**.

# Creating an Admin User in AD LDS

- 1. Select Server Manager > Roles > Active Directory Lightweight Directory Services.
- 2. Select ADSI Edit shown in the right side pane, under the Advance Tools section.

Time	Server Manager		
Cor · AD LDS	• @ I 🗾	Manage 🔤	Active Directory Administrative Senter
Contrological Services     Control Contro Control Control Control Control Control		1) General 1) General 1) General 1) General 1) General	Active Stready designs and Factor Active Stready designs and Factor Comparison of Active Comparison of A

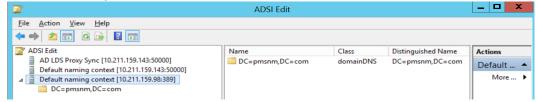
3. In ADSI Edit window, go to Action Menu, select Connect to... option, or right click on ADSI Edit in the left side pane.

2		ADSI Edit	- 0	
File Action View Help				
Connect to	159,143:50000] 211.159,143:50000] 211.159,98:389]	Name AD LDS Proxy Sync [10.211 Default naming context [10 Default naming context [10	domainDNS	Actions ADSI Edit More Actions

4. The Connection Settings window appears to fill the below details.

Connection Settings
Name: Default naming context
Path: LDAP://10.211.159.143:50000/DC=wbmusersadldsdomain,dc=c
Connection Point
Select or type a Distinguished Name or Naming Context:
DC=wbmusersadldsdomain,dc=com v
○ Select a well known Naming Context:
Default naming context 🗸 🗸
Computer
• Select or type a domain or server: (Server   Domain [:port])
10.211.159.143:50000
O Default (Domain or server that you logged in to)
Use SSL-based Encryption
Ad <u>v</u> anced OK Cancel

- 5. Enter Name to identify this AD LDS Instance.
- 6. In the Connection Point section, Select or type Distinguished Name or Naming Context and enter the Partition Name in AD LDS instance.
- 7. In the Computer section, Select or type a domain or server: (Server | Domain[:Port]) and enter the server IP of AD LDS and port details.
- 8. Click OK. The following ADSI Edit window appears.



- 9. Right click on Partition/ Distinguished Name > select New > Object.
- **10.** In ADSI Edit window, you can expand the right side pane to check Name and Distinguished Name.

#### **11.** In Create Object window > select container from the class list provided below.

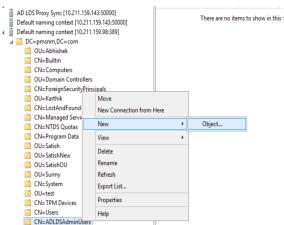
2	ADSI Edit	_ 🗆 X
File Action View Help	Create Object X	ned Name Actions
AD LDS Proxy Sync [10.211.159.143: Default naming context [10.211.159 Default naming context [10.211.159 Default naming context [10.211.159 Default naming context [10.211.159 CN=Builtin CN=Builtin CN=Computers OU=Domain Controllers OU=Domain Controllers OU=CN=ForeignSecurityPrincipe OU=Karthik CN=LostAndFound CN=Managed Service Accout CN=NTDS Quotas CN=Program Data	Select a dass:	hek,DC=pmsin p,DC=pmsin puters,DC=pm in Controllers gnSecurityPrin k,DC=pmsnm ndFound,DC= ged Service A Quotas,DC=p am Data,DC= ,DC=pmsnm, New,DC=pmsr
CUL-Satish CUL-Satish OU-SatishNew OU-SatishOU OU-SatishOU OU-Sunny CN-System	< <u>Back</u> <u>N</u> ext > Cancel Help ☐ CN=Users container CN=Use	y,DC=pmsnm, m,DC=pmsnn C=pmsnm,DC Devices,DC=p trs,DC=pmsnm,I

- **12.** Click Next. The Create Object window appears to add value.
- **13.** Enter name of the container in the Value box. For example, ADLDSAdminUsers and click Next.

	Create Object
Attribute:	a
Syntax:	Unicode String
Description:	Common-Name
<u>V</u> alue:	ADLDSAdminUsers
	< Back Next > Cancel Help
	< <u>B</u> ack <u>N</u> ext > Cancel Help

14. Click Finish.

**15.** Right-click on the newly created container which is added under the Partition Name and select New > Object.



16. In the Create Object window, select user from the list of Class items displayed. Click Next.

Create Object	2
Select a dass:	
volume	
< Back Next > Cancel Help	]

17. Enter a username (for example, adldsadmin) in the Value box.

<u>V</u> alue:	adldsadmin
	< Back Next > Cancel Help

18. Click Next ? click Finish.

**19.** Expand newly created container and right click on the newly created user. The following window appears to Reset Password.

CN=adldsadmin	user	<u>CN=adl</u> dsadmin,CN
	Move	
	New Connection from Here	
	Reset Password	
	New	•
	Delete	
	Rename	
	Refresh	
	Properties	
	Help	

**20**. Select Reset Password. The following window appears to assign a new password for user.

	Reset Password X
<u>N</u> ew password:	*******
Confirm password:	*******
The account must log off a effect.	and then log on again for the change to take
	OK Cancel

- 21. Enter the New password and Confirm password. Click OK.
- 22. Right click on the newly created user and select Properties.

urar	CNI-ad	ldsadmin, Cl
Move		
New Connection from Here		
Reset Password		
New	•	
Delete		
Rename		
Refresh		
Properties		
Help		
	Move New Connection from Here Reset Password New Delete Rename Refresh Properties	Move New Connection from Here Reset Password New > Delete Rename Refresh Properties

l=A

23. Right click on the newly created user properties dialog, select displayName and double click on it. The following String Attribute Editor appears.

CN=	adldsadmin F	Properties	? X	
ttribute Editor Security				isting N=ad
Attributes:				
Attribute	Value		^	
destinationIndicator	<not set=""></not>			
displayName	<not set=""></not>			
displayNamePrintable	<not set=""></not>			
	String Att	ribute Editor		X
<u>A</u> ttribute: c Value: adldsadmin Qlear	displayName	OK	Car	ncel
facsimileTelephoneN				
flags	<not set=""></not>		~	
< 111			>	
Edit			Filter	

- 24. Enter the same username while resetting the password.
- 25. Select distinguishedName ? double click on it to copy the distinguishedName value.
- 26. Click OK.

2	destinationIndicator	<not set=""></not>	
	displayName	adldsadmin	
	displayNamePrintable	<not set=""></not>	
	distinguishedName	CN=adldsadmin.CN=ADLDSAdminUsers.DC:	
	division	<pre><not set=""></not></pre>	
			×
	ttribute: distingui	ishedName	
Va	alue:		
	N=adldsadmin CN=ADLD	SAdminUsers, DC=pmsnm, DC=com	
	Clear	OK Cancel	
			_
	<	>	
	View	Filter	
			÷.
	OK	Cancel <u>A</u> pply Help	

27. In the same attribute editor Select msDS-UserAccountDisabled and double click on it. The following Boolean Attribute Editor window appears.

CN=a	adldsadmin Properties ? 🗙	
Attribute Editor Attributes:	Value	
msDS-HABSeniorityIn msDS-PhoneticComp msDS-PhoneticDepar msDS-PhoneticDisola	<not set=""> <not set=""></not></not>	
msDS-PhoneticFirstN msDS-PhoneticLastN	Boolean Attribute Editor     Attribute: msDS-UserAccountDisabled	×
msDS-PrimaryComputer msDS-Site-Affinity msDS-SourceObjectDN	In Value: In Value: In O True	
msDS-SupportedEncr msDS-SyncServerUrl	<r an="" false="" not="" set<="" td=""><td></td></r>	
msDS-UserAccountDi msDS-UserDontExpir ms-DS-UserEncrypte	cn OK Cancel	
< III		

- 28. Select False and click OK.
- **29.** Click Apply > OK.
- **30.** Expand the newly created partition name and CN=Roles. Right click on CN=Administrators?Properties to view the Attribute Editor.

¥.	ADSI Edit	Nan	ne Cl	Actions
	AD LDS Proxy Sync [10.211.159.143:50000 ⊿ 📋 DC=wbmusersadldsdomain,dc=com	l ha	ere are no items to show in this	CN=Administrators
	2 OC=worndsersadiosdomain, ac=com CN=LostAndFound		view.	More Actions
	CN=LOSTANDround CN=NTDS Quotas			
			_	
	CN=Adm Move			
	CN=Read	ion from Here		
	CIV=03CI:	ion non nere	-	
	▲ CN=ADLDSA New	,		
	CN=adld Default naming cont	,	-	
			-	
	Default naming cont			
1	Rename			
	Refresh			
	Export List			
	Properties			
	Help			

31. In the Attribute Editor, select member and click Edit.

CN=A	dministrators P	roperties	?	X
Attribute Editor				
Attri <u>b</u> utes:				
Attribute	Value			~
isCriticalSystemObject	TRUE			
labeledURI	<not set=""></not>			
last Known Parent	<not set=""></not>			
legacyExchangeDN	<not set=""></not>			
managedBy	<not set=""></not>			≡
member	CN=Administrators,	CN=Roles,CN=Co	onfigura	ati
memberUid	<not set=""></not>			
msDS-AzApplicationD	<not set=""></not>			
msDS-AzBizRule	<not set=""></not>			
msDS-AzBizRuleLang	<not set=""></not>			
msDS-AzGenericData	<not set=""></not>			
msDS-AzLastImporte	<not set=""></not>			
msDS-AzLDAPQuery	<not set=""></not>			
mS-DS-ConsistencyC	<not set=""></not>			~
< 111			>	•
Edit			<u>F</u> ilter	
ОК	Cancel	Apply	Н	elp

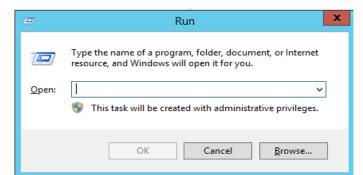
**32.** Click Add DN button > Enter DN of user created above (for example, CN=adldsadmin,CN=ADLDSAdminUsers,DC=wbmusersadldsdomain,DC=com) ? click OK.

Multi-	valued Distinguished Name With Secu	urity Principal Editor
<u>A</u> ttribute: memb Values:	er	
Name	Container	Distinguished Name / SID
Administrators	/{3F4B7CE3-7285-4C60-A9D2-0514813AB5	CN=Administrators,CN=Roles,CN
	Add Distinguished Name (E	DN) ×
	Enter a distinguished name (DN) for an obj	ect.
	DSAdminUsers,DC=wbmusersadldsdomain	n,DC=com
	ОК	Cancel
Add Windows Account.		<u>R</u> emove
Add <u>D</u> N		
		OK Cancel

**33.** Click OK > click Apply > click OK.

## **Checking User Authentication**

1. On the Start Menu, click Run. The following Run program window appears.



- 2. Type ldp.exe (Label Distribution Protocol) in the Run box and click OK to open Ldp.exe window.
- 3. In LDP window, Go to Connection and click Connect.

£?				Ldp	
Connection	Browse	View	Options	Utilities	Help
Connect	t				
Bind		Ctrl+B			
Disconn	ect				
New		Ctrl+N			
Save					
Save As					
Exit					

4. Enter the IP Server address and Port number of AD LDS Instance and click OK.

	Conne	ect X
Server:	10.211.159.143	
Port:	50000	Connectionless
<u>O</u> K	:	<u>C</u> ancel

5. Go to Connection and click Bind. The following Bind window appears.

	Bind				
<u>U</u> ser: <u>P</u> assword: Domain:	Password:				
Bind type Bind as <u>c</u> u Bind with Simple bin	_				
✓ Encrypt traffic after bind       Advanced       OK					

- 6. To connect and bind the server that hosts the forest root domain of your AD DS environment. Enter the following details:
  - a. User: [username which is created above]
  - b. Password: [Password of the above user]
  - c. Domain: By default, remains in deactivate mode
  - d. Bind Type: [select Simple bind]
  - e. Click OK.

NOTE: The user must be an authenticated user as mentioned in the above screen.

f. An example of successful authentication is given below.

res = ldap_simple_bind_s(ld, 'adldsadmin', <unavailable>); // v.3</unavailable>
Authenticated as: 'CN=adldsadmin,CN=ADLDSAdminUsers,DC=wbmusersadldsdomain,DC=com'.

