

Administrator User's Guide

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 2020, Mitel Networks Corporation

All rights reserved

1

GENERAL

This guide covers administrator tasks in the MX-ONE excluding telephony features. For information about telephony feature maintenance, see the documents in the CPI library folder Operation and Maintenance.

1.1

GLOSSARY

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

1.2

MANAGING THE MIVOICE MX-ONE

The MX-ONE can be managed in different ways. The tasks described in this document are mainly managed from the command line on the Linux server (the MX-ONE Service Node).

The MX-ONE can also be managed and configured using the MX-ONE Service Node Manager. see the directions for use for *MX-ONE SERVICE NODE MANAGER USER GUIDE*.

1.2.1

TERMINAL INTERFACE

The Linux operation system can be modified for local needs in a flexible way through localization. Environment variables determine language and country specific settings, like the format of date and time, how numbers are written, and what character encoding to use.

By locale settings the MX-ONE user can use the characters of their own language when entering local data, like users names, to the system.

To see how the localization is set, use the Linux *locale* command. It will list the variables on standard output, for example, as

```
LANG=en_US.UTF-8
LC_CTYPE=en_US.UTF-8
and so on.
```

The locale values have the form *language[_territory][.codeset]*, where the language codes usually are the two-letter codes defined in ISO 639-1 and the country codes (in territory) the two-letter codes defined in ISO 3166-1. Use the command *locale -a* to find the available locales and *locale -m* for the available character encoding.

In Europe many languages can use the ISO8859-1 encoding, but UTF-8 is more complete.

When operating the system (remotely) over SSH, for example, using the puTTY terminal emulation program, it is vital that the same character encoding is used in both puTTY as in the connected system. (In puTTY the character encoding can be modified thru "Translations" from the "Change Settings" menu).

Both parties must have the same settings for the communication to work.

1.3

CHARACTERISTICS OF LOAD PROGRAMS

The MX-ONE Service Node SW consists mainly of two types of load programs, the program units and the UNIX commands.

The characteristics of a program unit are:

- Identified with unique number and name
- Runs continuously in a working system
- Can be restarted (restart command)
- Can be reloaded (reload command)
- Communicates directly with other program units by sending and receiving messages

For a detailed information about the program units see the parameter description for *UNIT*, in the *Technical Reference Guide, MML parameters*.

The characteristics of a UNIX command are:

- Uses dynamic program numbers
- Communicates with other programs using the Application Message Proxy
- Runs only when the command is typed

2

MARKET

Market is selected during first time setup, see the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE*. If it is necessary to reconfigure the market parameters, see command description *TECHNICAL REFERENCE GUIDE, UNIX COMMANDS* for details.

Detailed market characteristics for each market can be found in the documents in the Market Characteristics folder.

3 BACKUP AND RESTORE

3.1 GENERAL

The backup procedure consist of three different steps:

1. Make a data backup. The backup of the exchange is stored on each MX-ONE Service Node and should be done often. See chapter 3.3 for details.
This backup is used for data reload by the system.
2. Create a configuration mirror on MX-ONE Service Node 1. Store the data backups and configuration information from all MX-ONE Service Nodes to MX-ONE Service Node 1. This is part of the preparations for a safety backup and should be done on a weekly basis.

This backup contains all data for the system and can be used for *repair_lim*.

3. Make a safety backup. Copy the configuration mirror from MX-ONE Service Node 1 to tape backup or to another media.

This is an external backup of the complete system and can be used for *repair_lim* or to restore a complete system when all hardware is lost.

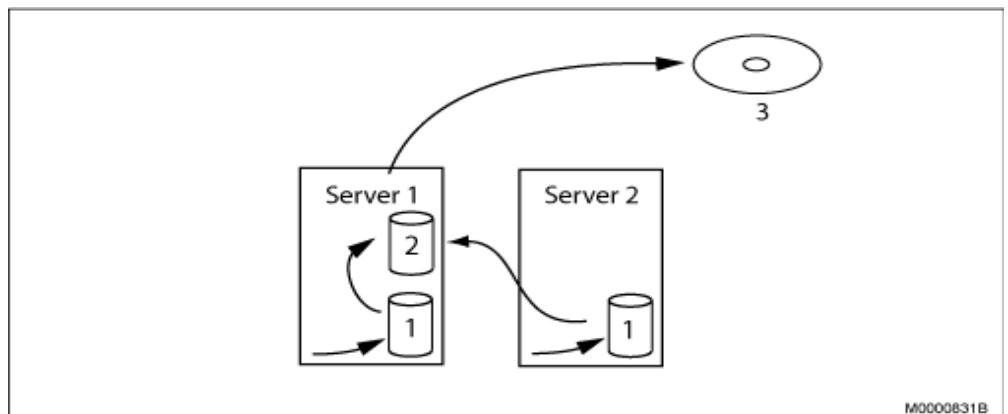


Figure 1: The Backup Steps

The three steps do not have to be performed at the same time. It is possible to make a data backup without creating a configuration mirror, and to create a configuration mirror without making a safety backup.

