

MiVoice MX-ONE

User Account Management - Operational Directions

Release 7.1

April 28, 2019



Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®)**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

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

®, ™ Trademark of Mitel Networks Corporation
© Copyright 2019, Mitel Networks Corporation
All rights reserved

Contents

Chapter: 1	General	1
Chapter: 2	Linux User Accounts	2
Chapter: 3	MX-ONE Provisioning Manager User Accounts	3
Chapter: 4	User Accounts for Logging into SNM	4
	Selecting Authentication Method During Installation	4
	Changing Authentication Method for Existing Installations	4
	Using MX-ONE Provisioning Manager User Accounts	4
	Using Linux User Accounts	5
	User Privileges in MX-ONE Service Node Manager	5
	MX-ONE SNM User Privileges in MX-ONE PM	5
	Correspondence Between SNM Privileges and Linux Authority Levels	5
Chapter: 5	Working with User Accounts	7
	Working with User Accounts in MX-ONE Provisioning Manager	7
	Working with User Accounts in Linux	7
	Creating User Accounts	7
	Changing User Account	7
	Changing Passwords	8
	System Database Maintenance	8
	Password Policies	8
Chapter: 6	Reconfiguring the System Service User (for V.24 Services)	10

General

MX-ONE uses two types of user accounts for MX-ONE Service Node management; MX-ONE Provisioning Manager and Linux user accounts.

MX-ONE Provisioning Manager user accounts are used for log-in to the primary Service Node management interface, MX-ONE Service Node Manager. Linux user accounts are used for log-in to the MX-ONE Service Node using the Linux MDSH shell.

For installations not using MX-ONE Provisioning Manager, Linux user accounts can also be used for logging in to MX-ONE Service Node Manager.

Linux User Accounts

During installation of MX-ONE Service Node, the following Linux user accounts are automatically created:

- a root administrator
- an MX-ONE Service Node administrator (`mxone_admin`)
- an MX-ONE Service Node Manager user (`mxone_user`).

The root administrator can be used for creating additional Linux user accounts on the MX-ONE Service Node. The root administrator user is not intended for MX-ONE Service Node management.

The MX-ONE Service Node administrator is named `mxone_admin` and is used when installing and upgrading MX-ONE.

NOTE: The root and `mxone_admin` user accounts are not intended for general maintenance. Instead, it is recommended that a separate user account with authority level 7 (unix group `snlev7`) is used.

The MX-ONE Service Node Manager user account is used for logging in to MX-ONE Service Node Manager for installations not using MX-ONE Provisioning Manager. This user account is created only if the authentication method option is set to Linux during MX-ONE Service Node installation.

NOTE: Do not use the `mxone_admin` account for MX-ONE Service Node Manager.

Authority levels in Linux are set using the `snlev` setting (`snlev0`-`snlev7`, where `snlev7` has the highest authority). Linux users created during installation have authority levels according to the table below.

Table 1: Administrator users and default authority level

Linux user	Authority level
<code>mxone_admin</code>	<code>snlev7</code>
MX-ONE Service Node Manager user (<code>mxone_user</code>)	<code>snlev7</code>

Which Unix commands that relates to a Linux authority level is defined in the `/etc/opt/eri_sn/mdsh.conf`file. For more information on commands and authority levels, see *Commands in MX-ONE Service Node*.

NOTE: The Linux user accounts created during installation are always managed using standard Linux user account management procedures.

MX-ONE Provisioning Manager User Accounts

MX-ONE Provisioning Manager manages user accounts for users and administrators in MX-ONE, and MX-ONE Service Node Manager users. To use MX-ONE Provisioning Manager user accounts for logging in to MX-ONE Service Node Manager, the authentication method option is set to MX-ONE Provisioning Manager during the MX-ONE Service Node installation.

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

A MX-ONE Provisioning Manager user account can be used for logging in both to MX-ONE Provisioning Manager and MX-ONE Service Node Manager.

A user's MX-ONE Service Node Manager privileges are defined using MX-ONE Provisioning Manager.

The MX-ONE Provisioning Manager feature for locking users after three incorrect log-in trials can be used.

Locked out users can unlock their accounts using MX-ONE Provisioning Manager.

MX-ONE Provisioning Manager user accounts cannot be used for logging in to MX-ONE Service Node using the MDSH shell. Linux user accounts can not be used for logging in to MX-ONE Provisioning Manager.

For more information on MX-ONE Service Node Manager user account management in MX-ONE Provisioning Manager, see *MX-ONE Service Node Manager Description*.