# Adding Attributes to UserProxyFull Class

1. On the Start Menu, type FMC, and then click OK. The following Console window appears.

			Ŷ	
<b>a</b>	Console1 -	[Console Root]		_ 🗆 🗙
🚟 File Action View Favorit	tes Window Help			_ & ×
⇐ ➡ 🔲 🖬 🖬				
Console Root	Name		Actions	
	There are no items to show i	n this view.	Console Root	<b>^</b>
			More Actions	•

2. Go to File menu > click Add/Remove Snap-in.

5					
	File	Action	View	Favorites	Window
٢		New			Ctrl+N
r		Open			Ctrl+0
		Save			Ctrl+S
		Save As			
		Add/Rem	ove Sna	p-in	Ctrl+M
		Options			
		1 adsiedit			
		2 lusrmgr			
		Exit			

3. Select Active Directory Schema, click Add and then click OK.

P				Console Root	Edit Extensions
Active Directory Domains a Active Directory Schema	Microsoft C	≡		Active Directory Schema	Remove
Active Directory Sites and Active Directory Users and ActiveX Control					Move Up
ACTIVEX CONTROL ADSI Edit Authorization Manager	Microsoft C Microsoft C		Add >		Move Down
Certificate Templates Certificates	Microsoft C Microsoft C				
Certification Authority Component Services	Microsoft C Microsoft C	1 1			
Computer Management Device Manager	Microsoft C Microsoft C				
III	>				Advanced

4. Right click on Active Directory Schema and select Change Active Directory Domain Controller.

<u>File</u> <u>Action</u> <u>View</u> Favo	rites <u>W</u> indow <u>H</u> elp
🗢 🔿 🙍 🖬 🖉	
Console Root	Name Name Change Active Directory Domain Controller Connect to Schema Operations Master Operations Master Permissions Reload the Schema View New Window from Here New Taskpad View Refresh Export List Help

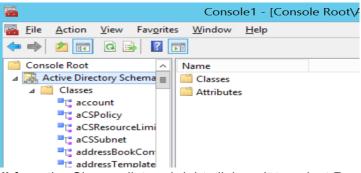
5. Select This Domain Controller or AD LDS instance.

	rrent Directory Server: WIN-I5QI9N3LK72.mxone.local								
Change to:	ange to:								
<u>Any write</u>	able Domain Contr	oller							
① This Do	main Controller or A	AD LDS instance							
<u>L</u> ook ii	n this domain:	mxone.local 🗸							
Nam	Name Site DC Type DC Version Status								
<typ< td=""><td colspan="7"><type a="" directory="" here="" name[:port]="" server=""></type></td></typ<>	<type a="" directory="" here="" name[:port]="" server=""></type>								
WIN	-15Q19N3LK72.mxo	ne.local	Default-First-Site-Name	GC	Windows	Unavailable			

6. Enter IP Address of the AD LDS Instance with port number and click outside of the highlighted edit area. The Status column value changes to Online.

Change to:										
O <u>A</u> ny writable Domain Controller										
● <u>T</u> his Domain Controller or AD LDS instance										
Look in this domain:	Look in this domain: mxone local									
Name		Site	DC Type	DC Version	Status					
10.211.159.143:50000										
• This Domain Controller or A	AD LDS instance									
Look in this domain:	mxone.local					¥				
Name		Site	DC Type	DC Version	Status					
10.211.159.143:50000					Online					

- 7. Select this entry (that is, anywhere outside from the edit section) > click **OK** > click **Yes**.
- 8. Expand **Classes** to select the required attributes displayed in the **Classes** list.



9. Select userProxyFull from the Classes list and right click on it to select Properties.

kayakile Royakile Royakile Royaki		Cornes		rowse View Opt	K72.moone.local.500 ions Utilities Help POLICY-HINTS (; 12.844 H 2444 11304   4.2044 Consolal   4.[Consol	3556 1.4 225	H	ama (10.211	159 142-5	_ D				
	H		an Min Ri	Artico View	Favorites Window		cine breakly built	ana (receri		toroj(dases/aserri	Judya		. 8 X	
	П					nep							- 214	
	Ш													
	Ш			timpleSecu			defaultClassStore	Туре	System Yes	Description Default-Class-Store	^	Actions	_	
	Ш			t site	nyoujeci		detautulassitore dynamicLDAPServer	Optional Optional	Yes	Dynamic-LDAP-Server	-	userProxyFull	•	
	Ш			stelink			lastLogonTimestamp	Optional	Ves	Last-Logon-Timestam		More Actions		
	Ш			💐 sitel.inkBris			preferredOU	Optional	Yes	Preferred-CU	1			
	Ш			💐 sitesContai	ner	- Li	userParameters	Optional	Yes	User-Parameters				
	Ш			storage		1	userFrincipalName	Optional	Yes	User-Principal-Name				
	Ш			t subnet			userCettificate	Optional	Yes	3509-Cet				
	Ш			subschem			businessCategory	Optional	Yes	Business-Category				
	Ш				AuxConfiguration		home?hone	Optional	Yes	Phone-Home-Primary				
	Ш			t syncEngine			initials	Optional	Yes	Initials				
	Ш	Ready		top .			mail	Optional	Yes	E-mail-Addresses				
	Ľ	_		trustedDor	rain		manager	Optional	Yes	Manager				
	Ŀ			typeLibrary			mobile	Optional	Yes	Phone-Mobile Primar	5			
	Ŀ			tser			o "pager	Optional	Yes	Organization-Name				
	Ŀ			usePrové volume	View		autio	Optional Optional	TES No	Phone-Pager-Primary The Audio attribute ty				
	Ŀ			Attributes	New Window from He		caticense	Optional	No	Vehicle license or regi				
	Ŀ			- HINDOND		re	departmentNumber	Optional	No	Identifies a department				
	R		۲.		New Taskpad View		Sector of College	II	110		1			
	F	-	Opens	the properties d	Refresh									
	-	_	-		Export List						-	-		
					Properties	_								
					Help	-								
						_								
8		2	3	) 🖁 \land	5									- 18 19 16 40

10. Go to Attributes tab and check for the sAMAcountName attribute. If sAMAcountName attribute is not available, then click Add button to include it to the Schema Object list.

	userProxyFull Properties
General Relation	nship Attributes
■t <mark>=</mark>	userProxyFull
<u>M</u> andatory:	
Optional:	roomNumber Add
	secretary uid userCettificate userParameters userPKCS12 userPfincipalName userSMIMECettificate x500uniqueIdentifier ✓
	OK Cancel Apply Help

11. Select sAMAccountName > click OK > click Apply > click OK.

Select Sch	nema Object
	,
Select a schema object:	
-	
rpcNsCodeset	<u>^</u> ОК
rpcNsEntryFlags	
rpcNsGroup rpcNsInterfaceID	Cancel
rpcNsObjectID	
rpcNsPriority	
rpcNsProfileEntry	
rpcNsTransferSyntax	
sAMAccountName	
sAMAccount Type	
samDomain Updates	
schedule	
schemaFlagsEx	
schemaIDGUID	
schemalnfo	
schemaUpdate	
schemaVersion	
scopeFlags	
script Path	
sDRightsEffective searchFlags	

In the same way, you can check and add the below attributes:

- objectSID
- sn
- department
- location
- whenChanged
- telephoneNumber
- wWWHomePage
- description
- physicalDeliveryOfficeName
- url
- streetAddress
- postOfficeBox
- I[Locality-Name]
- st
- postalCode
- c[Country-Name]
- profilePath
- scriptPath
- title
- company
- facsimileTelephoneNumber
- otherFacsimileTelephoneNumber
- msExchAssistantName
- roomNumber
- ipPhone
- objectClass
- objectCategory
- lastAgedChange
- 12. Restart AD LDS Instance when all the required attributes are added and checked.

## Editing Object (UserProxyFull) Class as User Object Class

 In the ADSI Edit Console tree, click ADSI Edit node and then click the Action menu. Select Connect to. The Connection Settings dialog box appears.

Connection Settings
Name: ADLDDSSynchPoxy1Schema
Path: LDAP://10.211.159.143:50000/Schema
Connection Point
O Select or type a Distinguished Name or Naming Context:
✓
• Select a well known Naming Context:
Schema 🗸
Computer
<ul> <li>Select or type a domain or server: (Server   Domain [:port])</li> </ul>
10.211.159.143:50000 🗸
O Default (Domain or server that you logged in to)
Use SSL-based Encryption
Ad <u>v</u> anced OK Cancel

- 2. In Connection Point section, click Select a well known Naming Context radio button.
- 3. In Computer section, select or type a domain or server: (Server | Domain [:port]) of AD LDS Instance.
- 4. Select **Schema** from the drop-down list.
- 5. Expand Schema from left side pane > expand CN=Shema, CN=Configuration, CN={XXXXXX}}.

<u>File Action View H</u> elp
🗢 🧼 🚈 🗮 🗮 🖬 🖬 🖬 🖬
📝 ADSI Edit
Default naming context [10.211.159.98:389]
DC=pmsnm,DC=com
ADLDDSSynchPoxy1Schema [10.211.159.143:50000]
CN=Schema,CN=Configuration,CN={9F809790-2BBA

6. Select **CN=User**, and then right-click on it and select **Properties**.

CN=UPN-S	Suffixes	
CN=U	Move	
CN=U	New Connection from Here	•
CN=U	View	•
CN=U	Delete	
CN=U CN=U	Rename Refresh	
CN=U	Export List	
CN=U	Properties	
CN=u CN=u	Help	

7. Select **IDAPDisplayName** and double click on it to modify the selected attribute value.

С	N=User Properties ? X
Attribute Editor	
Attri <u>b</u> utes:	
Attribute	Value ^
defaultSecurityDescri	D:(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0
description	<not set=""></not>
displayName	<not set=""></not>
dSASignature	<not set=""></not>
fSMORoleOwner	<not set=""></not>
isCriticalSystemObject	<not set=""></not>
isDefunct	<not set=""></not>
last Known Parent	<not set=""></not>
IDAPDisplayName	user
mayContain	audio; carLicense; departmentNumber; displa
mS-DS-ConsistencyC	<not set=""></not>
mS-DS-ConsistencyG	<not set=""></not>
mustContain	<not set=""></not>
objectCategory	CN=Class-Schema,CN=Schema,CN=Configu 🗸
< 111	>
Edit	Filter
Low	
ОК	Cancel Apply Help

8. Change value to **userADLDS** (this is just a dummy name), then click **Apply**, and click **OK**.

	String Attribu	ute Editor	X
<u>A</u> ttribute: <u>V</u> alue:	IDAPDisplayName		
userADLDS			
Clear		OK Cancel	

9. In the same way, you can change the **IDAPDisplayName** value of **user-Proxy-Full** to user. Once the changed attribute value is applied, you must restart **AD LDS Instance**.

CN=User-Principal-N	lame 🛛
CN=User-Proxy-Full	
CN=User-Share	Move
CN=User-Share	New Connection from Here
CN=User-SMIN	N
CN=User-Work	New •
CN=userClass	View 🕨
CN=userPKCS1	Delete
CN=USN-Chan	_
CN=USN-Creat	Rename
CN=USN-DSA-	Refresh
CN=USN-Inters	Export List
CN=USN-Last-	-
CN=USN-Sourc	Properties
CN=Valid-Acce	Help
CN=Vendor	-

10. Change it to user. Click OK. Click Apply and then click OK.

	String Attribute Editor	X
<u>A</u> ttribute: <u>V</u> alue: user	IDAPDisplayName	
<u>C</u> lear	ОК	Cancel

# Modifying MS-AdamSyncConf File

1. Go to C:\Windows\ADAM Directory in windows. Copy and Paste *MS-AdamSyncConf.xml* file. Rename the newly created file (for example, *MS-AdamSyncConf\_Document.xml*).

