

User Account Management

OPERATIONAL DIRECTIONS



NOTICE

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

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

TRADEMARKS

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

© Copyright 2017, Mitel Networks Corporation

All rights reserved

1

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.

2

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.

3

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.

4

USER ACCOUNTS FOR LOGGING IN TO MX-ONE SERVICE NODE MANAGER

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.

4.1

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.

4.2

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.

4.3 USING MX-ONE PROVISIONING MANAGER USER ACCOUNTS FOR LOGGING IN TO MX-ONE SERVICE NODE MANAGER

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.

4.4 USING LINUX USER ACCOUNTS FOR LOGGING IN TO MX-ONE SERVICE NODE MANAGER

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.

4.5 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.

4.5.1 MX-ONE SERVICE NODE MANAGER USER PRIVILEGES IN MX-ONE PROVISIONING MANAGER

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.

4.5.2

CORRESPONDENCE BETWEEN MX-ONE SERVICE NODE MANAGER 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 2 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.

5 WORKING WITH USER ACCOUNTS

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

5.1 WORKING WITH USER ACCOUNTS IN MX-ONE MX-ONE PROVISIONING MANAGER

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

5.2 WORKING WITH USER ACCOUNTS IN LINUX

5.2.1 CREATING USER ACCOUNTS

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

Follow the steps below to create a user:

1. Log-in as user *mxone_admin*.
2. Key the command `sudo -H /opt/mxone_install/bin/mxone_maintenance` to start the MX-ONE Maintenance Utility.
3. Select option **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

5.2.2 CHANGING USER ACCOUNT

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

1. Log-in as user *mxone_admin*.
2. Key the command `sudo -H /opt/mxone_install/bin/mxone_maintenance` to start the MX-ONE Maintenance Utility.
3. Select the option **User** and select **Change**. The Utility will prompt for the following items:
 - User account.
 - Comment describing the user

- Level of authority
- LDAP maintenance
- Password

5.2.3

CHANGING 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. By using the **passwd** command, change the passwords of the root and mxone_admin user accounts.
3. Repeat step 1 to 2 for all servers in the system.

5.2.4

LDAP MAINTENANCE

The users that are to do maintenance work or troubleshooting of the LDAP function need additional access. Change the user account, see section Changing User Account. At the item LDAP maintenance, type yes to add maintenance access to LDAP.

6

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 key the command `sudo -H /opt/mxone_install/bin/mxone_maintenance` and select option user -> daemon and follow the instructions on screen.