User Accounts for Logging into SNM

MX-ONE Service Node Manager is the primary management interface for MX-ONE Service Node. The application has no user database, instead MX-ONE Provisioning Manager or Linux user accounts are used for log-in. Which type of user to use for MX-ONE Service Node Manager log-in is defined by the MX-ONE Service Node Manager authentication method.

If MX-ONE Provisioning Manager is used for authentication, the MX-ONE Provisioning Manager user database is used for authenticating user log-in into MX-ONE Service Node Manager. If Linux is used for authentication, standard Linux procedures are used for the authentication.

Which authentication method to use is set during installation or, for existing installations, using the MX-ONE Maintenance Utility.

Selecting Authentication Method During Installation

During installation, the user is asked to select an authentication method for MX-ONE Service Node Manager. The authentication method defines which user database to use when authenticating users that log in to MX-ONE Service Node Manager. The following methods are available:

- authentication using MX-ONE Provisioning Manager
- authentication using Linux user accounts.

If Linux user accounts are used for authentication of MX-ONE Service Node Manager users, a Linux user account dedicated to MX-ONE Service Node Manager is created on the MX-ONE Service Node during installation. In this scenario, authentication of users that log in to MX-ONE Service Node Manager is managed by the MX-ONE Service Node, using the standard Linux user authentication procedure.

If MX-ONE Provisioning Manager is selected, no Linux user account for MX-ONE Service Node Manager is created on the MX-ONE Service Node. In this scenario, authentication of users that log in to MX-ONE Service Node Manager is managed by MX-ONE Provisioning Manager and its user database.

Changing Authentication Method for Existing Installations

The authentication method can be changed for existing MX-ONE Service Node installations using the MX-ONE Maintenance Utility option Web server config.

Using MX-ONE Provisioning Manager User Accounts

When using MX-ONE Provisioning Manager user accounts for logging in to MX-ONE Service Node Manager, log-in requests in MX-ONE Service Node Manager are authenticated using the MX-ONE Provisioning Manager user database. If the user is authorized to log in MX-ONE Service Node Manager, the log-in is executed.

Authenticating users using the MX-ONE Provisioning Manager user database provides a number of features not available when authenticating users using Linux accounts on the MX-ONE Service Node Manager server. For information on user authentication and authorities in MX-ONE Provisioning Manager, see *MX-ONE Provisioning Manager Description*.

Using Linux User Accounts

For installations not using MX-ONE Provisioning Manager, Linux user accounts on the MX-ONE Service Node are used for authentication for MX-ONE Service Node Manager. Using this method, a user's privileges in MX-ONE Service Node Manager are defined by the user's Linux authority level and the user authentication is managed by the MX-ONE Service Node, using standard Linux user authentication procedures.

The Linux authentication method can be used for MX-ONE Service Node Manager even when MX-ONE Provisioning Manager is used, even though it is not recommended.

NOTE: *It is important that the Linux user account that MX-ONE Provisioning Manager is using when logging in to MX-ONE Service Node Manager (as configured in the MX-ONE Provisioning Manager Subsystem task) must have **snlevel7** to avoid internal conflicts. The access restriction is enforced by MX-ONE Provisioning Manager instead.*

User Privileges in MX-ONE Service Node Manager

User privileges for MX-ONE Service Node Manager users are defined using MX-ONE Provisioning Manager or Linux authority levels, depending on the selected authentication method.

MX-ONE SNM User Privileges in MX-ONE PM

The following privileges can be associated to a MX-ONE Service Node Manager user in MX-ONE Provisioning Manager:

- Manage extension data
- Modify user data
- Manage configuration data
- Manage advanced features
- Command line interface access

Correspondence Between SNM Privileges and Linux Authority Levels

User privileges in MX-ONE Service Node Manager and Linux account authority levels approximately correspond according to the table below.

NOTE: *A task in MX-ONE Service Node Manager (for example, creating a user) usually comprises several procedures, where each procedure might require it's own privilege level. The table below shows the minimum authority level for MX-ONE Service Node Manager privileges.*

Table 1: Privileges and authority levels

Privilege in MX-ONE Service Node Manager	Corresponding Linux authority level in MX-ONE (approximate)
Manage extension data	Low
Modify user data	
Manage configuration data	
Manage advanced features	
Command line interface access	High

For information on the correspondence between tasks and privileges in MX-ONE Service Node Manager, see MX-ONE Service Node Manager Description.

Working with User Accounts

User accounts (including users for MX-ONE Service Node Manager log-in) are managed using MX-ONE Provisioning Manager and standard procedures for user account management in Linux.