	ADLDSSyncProxy_143	2/13/2019 6:14 AM	LDF File	1,895 KB
🌉 This PC	ldif.err	2/13/2019 6:09 AM	ERR File	1 KB
🛛 隆 Desktop	LDF file	2/12/2019 6:25 AM	LDF File	2 KB
🛛 📗 Documents	WBMSync	2/6/2019 2:15 PM	Text Document	2 KB
🛚 🗼 Downloads	MS-AdamSyncConf_Doc	1/8/2019 2:27 PM	XML Document	3 KB
🛛 🚺 Music	MS-AdamSyncConf1	1/8/2019 2:26 PM	Text Document	3 KB
🛛 📔 Pictures	ADLDSSyncProxy5_143	1/8/2019 1:20 PM	LDF File	3 KB
🛛 📔 Videos	🚳 adammsg.dll	1/8/2019 7:30 AM	Application extens	4 KB
🗅 🏜 Local Disk (C:)	adamntds.dit	1/8/2019 7:30 AM	DIT File	4,112 KB

2. Open the file in Edit mode (using Notepad) and modify below fields.

<source-ad-name>Domain Name of Active Directory</source-ad-name> <source-ad-partition>Partition Name of Active Directory</source-ad-partition> <source-ad-account>[user name of Active Directory Admin]</source-ad-account> <account-domain>[Above Username Account Domain]</account-domain> <target-dn>[DN/Partition in AD LDS]</target-dn> <base-dn>[DN of users from which we want to synchronize from Active Directory]</base-dn> For Example: <source-ad-name>pmsnmdomain.com</source-ad-name> <source-ad-partition>dc=pmsnmdomain,dc=com</source-ad-partition> <source-ad-account>administrator</source-ad-account> <account-domain>pmsnmdomain</account-domain> <target-dn>DC=wbmusersadldsdomain,dc=com</base-dn> Cause the medified file

3. Save the modified file.

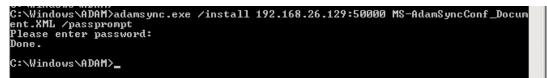
## Synchronizing Users from Active Directory to AD LDS Instance

- 1. Open Command Prompt. Go to C: \Windows\ADAM.
- 2. Execute the following 2 commands as mentioned below.
  - a. adamsync.exe /install [AD LDS Instance IP:Port] [MS-ADAMSyncConf.xml File Name] /passprompt

For example: adamsync.exe /install 192.168.26.129:53986 MS-AdamSyncConf Docuent.xml /passprompt

**NOTE:** To synchronize users from Active Directory to AD LDS Instance, you must run the Adamsync.exe utility.

Enter the password of Active Directory user which is mentioned in the XML file.



b. adamsync.exe /sync [AD LDS Instance IP:Port] "[DN/Partition Name of AD LDS]" /log [Log File Name]

For example: adamsync.exe /sync 192.168.26.129:53986 "DC=wbmusersadldsdomain,dc=com" /log WBMSync.log

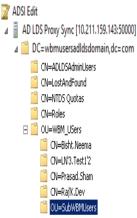


**NOTE:** WBMSync.log contains the user synchronization information from Active Directory to AD LDS. If any issues occurred while synchronization, it gets recorded in this log. All the users get synchronized from the Container to AD LDS except their passwords. So, you need to wait until the user synchronization process is completed.

## **Checking Synchronized Users in AD LDS**

- 1. Open Server Manager > expand Roles > select Active Directory Lightweight Directory Services.
- 2. In Advanced Tools section, select ADSI Edit that is displayed in the right side pane.
- 3. In ADSI Edit window, go to Action menu and select Connect to, then provide the below details.
- 4. In Connection Point section, click Select or Type Distinguished Name or Naming Context and enter Partition Name.
- In Computer section, click Select or type domain or server: (Server | Domain [:Port]) of AD LDS Instance.

6. (Enter the IP address of AD LDS server with port number, for example: 192.168.26.129:50000).



7. All the Active Directory Users of that particular container and sub-containers gets synchronized and visible under the **ADSI Edit** Console tree.

## Enabling LDAPS (SSL) for AD LDS in Window Server

- 1. Create a separate directory in the user location in the system.
- 2. Create a file adlds\_request.inf (file name can be anything with .inf extension).
- 3. Copy the below highlighted content in that file and change the required value in pink color.

**NOTE:** Remember that ";" is a comment in this file.

```
;-----[Version]
```

```
Signature="$Windows NT$"
```

```
[NewRequest]
```

```
Subject = "Fully Qualified name of AD LDS server" ; replace with the FQDN
of the DCKeySpec = 1KeyLength = bitsize can be any value from below line
values; Can be 1024, 2048, 4096, 8192, or 16384.; Larger key sizes are
more secure, but have; a greater impact on performance.Exportable =
TRUEMachineKeySet = TRUESMIME = FalsePrivateKeyArchive =
FALSEUserProtected = FALSEUseExistingKeySet = FALSEProviderName =
"Microsoft RSA SChannel Cryptographic Provider"ProviderType =
12RequestType = PKCS10KeyUsage =
0xa0[EnhancedKeyUsageExtension]OID=1.3.6.1.5.5.7.3.1; this is for Server
Authentication;------
```

4. Execute the below command in directory to create a certificate request.certreq -new <.inf file name> <certificate request file name>

An example of the command is mentioned below.



5. A new file is created in the same directory.

c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir>dir Volume in drive C has no label. Volume Serial Number is 3AC0-320A					
Directory of c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir					
11/11/2016 05:40 AM 〈DIR〉 . 11/11/2016 05:40 AM 〈DIR〉 . 11/11/2016 05:40 AM 〈DIR〉 . 11/11/2016 05:40 AM 1,380 ADLDS_Request_file.req 11/11/2016 02:19 AM 763 Certificate_request_details.inf 2 File(s) 2,143 bytes 2 Dir(s) 6,052,823,040 bytes free					
c:\Certificates\ADLDS_Certs\ADLDS_Keystore_Dir>_					

- 6. Share the file with Certificate Authority to provide the signed certificate.
- 7. Copy the file in the same directory (with preferred extension of .cer / .crt).

For example, the sample AD LDS Server Signed Certificate (in this **pmsnmdomain.com** is root certificate), which is certificate of Issuer who has issued certificate to AD LDS Instance. **Adldsserver.pmsnmdomain.com** – is the Signed Certificate of AD LDS Instance.

ertificate
General Details Certification Path
Certification path
View Certificate
Certificate status:
This certificate is OK.
Learn more about <u>certification paths</u>
ОК

8. Once you receive the signed certificate from Certificate Authority. Type the below mentioned command.certreq -accept <received signed certificate file name>

An example of the command is mentioned below.

c:\Certificates\ADLDS\_Certs\ADLDS\_Keystore\_Dir>certreq -accept ADLDS\_Cert\_Response.cer c:\Certificates\ADLDS\_Certs\ADLDS\_Keystore\_Dir>

- 9. Open Command Prompt and Run as Administrator.
- **10.** In the command prompt, execute *mmc* command that opens a new mmc window.

11. In the mmc window, go to File and select Add/Remove Snap-in option.

8	🚘 Console1 - [Console Root]						
-	File	Action	View	Favorites	Window	Help	
	Sa	en			Ctrl+N Ctrl+O Ctrl+S		
		ld/Remove tions	e Snap-i	n	Ctrl+M		

- 12. In the Add or Remove Snap Ins window, select Certificates from the left side pane and click on Add button.
- 13. Select Computer Account and click Next. Select Local Computer. Click Finish and then click OK.



 Extract Certificates > Personal > Certificates from the left side pane. All the certificates get listed in the right side pane.



- **15.** Open the Signed certificate which you have received from Certificate Authority.
- 16. Once the certificate is opened, go to **Details** tab and click on **Copy to File** button.
- 17. Click Next and select Yes, export the private key option.

Do you want to export the private key with the certificate? • Yes, export the private key • No, do not export the private key

18. Click Next.

<ul> <li>Personal Information Exchange - PKCS #12 (.PFX)</li> <li>Include all certificates in the certification path if possible</li> <li>Delete the private key if the export is successful</li> <li>Export all extended properties</li> </ul>	
<ul> <li>Delete the private key if the export is successful</li> <li>Export all extended properties</li> </ul>	Personal Information Exchange - PKCS #12 (.PFX)
Export all extended properties	$\square$ Include all certificates in the certification path if possible
	Delete the private key if the export is successful
Construction of contribution of contributions of contribu	Export all extended properties

- 19. Enter your password (double time) to assign to the Keystore and click Next.
- **20.** Save the .pfx file in the system in the same location where certificate request is created for easy identification.
- 21. Click Next and click Finish.
- 22. In the same mmc window, open File menu and select Add/Remove Snap-In option
- 23. Select Certificates and click Add.

ap-in	Vendor		Selected snap-ins:	Edit Extensions
Active Directory Do	Microsoft Cor			
Active Directory Sch	Microsoft Cor			Remove
Active Directory Site	Microsoft Cor	~~~~		
Active Directory Use	Microsoft Cor	Step 2		Move Up
Active Control	dicrosoft Cor	Ser -		
ADOTE Step 1	rosoft Cor		-	Move Down
Autoori	rosoft Cor	Add >		
Contribution Formy alles	Microsoft Cor	-		
Certificates	Microsoft Cor			
rcerancedon Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem				
Details Templates Ed		-1		Advanced
Device Manager	Microsoft Cor	<u> </u>	1	
cription:				

24. Select Service Account.



25. Select Local Computer, click Next.

Sele	ect Computer	X
	Select the computer you want this snap-in to manage.	
	This snap-in will always manage: C Local computer: (the computer this console is running on)	
	C Another computer: Browse	
	Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	

26. Select the Service Name / AD LDS Instance Name.

Ce	rtificates snap-in	×
	Select a service account to manage on the local computer.	
	Service account:	
	Active Directory Certificate Services	
I	Active Directory Web Services ADLDSProxySync1	
5	Application Experience Application Host Helper Service	
	Application Identity Application Information	
	Application Layer Gateway Service Application Management	
	ASP.NET State Service Background Intelligent Transfer Service	
	Base Filtering Engine Certificate Propagation	
	< Back Finish Cancel	

27. Click Finish and then click OK. The following Add or Remove Snap-ins window appears.

A	dd or Remove Snap-ins				
	You can select snap-ins for t extensible snap-ins, you can				r computer and configure the selected set d.
	Available snap-ins:			S	ielected snap-ins:
	Snap-in	Vendor		Γ	Console Root
	🛃 Active Directory Do	Microsoft Cor			🔜 Certificates - Service (ADLDSPr
	😹 Active Directory Sch	Microsoft Cor			
	📲 Active Directory Site	Microsoft Cor		۲	
	Active Directory Use	Microsoft Cor			
	📩 ActiveX Control	Microsoft Cor			-
	📝 ADSI Edit	Microsoft Cor		ı I	
	🛺 Authorization Manager	Microsoft Cor	Add >		-

- 28. In mmc Certificates window, expand Certificates Service (AD LDS Instance Name) on Local Computer. Add the AD LDS Signed Certificate in AD LDS Instance Name/Personal section.
- **29.** Click **Next** > **Browse**. Select the key store that you have created in previous step (file extension is .pfx) in File browser.
- 30. Click Next. Enter the password of key store (entered while creating .pfx file).
- **31**. Click **Next** > **Next** > **Finish**.

🚟 Console1 - [Console Root\Certificate	es - Service (ADLDSProxy	Sync1) on Local Computer\	ADAM_ADLD
🚟 File Action View Favorites Win	dow Help		
🗢 🔿 🙍 🖬 📋 🙆 🛃			
🧮 Console Root		Object Type	
🖃 🔄 Certificates - Service (ADLDSProxySy		Certificates	
	Find Certificates		
ADAM_ADLDSProxySync1\Enter     ADAM_ADLDSProxySync1\Interr	All Tasks I	Find Certificates	
E ADAM_ADLDSProxySync1\Trust	View	Import	
	New Window from Here	Advanced Operations 🔸	
	New Taskpad View	_	1
	Refresh		
	Export List		
	Help		
-		T	

Once it is added, certificate is available as shown below.

	www.console1 - [Console Root\Certificates - Service (ADLDSProxyS	sync1) on Local Computer\ADAM_A	DLDSProxySync1\Personal\Certifica	ites]		
	Tile Action View Favorites Window Help					
	** 2 🖬 🗋 0 3 🖬 🖬					
1	Console Root	Topyod To	Isound By	Expiration Date	Intended Purposes	Friendy Name
	Certificates - Service (ADLDSProxySync1) on Local Computer	adidsserver.pmsnmdomain.com	adldsissuer	11/9/2017	Server Authentication	<none></none>
	ADAM_ADLDSProxySync1(Personal					
	Certificates					
	ADAM ADLDSProxySync1\Trusted Root Certification Authoritik					

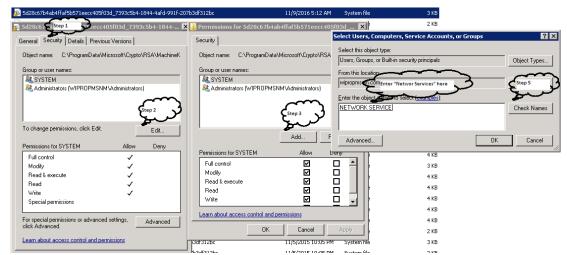
- 32. In the same way, add the AD LDS certificate's Root certificate (for example, pmsnmdomain.com) in AD LDS Instance Name/Trusted Root Certificate Authorities.
- 33. Add the AD LDS certificate's Root certificate in AD LDS Instance Name/Trusted Publishers.
- **34.** Add the other end certificate (for example, Provisioning Manager application certificate) in **AD LDS Instance Name/Trusted People**. An example is shown below.

	Console1 - [Console Root]
-	File Action View Favorites Window Help
	Console Root
	🗄 🧮 ADAM_ADLDSProxySync1\Trusted Root Certification Authoriti(
	🕀 🚞 ADAM_ADLDSProxySync1\Enterprise Trust
	🕀 🧮 ADAM_ADLDSProxySync1\Intermediate Certification Authoritie
	🗄 🧮 ADAM_ADLDSProxySync1\Trusted Publishers
	🗄 🧮 ADAM_ADLDSProxySync1\Untrusted Certificates
	🗄 🧮 ADAM_ADLDSProxySync1\Third-Party Root Certification Autho
	ADAM_ADLDSProxySync1\Trusted People
/nersh	hip to the added certificates to <b>Network Service</b> .

- **36.** Go to C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys.
- 37. Right click on each certificate where Lock like icon appears on the files.

📙 MachineKeys				
😋 🕞 🗢 Comput	er 🔹 Local Disk (C:) 🔹 ProgramData 👻 Microsoft 👻 Crypto 👻 RSA 👻 MachineKeys			
Organize 🔻 Include in li	orary 🔻 Share with 👻 New folder			
🔆 Favorites	Name	Date modified -	Туре	Size
🧮 Desktop	🚳 5d28c67b4ab4ffaf5b571eecc405f03d_7393c5b4+1844+4afd-991f-207b3df312bc	11/9/2016 5:12 AM	System file	3 KB
Downloads	fcaab588e2f0c2458ab11343dee9e941_7393c5b4-1844-4afd-991f-207b3df312bc	10/21/2016 6:43 PM	System file	2 KB
🖳 Recent Places	🔊 555a0477e214d0e2b6b0debc3cb4f6e2_7393c5b4-1844-4afd-991f-207b3df312bc	10/13/2016 8:57 PM	System file	2 KB
🧮 Libraries	🔊 16602d419d1c4a1f5ff53c985e650796_7393c5b4-1844-4afd-991f-207b3df312bc	8/18/2016 1:06 AM	System file	3 KB

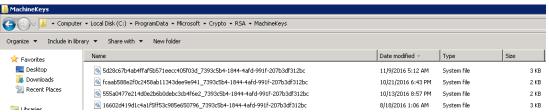
38. Open Properties and go to Security tab. Click Edit and then click Add. Enter Network Service.



- **39.** Enter the **Network Service** and select **Users, Computer, and Service Accounts or Groups** window.
- 40. Give Read, Read & Execute permission > click OK > OK.

Permissions for 5d28c67b4a	b4ffaf5b571eec	:c405f03d 🗵
Security		
' Object name: C:\ProgramData	\Microsoft\Crypto\	RSA\MachineK
Group or user names:		
SYSTEM		
& NETWORK SERVICE		
💁 Administratore (U/IPROPMS)	NMVA dministrators	
-		
1	Add	Bemove
	Add	
Permissions for NETWORK SERVICE	Allow	Deny
Full control		
	H	
Modify Board & average to		- H II
Read & execute		
Read		┛╠╺╢
Write		

**41.** In the same way, provide permissions to all certificates for **Network Service** user. When you give the permissions, all the **Lock** icons get disappeared.



**42.** Restart **AD LDS Instance**. Test LDAPS for AD LDS by using the below command from **PM installed** server.

```
openssl s_client -connect IPAddress of AD LDS:LDAPS port
For example:
openssl s_client -connect 192.168.26.129:53994
```

# Using AD LDS as a User Repository in PM Application

To Import Users into PM, do the following:

- 1. Login to PM application.
- 2. Select System menu > select Data Management sub menu > select Active Directory.

		MiVoice MX-ONE Provisio	×			
🕅 Mi	tel	Provisioning Ma	nager			
Users	Services	Administrators	System	Logs	Own Settings	
Location	Subsys	stem Data Manag	ement	Options	Email Server	Configuration Wize
Compare with	Subsystem	Active Directory	Server - C	hange		
Backup & Rest	ore	Apply				
Scheduling						
Active Director	у	Server Configure Do	mains			
		General Settings				

**3.** Enter the following fields details.

	General Settings			
?	IP Address:	*	$\not \supset$	192.168.26.129
?)	Port :		$\not \simeq$	53986
?)	User Name:	*	$\not \supset$	adldsadmin
?)	Password:	*	$\not \lhd$	•••••
?)	Confirm Password:		$\not \lhd$	•••••
	Notification			
?)	Email Address:			
	Rules			
?)	Create Default Password:			
?)	Automatically Remove Users:			
?)	Scan for Removed Users Interval [m]:			30
	Extension Handling			
?)	Extension/Mailbox Handling:			Try assign otherwise create new extension/mailbox
?)	Extension Number Length:			5
	Mailbox Handling			
8	No OneBox Server subsystem is available.P	lease i	nitia	te through Add Subsystem task.
	Add OneBox Server			
?	UDF Mapping:			Edit
	Remove Active Directory Server Config	jurati	on	
	Remove Configuration			

For example,

- IP Address: [IP address of AD LDS Instance located server]
- Port: [Normal LDAP port of AD LDS]
- User Name: [administrative user created in AD LDS in "Step V"]
- Password: [Password of above administrative user]

- Confirm Password: [Type the same password as entered in "Password" field]
- 4. Click on Apply. Authentication is Successful is displayed.

Server	
Property	Value
General Settings	
IP Address	192.168.26.129
Port	53986
User Name	adldsadmin
Rules	
Create Default Password	Yes
Automatically Remove Users	Yes
Scan for Removed Users Interval [m]	30
Extension Handling	
Extension Number Length	5
Mailbox Handling	
Create Mailbox	Yes
Configure Domains	
No property set	

- 5. Click Done.
- 6. Go to Configure Domains tab and click Add.

	Domain Configuration - Add
	Apply Cancel
	⑦ Search Domains:       *         ⑦ Description:       *
	<ul> <li>⑦ Select Location : Mitel ▼</li> <li>⑦ Select parent department for AD departments : Mitel ▼</li> <li>Extension Templates</li> </ul>
	Apply Cancel
Add the fol	lowing details.

 Search Domains: [The Domain which is created at AD LDS Side After Step X] For example, OU=WBMUSers, DC=wbmusersadldsdomain, DC=com

- 7. Click **Apply** and then click **Done**.
- 8. Configure the AD LDS Instance details as mentioned below.
- 9. Click Apply and then click Done.

Server Configure Domains	
Create	
Add	
Search Domains	Description
Search Domains       Q     Image: Search Domains       OU=WBMUSers,DC=wbmusersadldsdomain,DC=com	Description
	Description

10. Go to Configure Domains tab and click on Synchronization icon [5th icon from left side].

11. Go to Users menu and select User. Once, the synchronization completed.

Users	Services	Administrators	System	Logs	Own Settings	5				
User	Departments	UDF Mapping	Unlock							
User										
Add										
		nsion Number, Department:	Example: * or Will Smit							
<ul> <li>(?) Impo</li> <li>View</li> </ul>	rted from :		Active Directory ( Maximum rows pe		$\Leftrightarrow \Rightarrow$					
	Y User I	d ↔ Last Name ↔	First Name 😽 E	xtension / Teleph	ony System 🔌	Department(s)	<b>₽</b> <sub>©</sub>	Import from	🍫 Custom	ner 🍫

- 12. Enter "\*" in Enter User Name(s), Extension Number, and Department field.
- 13. Select Active Directory (AD) in Imported from drop-down list.
- 14. Select **View** to view the list of users who are synchronized from AD LDS.

#### **Enabling SSL for PM Application**

- 1. For the AD Authentication, Description refer to the file number 18/1551-ANF 901 15, Section 4 of the CPI Document.
- 2. Place the certificates of PM at AD LDS side as mentioned in step XII.

#### Enabling AD Authentication in PM Located Server

For the **AD Authentication**, **Description** refer to the file number *18/1551-ANF 901 15*, *Section 4.4* of the CPI Document.

To do this, do as follows:

- 1. Leave the **Principal DN Suffix** field empty.
- 2. Enter LDAPS port of AD LDS in the port field.
- 3. Except this everything is same as we do for Active Directory.
- 4. After this configuration, restart of PM application and try to login with the synchronized users from AD LDS.

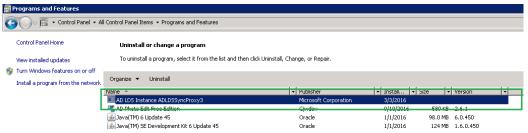
### Uninstalling AD LDS Instance and AD LDS Roles from Server

To uninstall AD LDS Instance from the system, do the following:

1. Go to Control Panel and select Programs and Features.



2. Select the AD LDS Instance Name > select Uninstall.



- 3. Remove AD LDS Roles from server.
- 4. Open Server Manager and select Remove Roles. Click Next button in the opened new dialog window.

📕 Server Manager							
File Action View Help							
🗇 🔿 📩 📰 🛛							
Server Manager (WIN-KNHRYMKHBUC)	Roles						
H P Roles P gi Features H pignostics P gi Configuration H Storage	Were the health of the roles installed on your server and add or remove roles and features.						
E - Storage	⊘ Roles Summary	Roles Summary Help					
	Roles: 6 of 17 installed     Active Directory Certificate Services	Add Roles					
	Active Directory Domain Services						

5. Unselect Active Directory Lightweight Directory Services check box.

Remove Roles Wizard     ×       Remove Server Roles								
Before You Begin Server Roles	To remove one or more installed roles from this server, clear their cl Roles:	heck boxes. Description:						
Confirmation Progress	Active Directory Certificate Services     Active Directory Domain Services	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services						
Results	Active Directory Lightweight Directory Services (Not Installed)     Active Directory Lightweight Directory Services     Active Directory Rights Management Services (Not Installed)     Application Server (Not Installed)     DHCP Server (Not Installed)	that allow you to issue and manage certificates used in a variety of applications.						

- 6. Click **Next** and then click **Remove** in the next dialog windows.
- 7. Click **Close** when it is removed successfully.

# **Quick Reference Instructions**

## **Create a User with IP Extension and Optional Mailbox**

When you create a user in MX-ONE Provisioning Manager (PM) you can also add an IP extension with or without a mailbox.

This step-by-step instruction guides you how to set up a user with an IP extension and a mailbox. You can combine how you will set your user information. First you can create a new user, or import user information. Second you add a new extension, and third you add a new mailbox or use an existing mailbox. **NOTE:** If you want to add more settings then this guide describe, please see the PM online help.

### Log in to PM

Do as follows:

Open Provisioning Manager (PM). The start page is displayed.

Type the User name in the field User.

Type the Password in the field Password.

Click Login. The main page is displayed.

#### Create a user

Do as follows:

Click Users and then User. The User page is displayed.

Click Add. The step Add User - Step 1/3 is displayed.

Type the last name of the user in the field Last Name.

Type the user ID in the field User ID.

It is optional to enter a password, but Mitel recommend you to select a password, minimum 6 characters. Enter needed information.

Select one or more options in the list Existing Department(s); Location(s) and then click on the right-arrow. Under Selected Department(s) Location(s) you will see the selected option. Sort the list with the button Move Up and Move Down.

Click Next. The step User - Add – step 2/3 is displayed. Next step is to add an IP extension.

### Add an IP extension

You can add an IP extension in two ways:

Add a new IP extension.

Use an existing extension.

### Add a new IP extension

Do as follows:

Click the tab Service Summary.

Click Add to the right of the field Add New Extension. The page Extension - Add - Step 1 / 2 is displayed.

Select IP from the list Extension Type.

Click Next. The page Extension - Add - Step 2 / 2 IP is displayed.

Select if the user allows dialing internal, regional, national or international phone calls, from the list Common Service Profile. (Note! This is depending on how the system was configured in the startup.) Enter needed information.

Click Continue. The page User - Change is displayed again.

Click Apply. The page User - Change – Result is displayed.

Click Done.

### Assign an Existing Extension

Do as follows: Click the tab Service Summary. Type the extension number under Extension Number. Click Apply. The page User - Change –Result is displayed. Click Done.

### Add a mailbox

If the user needs a mailbox you can add an existing mailbox number or add a new mailbox. Note! Add a mailbox is optional.

Do as follows:

### Add a new Mailbox

Click Add to the right of the field Add New Mailbox. The page Mailbox - Add - Step 1 / 2 is displayed.

Click Next. The page Mailbox - Add - Step 2 / 2 is displayed.

Type the name of the user in the field Subscriber Name.

If required, enter needed information in the other fields.

Click Continue. The page User - Add - Step 2 / 3 is displayed again. The mailbox number is displayed in the field Assigned Mailboxes.

Click Next. The page User- Add - Step 3 Scheduling is displayed.