Working with User Accounts in MX-ONE Provisioning Manager

For information on how to create, modify, and delete user accounts in MX-ONE Provisioning Manager, see *MX-ONE Provisioning Manager User Guide*.

Working with User Accounts in Linux

This section provides tasks on how you can create and maintain user accounts in MX-ONE Service Node for users accessing the Linux MDSH shell

Creating User Accounts

Only the root administrator can create users and groups in Linux.

Before you create a user you should be familiar with the password policies described in [Password Policies](#). It is also important that all Linux users are informed about actual policies.

Follow the steps below to create a user:

- 1) Log-in as user **mxone_admin**.
- 2) Run the `sudo -H /opt/mxone_install/bin/mxone_maintenancecommand` to start the MX-ONE Maintenance Utility.
- 3) Select **User and select Add**.

The Utility will prompt for the following items:

- What type of user to create. The user account will get the same supplementary groups as the reference user account.
- Login shell
- Desired level of authority
- Login name and comment describing the user
- Password

Changing User Account

The user accounts that are not automatically created can be modified by using the MX-ONE Maintenance Utility.

Before you modify a user you must be familiar with the password policies described in [Password Policies](#). All Linux users must be informed about actual policies.

- 1) Log-in as user **mxone_admin**.
- 2) Run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command to start the MX-ONE Maintenance Utility.
- 3) Select **User** and then select **Change**. The Utility will prompt for the following items:
 - User account.
 - Comment describing the user
 - Level of authority
 - System Database maintenance
 - Password

Changing Passwords

This section provides information on how to change passwords for the root and mxone_admin user accounts. For information on how to change the default passwords of the root and mxone_admin user accounts during installation, see Installing and Configuring MiVoice MX-ONE Installation Instructions.

Follow the steps below to change the passwords for the **root** and **mxone_admin** user accounts in an already installed system:

- 1) Log on a server using the root user account.
- 2) Run the `passwd` command to change the passwords of the root and mxone_admin user accounts.
- 3) Repeat step 1 to 2 for all servers in the system.

System Database Maintenance

The users that are to do maintenance work or troubleshooting of the system database function (Cassandra) need additional access. Change the user account, see section Changing User Account. At the item System Database maintenance, type yes to add maintenance access to the system database.

Password Policies

This section describes the password policies for Linux users in the MX-ONE system. Some of the policies are applicable at the system level (apply to all existing users) and while others are applicable at the user level (apply only to new users created).

NOTE: Note that the password policies are only fully verified when a user changes password with the `passwd` command or is forced to set password at login (that is, not during initial installation and when a user is created/modified in MX-ONE Maintenance Utility).

The following default system level policy is enforced on all Linux users, except root:

- Password must contain at least 9 characters.
- A password must contain at least one each of the following characters:
 - lower case

- upper case
- digit
- other/special character: ~!@#%&* _+=|\\(){}[];:"'<>,.?/

The following default user level policy is applicable to new users created from MX-ONE Maintenance Utility:

- Password change is enforced on first login
- Password aging is disabled

Following are the steps for viewing and changing password policies from MX-ONE Maintenance Utility:

- 1) Log in as user `mxone_admin`.
- 2) Type the command `sudo -H /opt/mxone_install/bin/mxone_maintenance` to start the MX-ONE Maintenance Utility.
- 3) Select the option **More Configuration**, then **Password Polices** and then **Change**. The Utility prompts specifying the following system and user (*) level policies:
 - Password minimum length
 - Characters allowed in the password
 - Password history (number of passwords to remember)
 - Force password change at first login *
 - Password aging parameters (that is, number of days before password expires)
- 4) Any changes made to the settings is applied to all servers in the system.

***NOTE:** Note that the user level policies are not re-applied to the existing users. It is important to inform users about changes in the password policies because users are not notified about the changes when they are prompted to change their passwords.*

Reconfiguring the System Service User (for V.24 Services)

The V.24 serial interface is normally not used by the MX-ONE. When it is needed, for example, at *Call Logging* to a V.24 port, the system service user (a Unix daemon), **eri_sn_d**, must be reconfigured. This operation must be performed for all LIMs where the service is needed.

NOTE: *The eri_sn_d user is not intended for MX-ONE Service Node management. For that reason, this user is not included in the list of Linux user accounts created during installation in chapter 2, Linux User Accounts.*

Log-in as user **mxone_admin**, and run the `sudo -H /opt/mxone_install/bin/mxone_maintenance` command and select **user > daemon** and follow the instructions on screen.