If required, enter schedule information. Note! This optional.

Click Apply. The User – Add –Result page is displayed. If the settings were successful, you will get an information notice, see the following figure.

Jser - Add - Result	
Done	
Add operation success	aful for:
<ul> <li>User Id: fsten</li> </ul>	
User	
Property	Value
User Id	fsten
Last Name	stenen
Department(s)	
Department(s)	Company01; Location01
Preferences	
Use Last Selection	Yes
Language	English
Service Summary	
Property	Value
Extensions	
Extension / Telephony System	205/TS-Local
Secret / Main User / List	false/true/false
Mailboxes	laise/true/laise
Mailbox / OneBox Server	205 (Onchoy Q
in the second second	205/Onebox 🔍

Click Done, to close the page.

## Import a CSV file with user information using PM

You can import users, extensions and mailboxes via a CSV file using PM and the subsystem CMG. For more information of the contents in CSV file, see QRG Edit CSV file.

Note! The PM and CMG use different term for the same meaning, department or unit.

#### Log in to PM

Do as follows: Open Provisioning Manager (PM). The start page is displayed. Type the User name in the field User.

Type the Password in the field Password.

Click Login. The main page is displayed.

#### Preparation before the import of the CSV file

You have to enter information about the company and the units before you can import the information in the CSV file. You have to enter the company name in PM and the company (organization) structure in CMG. Note! The structure in CMG has to be exactly as the structures in the CSV file and the usage of capitals have to be the same.

Do as follows:

Click Users and then Departments. The Departments page is displayed.

Change the name in the field Department Name.

Click Apply.

### Log in to CMG

Do as follows:

Click System, Subsystem and then CMG DM. The Start page is displayed.

Type the user name in the field User name.

Type the password in the field Password.

Click Log in. The CMG Directory Manager page is displayed.

#### **Enter Company structure in CMG**

It is important that a valid company structure is entered in CMG before you import a CSV file! When you enter information in CMG you have to end all setting with a click on the Save button.

Do as follows:

Select All COMPANY01 from the list Select Directory.

Under Organization select Company01. The Manage Organization page is displayed.

Under Organization type the new organization name.

Click Save.

#### Add a New Unit in CMG

Do as follows:

Select the new organization under Organization. The Manage Organization page is displayed.

Click New Unit. The New unit page is displayed.

Type the name of the unit in the field Organization.

Click OK, and then click Save. The new name is inserted in the structure.

Continue to enter all the other units to the structure. Note! It is important that the structure is the same as the information in the CSV file!

### Import the CSV file in PM

Do as follows:

Select System, Data Management and then Import. The Import Data page is displayed. Click Import. The Import Data -Step 1/4 is displayed. Select CSV file on A700 format for Aastra 700, and CSV file for MX-ONE. Click Next. The Import Data -Step 2/4 is displayed. Click Browse. The Choose File to Upload page is displayed. Select the file you want to import and click Open. From the list Character encoding of CSV file select ISO 8859-1. Click Apply. The file is now imported. Note! This can take a while. Click Done. The Import Data page is displayed again. If the import was successful, you will get an information notice.

To check if all values are imported, click Successful Items. A list is displayed. Please read the whole list.

#### If something went wrong

If something went wrong with the import, please check the list below.

#### **Check list**

Check the user information.

Check the structure of the organization in PM and CMG.

Check user information in CMG.

Check the use of uppercase and lowercase letters in the structure of the organization. It must be the same in PM and CMG.

#### Check the Organization Structure in PM

Do as follows:

Click Users, User and then Departments. The Departments page is displayed. Check the structure.

### Check the Structure in CMG

Do as follows:

Click System, Subsystem and then CMG DM. The Start window is displayed.

Type the user name in the field User name.

Type the password in the field Password.

Click Log in. The CMG Directory Manager window is displayed.

Under Organization select the organization.

The structure is displayed to the right.

5. Check the structure.

#### Search for a User without a Unit in CMG

#### Do as follows:

Open CMG. Click Advanced Search under Records. The Advanced Search page is displayed.

From the list First criteria select Last name.

Click Search. The Record list page is displayed.

Click Organization to sort the list.

Select the user. The user information is displayed. All users without a unit are displayed first in the list. You can now add users to the right unit.

#### Add a User to a Unit in CMG

Do as follows:

Select a user. (Please see previous step-by-step-instruction Search for a user without a unit in CMG.)

Click the tab Organization and then Add. A page is displayed with the structure.

Expand the list.

Select a unit.

Click OK. The selected unit is displayed in yellow.

Click Save.

#### Add a new unit in CMG after a CSV File Import

If you find out that a unit is missing, you can add a new one in CMG.

Do as follows:

Under Organization select the organization. The Manage Organization with the structure page is displayed.

Select were in the structure the new unit shall be added.

Click New Unit. The New Unit page is displayed.

Type the required information of the unit in the fields.

Click OK.

Click Save.

Add users to the unit, see step-by-step-instruction Add a User to a Unit in CMG.

## **Edit CSV file**

Do as follows:

The figure below shows an example of a CSV file, in .xlsx format.

To edit a CSV file, follow the syntax below.

						Import 20 use	rs.xlsx - Mi	crosoft Excel							
Home Insert	Page Layout Formula	s Data Review	View Acrobat												0 -
H N			View Acrobat											Σ AutoSum *	A da
🗐 🖓 Copy		$A^* A^* = =$			neral			Normal	Bad	Good	Neutral			😺 Fill 🕆	27 A
ste 🍼 Format Painter	B I U - 🖽 - 🖄		📕 🗱 🔛 Merge & Cent	ter 🔹 📳	- % ,	Conditiona Formatting	Format	Calculation	Check Cell	Explanator	/ Input	Insert De	ete Format	2 Clear *	Sort & Find & Filter * Select *
Clipboard 🕞	Font	6	Alignment	G	Number	5	as rubic		Styles			C	lls		liting
A1 -	fx IP Extens	ion Number													
А	В	С	D	E	F	G		н	1	J		К	L		M
IP Extension Number	Mobile Extension Numbe	er Remote A-number	Received A-Number	CSP	First Name	Last Name	Departm	ent I	User ID	Password	Email		Mailbox (	y/n) CMG Ac	count (y/n)
67879				0	Alireza	Vasseghi	Design		avasseghi	aastra	alireza.vasseghi@	aastra.com	у	У	
67342				1	Anders	Andersson	Sales		aandersson	aastra	anders.andersson		У	У	
67920				2	Anders	Gustafsson	Test		agustafsson	aastra	anders.gustafsson		у	y	
67036				3	Anders	Holm	Design		aholm	aastra	anders.holm@aas		у	У	
67545				0	Anders	Larsson	Sales		alarsson	aastra	anders.larsson@a		у	У	
57759				1	Anders	Nathanson	Test		anathanson	aastra	anders.nathanson		у	У	
57948				2	Anders	Nordin	Design		anordin	aastra	anders.nordin@aa		У	У	
57212				3	Anders	Olsson	Design		aolsson	aastra	anders.olsson@aa		У	Y	
57147				0	Andreas	Jansson	Sales		anjansson	aastra	andreas.jansson@		y	Y	
67226				1	Andreas	Linden	Test		alinden	aastra	andreas.linden@a		y .	Y	
67058 67760				2	Anek Anna	Natesuwan Hillertz	Sales Design		anatesuwan ahillertz	aastra	anek.natesuwan@ anna.hillertz@aas		y .	Y	
57123				3	Anna Annika		Test			aastra			y	y	
7324				1	Annika	Engstrom Hulten Johansson	Test		aengstrom ahultenjohansson	aastra	annika.engstrom@	ansson@aastra.com	y .	Y	
7609				2	Annika	Miler	Design		amiler	aastra aastra	arne.miler@aastr		y V	Y V	
57862				3	Asad	Raza	Design		araza	aastra	araza@aastra.cor		y v	y V	
57961				0	Aurea	Moemke	Design		amoemke	aastra	aurea.moemke@a		y v	v	
57943				1	Bengt	Edlund	Sales		bedlund	aastra	bengt.edlund@aa		y v	y	
67536				2	Bertil	Johansson	Sales		bjohansson	aastra	bertil.johansson@		v	v	
57770				3	Bjarne	Egeland	Sales		begeland	aastra	bjarne.egeland@a		v	v	
					-,	-0					.,		· /	'	
a700-user-imp	ort-template 🖉 😓 🦯 👘								14			11			

## **Create an Extra Directory Number (EDN)**

Before you can create an Extra Directory Number, a user must exist with one IP extension.

### Log in to PM

- 1. Open MX-ONE Provisioning Manager (PM). The start page is displayed.
- 2. Type the User name in the field User.
- 3. Type the Password in the field Password.
- 4. Click Login. The main page is displayed.

### **Create an extra IP Extension**

Do as follows:

- 1. Click Services and then Extension. The Extension page is displayed.
- 2. Click Add. The Extension Add step 1/2 is displayed.
- 3. Select IP from the list Extension Type.
- 4. Click Next. The Extension Add step 2/2 IP is displayed.
- 5. Select a range from the list Extension Number Range.
- 6. Select an option from the list Common Service Profile.
- 7. Click Apply. The Extension Add Result is displayed. An information notice is displayed about the operation.
- 8. Click Done. The Extension page is displayed.

#### **View an Extension**

Do as follows:

Type the extension number or type \* to view all in the field Enter Extension Number(s). A list is displayed below.

#### Add an Extra Directory Number (EDN)

Do as follows:

- 1. Click Change, before the extension number you want to add an extra directory number for. The page Extension Change Extension number is displayed.
- 2. Under Function Keys, select the phone type from the list Phone Type.
- 3. Click Change. The page Function Keys is displayed. All the phone's keys are displayed.
- 4. Select one of the key numbers, and click to the left of the number. A field to the right is displayed.
- 5. Select EDN Extra directory number from the list Function.
- 6. Type the name of the extra directory number in the field Key Label. Note! This is optional.
- 7. Type the extra number you created in the step Create an extra IP Extension, in the field EDN Number.

**NOTE:** This number is reliable of the user's settings, if the user is allowed to dial local, national or international.

- 8. Click Ok. The Function Keys page is displayed again. Now is the information about the selected key displayed to the right of the key.
- **9.** Click Continue. The Extension Change page is displayed. Now is the information about the selected key displayed in the field Function Keys.
- **10.** Click Apply. The page Extension Change Result is displayed.

11. Click Done.

## Set Group Hunting

Group Hunting (Internal) group means that a number of extensions are assigned a common call number. When this number is called one of the extensions (members) is selected. The call is signaled on the telephone of the selected member. The call will be queued if no free member exists.

## Log in to PM

Do as follows:

- 1. Open Provisioning Manager (PM). The start page is displayed.
- 2. Type the User name in the field User.
- 3. Type the Password in the field Password.
- 4. Click Login. The main page is displayed.

### **Set Group Hunting**

Do as follows:

- 1. Select System, Subsystem, and then click on the link for the Telephony system. A Manager Telephony System page is displayed.
- 2. Select Telephony, and then Groups. A menu to the left is displayed.
- 3. Select Hunt Group. The Hunt Group page is displayed.
- 4. Click Add. The Hunt Group Add Step 1 / 3 is displayed.
- 5. Select an interval from the list Available Directory Number Intervals.
- 6. Click Next. The Hunt Group Add Step 2 / 3 is displayed.

### **Add Group Hunting Information**

- 1. Select a number from the list Direct Number.
- 2. Select an option from the list Direct In-dialing.
- 3. Select an option from the list Display of Called Number.
- 4. If required select options from the list:
  - a. Music on Wait
  - b. Allow Collect Call
  - c. Permit Automatic Extending.
- 5. Select 15 from the list Traffic Connection Class.
- 6. Select an option from the lists:
  - a. Member Selection Or.
  - b. Queue Internal Calls.

- c. Diversion.
- d. Diversion Number.
- 7. Click Next. The Hunt Group Add Step 3 / 3 is displayed.
- 8. Type the first name in the field First Name.
- 9. Type the last name in the field Last Name.
- 10. Click Apply. An information notice if the operation is displayed.
- 11. Click Done.

### **Select Group Hunting Members**

Do as follows:

- 1. Select System, Subsystem, and then click on the link for the Telephony system. A Manager Telephony System page is displayed.
- 2. Select Telephony, and then Groups. A menu to the left is displayed.
- 3. Select Hunt Group Member. The page Hunt Group Member is displayed.
- 4. Select the group you created before, and click Change,. The Hunt Group Members page is displayed.
- 5. Type one or more extension number, separated with a comma.
- 6. Click Apply. An information notice of the operation is displayed.
- 7. Click Done.

## Set Multiple Name Selection (MNS)

Before you can create a Multiple Name Selection, you have to create one user, with one mail box and one IP extension.

### Log in to PM

- 1. Open MX-ONE Provisioning Manager (PM). The start page is displayed.
- 2. Type the User name in the field User.
- 3. Type the Password in the field Password.
- 4. Click Login. The main page is displayed.

#### **View Extension**

Do as follows:

- 1. Click Services and then Extension in the start page. The Extension page is displayed.
- 2. Type the extension number or type \* to view all in the field Enter Extension Number(s).
- 3. Click View. A list is displayed below.
- 4. Click Change,, before the extension number you want to set Multiple Name Selection for. The page

Extension - Change - Extension number is displayed.

### Set Multiple Name Selection

Do as follows:

- 1. Click Service Summary Tab.
- 2. Under Function Keys, select the phone model from the list Phone Type.
- 3. Click Change. The page Function Keys is displayed. All the phone's keys are displayed.
- 4. Select one of the key numbers, and click to the left of the number. A field to the right is displayed.
- 5. Select MNS Multiple name selection from the list Function.
- 6. Type the name of the key in the field Key Label. Note! This is optional.
- 7. Type the extension number in the field MNS Number. (Note! Please see your number plan.).
- 8. Click Ok. The Function Keys page is displayed again. The information about the selected key is displayed to the right of the key.

#### Save the Settings

Do as follows:

- 1. Click Continue. The page Extension Change is displayed. The information about the selected key is displayed in the field Function Keys.
- 2. Click Apply. The page Extension Change Extension number Result is displayed.
- 3. Click Done.

## Set Personal Number (PN)

The Personal Number function allows you or the end-user, to handles incoming calls and route them, for example to the mobile or to the desk phone.

This step-by-step instruction gives you examples how you can set the function Personal Number, when you are:

- In the office
- On a business trip.

### Log in to PM

Do as follows:

- 1. Open Provisioning Manager (PM). The start page is displayed.
- 2. Type the User name in the field User.
- 3. Type the Password in the field Password.
- 4. Click Login. The main page is displayed.

#### **View User**

Do as follows:

- 1. Click Users and then User. The User page is displayed.
- 2. Type the name of the user in the field Enter User Name(s), Extension Number, Department.
- 3. Click View. The User ID table is displayed below.
- 4. Select the user, and click Change. The User Change page is displayed.

#### Set Personal Number (PN)

You start to enter the settings on the page User – Change. You can set up to 5 PN for an extension. The following step-by-step-instruction describes how you set 2 PN.

Do as follows:

#### Set Profile 1 - In Office

- 1. Click the tab Service Summary. The tab Service Summary is displayed.
- 2. Select an extension under Extension number, and click Change, . The Extension Change page is

displayed.

- 3. Click Edit to the right of the field Personal Number List. The Number list page is displayed.
- 4. Select Profile 1, and click Change, . The page Personal Number List Change 1 is displayed.

#### Set profile 1 - In Office

Click the tab Service Summary. The tab Service Summary is displayed.

Select an extension under Extension number, and click Change, . The Extension – Change page is

displayed.

Click Edit to the right of the field Personal Number List. The Number list page is displayed.

Select Profile 1, and click Change, . The page Personal Number List – Change 1 is displayed.

#### **Enter Number List Information**

Do as follows:

- 1. Type for example In Office, in the field List Name. Note! The limit of the list name is 10 characters.
- 2. Under Call Sequence 1 type your extension number in the field Number.
- 3. Select ring durations in seconds, for example 30 seconds, type 30 in the field Ring Duration [s].
- 4. Under Call Sequence 2 type for example the voice mail number in the field Number.
- 5. Select ring durations in seconds, for example 15 seconds, type 15 in the field Ring Duration [s].
- 6. Click Continue. The page Personal number List is displayed. You see the new PN in the table with the status active. Note! Now you can continue to add more PN, or save the settings and go back to the main page.

#### Set profile 2 – On a business trip

Do as follows:

Click Edit to the right of the field Personal Number List. The page Number list is displayed.

Select Profile 2, and click Change, . The page Personal Number List is displayed.

#### **Enter Number List Information**

Do as follows:

- 1. Type for example Business (for business trip) in the field List Name. Note! The limit of the list name is 10 characters.
- 2. Under Call Sequence 1 type your mobile number in the field Number.
- 3. Select ring durations in seconds, for example 15 seconds, type 15 in the field Ring Duration [s].
- 4. Under Call Sequence 2 type for example the voice mail number in the field Number.
- 5. Select ring durations in seconds, for example 15 seconds, type 15 in the field Ring Duration [s].
- 6. Click Continue. The page Personal number List is displayed. You see the new PN in the table with the status active.

#### Save the Settings

- 1. Click Continue. The page Extension Change is displayed. The PN is displayed under the button Edit in the field Personal Number List.
- 2. Click Continue. The tab Service Summary is displayed.

- Click Apply. The page User Change Result is displayed. An information notice of the operation is displayed.
- 4. Click Done.

## **Set Boss-secretary**

The Boss-secretary function is to allow the boss and the secretaries to control the diversion of incoming calls for the boss telephone. Both the boss and the secretaries can activate the function by pressing a predefined key on the phone.

#### Login to PM

Do as follows:

- 1. Open Provisioning Manager (PM). The start page is displayed.
- 2. Type the User name in the field User.
- 3. Type the Password in the field Password.
- 4. Click Login. The main page is displayed.

#### View the Extension of the Boss

Do as follows:

- 1. Click Users and then User. The User page is displayed.
- 2. Type the name or the extension number of the boss in the field Enter User Name(s), Extension Number, Department.
- 3. Click View. The User ID table is displayed below.
- 4. Click Change, . The User Change page is displayed.
- 5. Click the Service Summary tab.

#### **Set Personal Number Lists**

You have to create two personal number lists and two profiles, one for the boss (profile 1) and one for the secretary (profile 2).

#### Set Profile 1 for the Boss

- 1. Click Change, under Extension Number. The Extension Change page is displayed.
- 2. Click Edit under Personal Number. The Personal Number List page is displayed.

- 3. Click Change, to the left of Profile 1. The Personal Number List Change page is displayed.
- 4. Under Call Sequence 1 type the number of the Secretary.
- 5. The option Individual Repeated Distribution Bypass is default. Do not change.
- 6. Click Continue. The Personal Number List page is displayed.

#### Set Profile 2 for the Secretary

Do as follows:

- 1. Click Change, to the left of Profile 2. The Personal Number List Change page is displayed.
- 2. Under Call Sequence 1 type the number of the Boss.
- 3. The option Individual Repeated Distribution Bypass is default. Do not change.
- 4. Click Continue. The Personal Number List page is displayed.
- 5. Click Continue. The Extension Change page is displayed.
- 6. Click Continue. The User Change is displayed.
- 7. Click Apply. The User Change Result is displayed.
- 8. Click Done. The User page is displayed.

#### Select Key with Boss-secretary Function

- 1. Click Change, to the left of the extension of the Secretary. The User Change page is displayed.
- 2. Select the Service Summary tab.
- 3. Click Change, under Extension Number.
- 4. Click Change. The page Function Keys is displayed. All the phone's keys are displayed.
- 5. Select one of the key numbers, and click to the left of the number. A field to the right is displayed.
- 6. Select PEN Personal Number.
- 7. Type the name of the boss in the field Key Label. Note! This is optional.
- 8. Type the extension number of the boss in the field Monitored Number.
- 9. Profile 1 is default in Active Number List. Do not change.
- 10. Select Profile 2 from the list Passive Number List.
- **11.** Click Ok. The Function Keys page is displayed. The information about the selected key is displayed to the right of the key.

### Save the Settings

Do as follows:

- 1. Click Continue. The Extension Change page is displayed. The information about the selected key is displayed in the field Function Keys.
- 2. Click Continue. The tab Service Summary is displayed.
- Click Apply. The page User Change Result is displayed. An information notice of the operation is displayed.
- 4. Click Done.

## Set Telephone Name Selection (TNS)

Before you can create a Telephony Name Selection you have to create one user, with one mail box and one IP extension.

### Log in to PM

Do as follows:

- 1. Open Provisioning Manager (PM). The start page is displayed.
- 2. Type the User name in the field User.
- 3. Type the Password in the field Password.
- 4. Click Login. The main page is displayed.

#### **View Extension**

Do as follows:

- 1. Click Services and then Extension in the start page. The Extension page is displayed.
- 2. Type the extension number in the field Enter Extension Number(s).
- 3. Click View. The User ID table is displayed below.
- 4. Click Change, . The Extension Change page is displayed.

### **Set Telephone Name Selection Information**

- 1. Under Function Keys, select the phone model from the list Phone Type.
- 2. Click Change. The page Function Keys is displayed. All the phone's keys are displayed.
- 3. Select one of the key numbers, and click to the left of the number. A field to the right is displayed.
- 4. Select TNS Telephony Name Selection from the list Function.

- 5. Type the name of the key in the field Key Label. Note! This is optional.
- 6. Type the whole number (incl. access code) in the field Digit. (Note! Please see your number plan.).
- 7. Click Ok. The Function Keys page is displayed again. The information about the selected key is displayed to the right of the key.

### Save the Settings

Do as follows:

- 1. Click Continue. The Extension Change page is displayed. The information about the selected key is displayed in the field Function Keys.
- 2. Click Apply. The page Extension Change Extension number Result is displayed.
- 3. A information notice of the operation is displayed.
- 4. Click Done.

## **Delete a User**

When you delete a user you also delete the extension and the mailbox.

### Log in to PM

Do as follows:

- 1. Open MX-ONE Provisioning Manager (PM). The start page is displayed.
- 2. Type the User name in the field User.
- 3. Type the Password in the field Password.
- 4. Click Login. The main page is displayed.

#### **Delete a User**

- 1. Click Users and then User. The User page is displayed.
- 2. Type the name of the user in the field Enter User Name(s), Extension Number, Department.
- 3. Click View. The User ID table is displayed below.
- 4. Click Remove, on the same row as the user name. An information window is displayed with a question if you want to remove the user and related extensions and mailboxes.

5. Click OK. The User page is displayed. If the operation went well you will get the following message.



## Take a Backup of PM/SNM

When you have performed the installation and after making changes in PM and SNM, it is a good idea to take a backup of the settings.

### Log in to PM

Do as follows:

- 1. Open MX-ONE Provisioning Manager (PM). The start page is displayed.
- 2. Type the User name in the field User.
- 3. Type the Password in the field Password.
- 4. Click Login. The main page is displayed.

### Take a backup of MP

Do as follows:

- 1. Click System and then Data Management. A menu to the left is displayed.
- 2. Click Backup & Restore. The Backup & Restore page is displayed.
- 3. Click Backup. The Backup & Restore Backup page is displayed.
- 4. Click Apply.
- 5. To save the backup, click Download, . The File download page is displayed.

Ð

- 6. Click Save. The Save as window is displayed.
- 7. Select location from the list Save in.
- 8. Click Save.

### Take a Backup SNM

- 1. Click System and then Subsystem. The Subsystem page is displayed.
- 2. Click SN. The MX-ONE Service Node Manager (SNM) page is displayed.
- 3. Click System and then Backup & Restore. The Backup & Restore page is displayed.
- 4. Click Backup.
- 5. If the backup was successful, you get the following message:



## **Service Node Manager User Instructions**

This topic discusses the installation and configuration information for SNM.

## Introduction

This user guide describes how to use MX-ONE Service Node Manager (SNM), which is a web-based management tool used to configure MiVoice MX-ONE.

### Scope

The user guide contains:

- A description of the navigation and the user interface in MX-ONE Service Node Manager
- · An overview of how to work using MX-ONE Service Node Manager.
- An overview of system messages and error handling within MX-ONE Service Node Manager

### **System Requirements**

MX-ONE Service Node Manager can be accessed from anywhere using a commercially available browser. The browser requirements are:

- Microsoft Internet Explorer 8.0 (or later versions)
- Mozilla Firefox 18 (or later versions)
- Microsoft Edge 80.0.361.48 (Official build) (64-bit)
- Google Chrome (latest version)

Both HTTP (TCP Port 80) and HTTPS (TCP Port 443) are supported. If HTTPS is used, this needs to be configured. For higher security, it is recommended to use a commercial digital certificate issued by a commercial Certification Authority (CA).

### **Prerequisites**

To be able to use MX-ONE Service Node Manager, user accounts must be defined. Users can be defined in MX-ONE Provisioning Manager, that is used to manage users and administrators for MX-ONE. For more information about MX-ONE Provisioning Manager, see the description for MX-ONE PROVI-SIONING MANAGER. One user is defined during the installation of the MX-ONE Service Node, for more information see INSTALLING AND CONFIGURING MIVOICE MX-ONE. Javascript must be enabled in the browser in order use MX-ONE Service Node Manager. The browser must be configured to refresh pages on every visit. For information on how to configure, refer to help and documentation specific to your browser.

## **MX-ONE Service Node Manager Overview**

MX-ONE Service Node Manager is part of the MX-ONE Manager concept that consists of several operation and maintenance applications providing management functions for MX-ONE. For more information about MX-ONE Service Node Manager, see the description for MX-ONE SERVICE NODE MANAGER. For more information about MX-ONE Service Node Manager in MX-ONE, see the system description, MIVOICE MX-ONE.

### **Configuration Areas and Tasks in MX-ONE Service Node Manager**

The configuration areas in MX-ONE Service Node Manager are the following:

- Initial Setup
- Number Analysis
- Telephony
- Services
- System
- Tools
- Logs

Each configuration area handles a number of tasks and subtasks. For example:

Figure 9.1: Tasks in Number Analysis

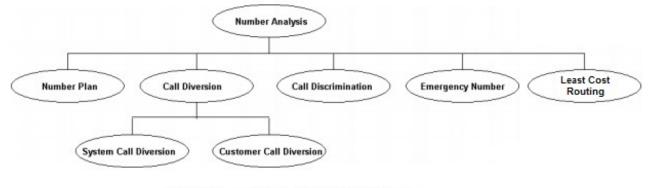


Figure 1: Tasks in Number Analysis

**NOTE:** Which configuration tasks for each area that are displayed, depends on system configuration and user privileges.

For a complete list of the tasks available in MX-ONE Service Node Manager, see the Site Map. A link to the site map can be found in the upper right corner.

## Using MX-ONE Service Node Manager

This section describes the user interface and navigation in MX-ONE Service Node Manager. How to use each task is explained in the online help, see Using the Help.

## Logging in and Logging Out

Browse to the login screen of MX-ONE Service Node Manager (SNM) and enter username and password provided by the administrator to log in to the application. The password is case sensitive.

**NOTE:** If MX-ONE Service Node Manager and MX-ONE Provisioning Manager server is configured for AD Authentication, the user password will not be provided by the administrator, but instead be the same as defined for the domain.

Click Logout in the upper right corner to log out from SNM. Closing the browser window will also log you out from the application.

The application has a time limit, after which an inactive user is automatically logged out. The time limit is by default set to 45 minutes and the time left, before automatic logout, is indicated in the browser status bar (lower left corner).

To be enable to see this indicator, the browser must be configured for allowing status bar updates using JavaScript. For more information, see Enabling the Automatic Logout Indicator on page 9.

**Application ID**: When using the SNM it is advisable to set the basic application information in order to recognize the site and application. Settings for the Application ID can be found by selecting Initial Setup and then Application ID. The Site name is displayed in the upper right corner and on the login screen.

### Navigating in MX-ONE Service Node Manager

The user interface is divided into menu tabs and sub menus relating to different configuration tasks in the system. For most of the tasks it is possible to add, change, view or remove configuration properties. How to use the different functions can be found in Actions on page 10.

Service Node Manager							d in as: <b>Alacarte</b>
Initial Setup	Number Analysis	Telephony	Services	System	Tools	Logs	
Number Plan	Call Diversion	Call Discrimination	Emer	gency Number	Least Co	ost Routing	
Least Cost Routing							

#### Figure 9.2: MX-ONE Service Node Manager User Interface

Item	Description
A	Main menu
В	Submenu
С	Task menu
D	Work area

ltem	Description
E	Summary and Help frame

**NOTE:** Do not use the back and forward buttons in the browser when you are working in MX-ONE Service Node Manager.

Using back or forward buttons will result in an error message. Reload the page to go back to MX-ONE Service Node Manager

#### Icons, Symbols and other Graphical Elements

The following icons and symbols can be found in MX-ONE Service Node Manager:

 Table 9.1: Icons and Symbols in the GUI (Sheet 1 of 3)

Symbol	Name/Function	Description
(?	Help	Information on how to set properties for the field.
Ø	Change	Change the properties for an existing configuration.
Q	View Details	View details for a configuration.
×	Remove	Remove the selected configuration.
	Add new using this as template	Add a new configuration using an existing as a template.
<b>B</b>	Create template from this	Create a template with the values in the existing configuration item.
8	Information	Information exclamation mark followed by system information.
~~	Update field	Update a specific field.

#### Table 9.1: Icons and Symbols in the GUI (Continued) (Sheet 2 of 3)

Symbol	Name/Function	Description
6	Restore	Restore the system to a previous state.
*	Mandatory	The field is required and mandatory to fill in.
4	Undo changes	Undo the changes just made for a specific field.
R	Change	Open the field for editing.
4))	Play the message	Plays a recorded soundfile.
<del>ବ</del> ୍ଦ କ <sub>ଦ</sub> ୁ କ <sub>ିକ୍କ</sub>	Sort the list	Sort the list in ascending or descending order. The arrow pointing in both directions indicates that the column is unsorted.
•	Run	Run a selected batch operation.
(j)	Download	Download a template or a batch operation as an xml file.
I¢	Reset	Reset the configuration.
<b>a</b>	Block	Block the board.

Symbol	Name/Function	Description
	Deblock	Deblock the board.
•	Logged on	The IP phone is logged on to the system.
•	Logged off	The IP phone has logged of from the system.
•	Unknown	The IP phone has not reported anything to the exchange in the last 48 hours.
۲	Not used	Initial mode after the IP phone is registered, but no log on attempt to the system has been done.
Φ	Log on rejected	The IP phone has attempted to log on, but has been rejected by the system.

#### Using the Help

There are several levels of Help in the MX-ONE Service Node Manager:

- User Guide: This User Guide, which can be found in the upper right corner of the application.
- Help: Online help for a specific task. There are three different types of help, overview of the task, help for adding a task (step by step instruction), and help for changing a task. The online help is opened in a pop-up window or the Help frame. See also Summary and Help frame on page 8
- Context help for a specific property. The context help describes the property usage, options and if

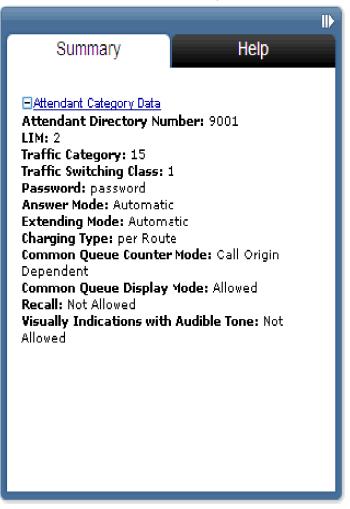
special conditions are to be considered.

• Walkthrough Help: Help for a specific walkthrough. Each step in the walkthrough, and the purpose of it, is explained.

#### Summary and Help frame

For some configuration tasks that contain several steps, a frame with summary and help information is displayed. The summary shows configuration information for all properties that have been configured in the task. Help shows step by step instructions related to the task. The summary and help frame can be minimized by clicking the arrow, below or on top of the frame.

Figure 9.3: Summary and Help frame



#### **Basic or Advanced Settings**

Property settings that are not often used and not mandatory are grouped in advanced settings for a task. Some fields in advanced settings have default values. The advanced settings are displayed by clicking Advanced. Basic settings are displayed by clicking Basic.

#### **Enabling the Automatic Logout Indicator**

To be able to see this information, the browser must be configured for allowing status bar updates using JavaScript. For information on how to enable this function in the browser, see the browser documentation.

MX-ONE Service Node Manager comprises a function for displaying the remaining time until an automatic logout due to inactivity is performed. The information is displayed in the status bar of the browser.

Figure 9.4: Automatic logout indicator

29 minutes left to log out due to inactivity.

This section describes the actions that can be performed in the different tasks. Most of the actions can be performed at different stages, for example from a result screen or from a list view.

## Actions

Figure 9.5: List viewData can be added to a new configuration item in the following ways:

Add Using Template	e: <pre></pre>	•	Manage Tem	<u>plates</u>	
② Enter Directory Numb	Example: '7040,7045-7050 Maximum rows per p	age 200 🔻 🔶	\$		
	Directory Number	Server Number &	First Nama 🔒	Lact Nama &	
		Server Number 🍕	First Name 🎄	Last Name 🖓	
	Directory Number %	Server Number $\theta_{\widehat{V}}$ 1	First Name 🦓	Last Name 🖓	
	8889	Server Number $\[mathchar]{}_{0}$ 1 1 1	First Name 🔌	Last Name 🔌	
🗋 Q 🥒 🗙 🛅 🔯	8889 8890	Server Number $\$ 1 1 1 1 1	First Name 🔸	Last Name 🔌	

- Click Add. System default values are displayed for the new configuration item. To create a configuration item without using a template, the value <Default template> must be selected in the Using Template drop-down list before clicking the button. To create a configuration item using a template, see Using a Template for a Configuration Task on page 14.
- From a result screen or a view details screen, click Add from this.... The previously added configuration item is used as a template.
- From a list view, click (Add new using this as template). The selected configuration item is used as a

tem	plate.	

Some configuration tasks have predefined values and can only be changed.

#### **Viewing Data**

Configuration items can be viewed in the following ways:

- For some tasks the list view is displayed by clicking View. The list displays the existing configuration items with a subset of the property values or all property values.
- From a list view, click (View details). The details of the configuration item are displayed. Click on the



arrows to view the previous or the next configuration item. Data for selected configuration items can also be compared, see 4.3 Comparing dataon page 11.

The list in the listview can be sorted by the items in the column clicking

(Sort by <column name>), (Sort descending), or (Sort ascending).



#### **Comparing data**

Configuration item properties can be compared with the compare function. The compare function is available in list views.

Perform the following steps to compare two configuration items:

1. Select two items to compare in the list.

		CSP Number 🔌	CSP Name 🛛 🍫	Customer 🚸
•	Q 🥖 🗙 🗎 🐚	0	Test	None
-	Q 🥖 🗙 🗈 🛐	1	Test 2	None
	Q 🥖 🗙 🖹 🗞	2	CSP 2	None
	Q 🦉 🗙 🗈 🚱	3	DECT SMS	None
0	Q 🥖 🗙 🗈 🛐	4	DECT SMS 2	None
	Q / 🗶 🗎 🖏	256	CSP 256	None

2. Click Compare.

A new screen with the result of the comparison is displayed. Property values that differ in the comparison are displayed in orange. The property values can be changed by clicking one of the Change <item> ... buttons.

<b>Common Service Profiles - Compare</b>	e - 0, 1	
Done		
Name Identity		
Property	Value	Value
CSP Number	0	1
CSP Name	Test	Test 2
Customer	None	None
Number Presentation Category		
Property	Value	Value
Request A-number from the PSTN	Restricted for extension	Restricted for extension
Use Number Presentation Restriction	Not restricted	Not restricted
Number Presentation Restriction is Permitted per Call	No	No
Allow Network Attiliation	Allowed	Allowed
Calling Line Identification Presentation Restriction Override	Permitted when type of connected party is private	Permitted when type of connected party is private
Never Display Number from PSTN	No	No
Calling Party Display	PBX member	PBX member
Traffic Category		
Property	Value	Value
Block Emergency Switching Characteristics	No	No
Direct Indialing Characteristics	Open	Open

#### **Changing Data**

Configuration items can be changed in the following ways:

- From a list view, click (Change). The configuration item is opened and the set values can be edited.
- From a list view, select one or more configuration items and click Change.... Makes it possible to change values for all selected configuration items at the same time. If changing values for more than one configuration item, (Change) enables the field.



• From a result screen, click Change This.... The configuration item is opened and the set values can be edited.

To restore the previously saved value in a field, that is to undo the change, click (Undo Change). Click Apply to save and apply the changes.



#### **Removing Data**

Configuration items can be removed in the following ways:

• From a list view, click (Remove).



- From a list view, select one or more configuration items and click Remove.
- From a result screen, click Remove This.

A pop-up confirmation window is displayed before a configuration item is removed.

#### **Printing Data**

Configuration data can be printed in the following ways:

- From a list view, click Print.... Prints the properties of selected configuration items.
- From a list view, click the Print All link. Prints the properties of all existing configuration items.
- Clicking Print..., Print All or Print opens a pop-up window that displays the print preview.
- From a view details screen, click the Print link. Prints the properties of the configuration item.

#### **Example: Printing External Number Series**

- 1. Click Number Analysis, Number Plan and then Number Series.
- 2. Select External Numbers from the Number Series Type list and click Print All.

3. A new window opens showing the print preview.

🔀 Mitel	Service Node Manager
Print Close Number Series -	1011
Property	Value
Number Series	1011
Number Series Type	Directory numbers
Number Series -	1500

Property	Value
Number Series	1500
Number Series Type	Directory numbers

Number Series - 1600-1700

Property	Value
Number Series	1600-1700
Number Series Type	Directory numbers

Number Series - 5000-5999

Property	Value
Number Series	5000-5999
Number Series Type	Directory numbers

4. Click Print. The browser print dialog box is opened, make desired selections and print the page.

#### **Handling Templates**

A template is a set of predefined values that can be used when a new configuration item is added. Templates are used to simplify the process of adding many configuration items with similar property values. Only property values that can be identical for several configuration items can be set in the template. Property values set in templates will not be set in the MX-ONE.

Click the Manage Templates link in a task to display the list view with the existing templates for that task. In the list view, the templates are displayed with the defined name, the type, the user that created it, and the date when it was created, for example, Template name(by Username, 12/30/06)

#### Creating a Template for a Configuration Item

#### CHAPTER 9

There are two ways to create a template:

- Create a new template, that is, a template with no predefined values:
  - Click the Manage Templates link.
  - Click Add and enter property values in the configuration task where applicable.
  - Enter a template name and click Apply to save the template
- Create a template based on an existing configuration item:
  - Click (Create template from this) in the list view.

#### - Enter a template name and click Apply to save the template.

NOTE: Creating a template will not alter any data on the MX-ONE Service Node.

#### Uploading or Downloading a Template

Templates can be created in one system and transferred to another. To

upload a template, click Upload.... To download a template, click (Download). Templates are saved in



.xml format.

#### Using a Template for a Configuration Task

Perform the following steps to use a predefined template for a configuration task:

1. Select a template from the list.

Analog Fax		Shortcuts:	<manage \$<="" th=""><th>Shortcuts&gt; 💊</th><th>• Go</th></manage>	Shortcuts> 💊	• Go
Add Using Template	: Test (by aastra, 8/25/09)		~	<u>Manage T</u>	<u>emplates</u>
	<default template=""></default>				
	Test (by aastra, 8/25/09)				

- 2. Click Add and enter property values in the configuration task where applicable.
- 3. Click Apply to save the new configuration item.

#### **Using Shortcuts**

Shortcuts can be used when you want to create or use a shortcut to another configuration task. For example, after adding an Operator Group, a shortcut to a related task could be to add members to the Operator Group.

Select desired shortcut from the list and click Go... to go to the task directly.

 Figure 9.6: Selecting Shortcut

 Shortcuts:

 Go...

#### **Creating Shortcuts**

- 1. Select <Manage Shortcuts>and click Go... to create a new shortcut.
- 2. Select the desired shortcuts from the list of available configuration tasks.
- 3. Click Apply.

**NOTE:** The shortcuts must be defined for each configuration task. When adding a shortcut from task A to task B, task B does not automatically get the shortcut to task A.

#### **Using Walkthroughs**

Walkthroughs can be used for guidance with a setup of several tasks. Walkthroughs are predefined, ordered flows from A to B, for example the setup of recorded voice announcements. It is possible to step forward or backward in a walkthrough, but in order to set the configuration, the property values for each task must be applied before continuing with the next step. Each task in the walkthrough is optional.

风 Mitel	Service Node Manager	Number     Space     Space     Logs	
	er Analysis Telephony Services System Tools Logs Kalion D		
Full Setup Route Operator	Full Setup - Well-through - Step: 1/28           Purpose Set bit news to show on login screen, and add contact infe for the system administrators.           Here Stackborthald Setup - Application ID           C Stack         (Martin)		Weikthrough Hele
Voice Announcement Branch Office Routing Server	Application ID Apply Cancel		the la
Routing Satelite	Revision: 6.0_SP2		

Item	Description
A	Walkthrough field
В	Task field
С	Apply for a task

#### Starting a Walkthrough

The following steps are general and applies to all walkthroughs.

- 1. Select Initial Setup and then Walkthroughs.
- 2. Select a walkthrough from the task menu.
- 3. Click appropriate button in the task, for example Add.
- 4. Enter desired property values for the task and click Apply.

**NOTE:** A task within the walkthrough may consist of several steps.

- 5. Click Next-> in the walkthrough field to go to the next configuration task.
- 6. Repeat Step 4 (Enter desired property values for the task and click Apply) to Step 5 (Click Next->in the walkthrough field to go to the next configuration task) until the last step of the walkthrough.

#### **Using Batch Operations**

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 possible to record several configuration tasks into one batch operation and change the order of the operations.

Figure 9.7: Batch Operation



#### View/Edit

					Name 🔩	
Q	0	×	Þ	Ð	Batch operation tes	st

The following options are available in Batch Operation:

- Add new
- Upload or Download a previously defined batch operation.
- · View, Change, Add from this
- Run a previously defined batch operation.

The batch operations are saved in xml format. Batch Operations can be created in one system and transferred to another.

#### Adding a new Batch Operation

- 1. Select System, then Batch Operation and click Add.
- 2. Add a name for the Batch Operation and click Next->.
- 3. Click Record to add the configuration item and Stop to end the recording.
- 4. Click Apply to save the Batch Operation or Record to add a new instruction to the batch operation

**NOTE:** Configuration properties set during the recording are not sent to the MX-ONE Service Node.

#### **Running a Batch Operation**

- 1. Select System, and then Batch Operation.
- 2. Click Run to execute the batch operation.

#### **Using Command Line Interface**

The Command Line Interface (CLI) in MX-ONE Service Node Manager is used to execute commands that cannot be handled using the web based interface of MX-ONE Service Node Manager. To have access to the CLI, the user must be logged in to an account with the privilege Command line interface included in the security profile.

Select Tools and then Command Line to open the CLI.

🛤 Mitel	Service Node Manager		Sile: technoo	Logged in as: Mitel	About	User Guide
> summer_prist						
MARCER AVELTIS DATA : TTA DO MARCEN RETRIETO MOMENT PROTECT OFFICIATION THEORY, MECHANICS	NERVAN XANEYA 10011 14400 2700 4010 - 2499 9000 - 9050					
Commands 20 Latest Commandes Toput File:	<pre>clainticrove.ascorroanda&gt; • Emana No Sa usiachud</pre>	Apply				Help
On emitted transmict	Digeore error Frecate Stop Pai	Rasera		Cia ne W	intee	Since Window

Figure 9.8: Command Line Interface

The following types of commands can be used:

- UNIX-style commands, which are separate executable files in the UNIX<sup>™</sup>/Linux<sup>™</sup> 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 the aspect that they cannot be concatenated. Each parameter must be separate.
- Built-in commands, which are UNIX/Linux commands that are executed by mdsh as an integrated part of the shell. Examples are the commands cd and threads.
- MML commands, which comply with the CCITT MML format familiar to, for example, the MD110 user. These commands are sent by mdsh to a program (CIOR), which finds the appropriate command handler (for example GEH) to execute the command.

**NOTE:** Interactive commands cannot be used.

NOTE: No confirmation questions are provided for dangerous commands.

For an overview of command handling see the command description COMMANDS IN MX-ONE SERVICE NODE.

The latest 20 commands are stored in the system, and any of them can be executed in the following way:

- 1. Select the command in 20 Latest Commands. The command is copied into Command.
- 2. To execute the command, click Apply.

Instead of entering each command separately it is possible to upload a file containing a number of commands to be executed:

- 1. Enter the search path of the file to upload, or click Browse to search for the file.
- 2. Click Execute.

The upper window displays the results of the operation. Executed commands are highlighted by an arrow (-->), preceding the output.

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

- 1. Click the Download link.
- 2. Select where to store the log file and click Save.

The log file can contain a maximum of 10 000 lines. When the number of lines is exceeded, the oldest lines are removed from the log so that new operations can be added.

To clear the list of 20 Latest Commands, click Clear List.

To clear the display window, click Clear Window.

To close the CLI window, click Close Window.

NOTE: Using the CLI to alter data on the MX-ONE Service Node (SN) may lead to data inconsistencies between MX-ONE Provisioning Manager (PM) data and SN data.

#### **Using Backup & Restore**

It is possible to back up and restore MX-ONE data. Each backup file is identified by a backup number, a time stamp and the system release version number. MX-ONE Service Node Manager stores exchange data on the MX-ONE Service Node and data concerning for example names of routes and common service profiles in an SQL Database. The exchange data and the SQL database are both included in a backup or restore session.

- -

.

. .

Select System and Backup & Restoreto start using the functions for Backup & Restore. \_...

Backup & Restore Backup Backup No. % Timestamp % Versio 1 2012-03-16 16:20:35 13.212 2 2012-03-01 01:03:29 13.212	store
Backup No.         ⊕         Timestamp         ⊕         Version           I         2012-03-16 16:20:35 13.213	
•	0
2 2012-03-01 01:03:29 13.21	4
	4
4 2012-03-01 00:42:40 13.130	45
5 2012-03-01 00:23:29 13.136	45

Click Backup to start a backup.

Click (Restore) to restore the system.

1 Restoring data can result in user and extension data inconsistencies.

2 The backups are possible to take from the Provisioning Manager subsystem task. The backups, thus performed are listed here and restored.

#### System and Error Messages

MX-ONE Service Node Manager provides system messages and error messages directly or when a configuration item is submitted.

Icons are displayed together with system information.

#### Table 9.2: System and Error Messages

Туре	lcon
Error Message	X Add operation failed for:
	User Id: Test Reason: Already initiated Field: User Id Value: Test
Information Message	Session has expired! Please relogin
System Message	<ul> <li>Remove operation successful for:</li> <li>Log Date and Time: 2009/08/21 16:12:58</li> </ul>

For some operations a pop-up window is displayed. For example when entering invalid or too many characters in a field.



#### Logs

MX-ONE Service Node Manager provides three logs with different information level:

- Audit trail: information about all changes made by a user in the system.
- Event Log: system log information useful for fault tracing.
- Security Log: information about successful and unsuccessful login attempts.

MDSH log: Information about commands send from SNM to the Service Node.

NOTE: Log files are created every day even if no data is logged. Logs older than 90 days will be overwritten

## **System and Error Messages**

MX-ONE Service Node Manager provides system messages and error messages directly or when a configuration item is submitted. Icons are displayed together with system information.

#### Table 9.3: System and Error Messages

Туре	Icon
Error Message	Add operation failed for: • User Id: Test Reason: Already initiated Field: User Id Value: Test
Information Message	I Session has expired! Please relogin
System Message	<ul> <li>Remove operation successful for:</li> <li>Log Date and Time: 2009/08/21 16:12:58</li> </ul>

For some operations a pop-up window is displayed. For example when entering invalid or too many characters in a field.



### Logs

MX-ONE Service Node Manager provides three logs with different information level:

- · Audit trail: information about all changes made by a user in the system
- · Event Log: system log information useful for fault tracing.
- Security Log: information about successful and unsuccessful login attemps

MDSH log: Information about commands send from SNM to the Service Node.

NOTE: Log files are created every day even if no data is logged. Logs older than 90 days will be overwritten





Delete WebSEAL IP 78 Delete Input 78 PM Welcome Page after Successful WebSEAL Registration 79 Connections between AD/PM and MiVoice MX-ONE/MiCollab AM/CMG 81 Active Directory Users and Computers GUI - 1 85 Active Directory Users and Computers GUI - 285 Provisioning Manager 87 Active Directory Values 88 Enabling/disabling automatic notification 88 Exceution flow 89 Configure web Server - 194 Configure web Server - 295 Enter the Certificate Signing Request Details screen 95 Example of Common Name field 96 Successful creation of CSR file 96 Creating the Key Store - 1 97 Selecting the directory and files 98 Confirming whether you have Root/Chain Certificates 99 Certification Path 99 Selecting the Root / Chain Certificate file 100 Creating the Key Store 101 Validating Key Store creation 101 Key Store File creation 101 User authenticated and authorized in PM user database 109 User authenticated in AD and authorized in PM user database 109 The examples above are in the following scenarios referred to as 110 Scenario 1: PM Login 110 Scenario 2: SNM Login 111 Scenario 3: SNM Login over HTTP 112 Scenario 4: PM Login + use case 'Add Extension' 113 Scenario 5: In PM "click on subsystem" 114 Tasks in Number Analysis 193 MX-ONE Service Node Manager User Interface 194 Summary and Help frame 198 Automatic logout indicator 198 List viewData can be added to a new configuration item in the following ways: 199 Selecting Shortcut 203 Batch Operation 205 Command Line Interface 206 Backup and Restore 207