By using crontab, it is possible to create automatic data backups, configuration mirrors, and safety backups.

When there is inconsistency in the exchange data in the system it is necessary to restore from a backup. The restore procedure consist of three corresponding steps:

1. Restore a safety backup. Restore the safety backup to MX-ONE Service Node 1.
2. Restore a configuration mirror to MX-ONE Service Node 1. Restore the data backups and configuration information from MX-ONE Service Node 1 to all MX-ONE Service Nodes.
3. Restore a data backup. Restore the data backups on all MX-ONE Service Nodes.

As for the backup procedure, the three steps do not have to be performed at the same time. If there are inconsistencies in the exchange data, it may be sufficient to restore the last data backup.

3.2 DATA BACKUP

3.2.1 GENERAL

At a data backup, the exchange data for program units is stored in the file system. When a program unit is reloaded, exchange data for all program units is restored to prevent exchange data inconsistency.

Restore of exchange data can result in loss of exchange data. However, the exchange data in the system is consistent after a complete data restore.

As part of certain error recovery routines, the exchange data will be restored from the backup in order to revert the system to the last known state with data consistency.

Exchange data includes:

- System configuration data
- Application data (for example, extensions and trunks). The application data are altered either by command (for example, adding extensions) or by extension procedure (for example, call diversion)

Exchange data should be saved to backup regularly. The data should also be stored after:

- Loading the system initially
- Changing hardware configuration
- Upgrading a program unit
- Altering application data by command (for example, adding extensions)

A new directory is created for each backup in the directory `/var/opt/eri_sn/<version>` where `<version>` is the version of MX-ONE Service Node. The backup directory is named `xdata_y_z`, where `y` is MX-ONE Service Node number and `z` is a time stamp (date and time). A backup file for each program unit that has exchange data is created in the backup directory. Only program units that have exchange data have files in the backup directory. An LDIF file is also created in the backup directory. The LDIF file contains a snapshot of the exchange data in LDAP at the time for the backup. The LDAP data is written in Ldap Data Interchange Format.

The data configuration file `xdata_y.conf` is updated to include the new backup. Valid backups are specified in the data configuration file. The five latest backup directories are stored. If more backups are made, the oldest backup directory is deleted.

At a data restore, the newest valid backup file is used. Exchange data in the entire system is restored from the data backup and the start phase after data restore is executed in all program units in the system.

To succeed with a backup, all program units in the system must have status Started. A program unit must have status Alive, Halfstarted, or Started to restore any data.

3.2.2 INITIATE A DATA BACKUP

Use the command *data_backup* to initiate a backup. The command can be executed on any MX-ONE Service Node (not in stand-by server).

Restore from data backup is sometimes done automatically by the system.

3.2.3 RESTORE FROM A DATA BACKUP

When there is inconsistency in the exchange data in the system it is necessary to restore from a data backup.

Use the command *data_restore* to restore exchange data. The command can be executed on any MX-ONE Service Node.

3.3 PERFORM DATA BACKUP OFTEN

The *data_backup* command is more light-weight, and the *data_restore* operation is heavier. The more un-committed changes there are, the heavier the *data_restore* operation will be.

The data in the LDIF file is compared to the data currently in LDAP. It then uses (slow) LDAP write operations to write all the changes needed in LDAP to make it match the data in the LDIF file. If there is much data that needs to be changed to make LDAP match the LDIF file, the operation becomes very slow and heavy.

Make it a habit to always commit all configuration changes, by doing a *data_backup* at once. During peak traffic, it is not a good idea to do any bigger configuration changes. At any time when bigger configuration changes can be made (with respect to traffic disturbance) a *data_backup* can also be made.

3.3.1 RELOAD AND LDAP DATA

As exchange data configuration data is stored as a mix of reload data and LDAP data, system actions are needed to make sure they are consistent with each other. Until these operations are completed, the system is in an inconsistent and unstable state. The duration of this inconsistent and unstable state must be kept as short as possible. To achieve this the differences between the current LDAP data and the most recent LDIF file must be kept small, by doing frequent data backups.

3.3.2 SET ENVIRONMENT VARIABLE

To avoid getting dangerously large differences between the LDAP data and the most recent LDIF file, both *mdsh* and the new commands have logic to check this and remind the administrator. This behavior can be configured by the use of the `$_MD_BACKUP_OPTION` environment variable.

The environment variable `$_MD_BACKUP_OPTION` can be set to:

AUTO

meaning that *data_backup* will be done automatically when needed for system stability. Manual *data_backup* is still needed to commit changes done after the automatic *data_backup*.

WARN-AUTO

meaning that warnings will be printed when *data_backup* is needed for system stability. When critically needed for system stability, an automatic *data_backup*

will be done. (Manual `data_backup` is still needed to commit changes done after the automatic `data_backup`.) (WARN-AUTO is the default if `$_MD_BACKUP_OPTION` is unset.)

WARN-BLOCK

meaning that warnings will be printed when `data_backup` is needed for system stability. When `data_backup` is critically needed for system stability, data changes will be blocked until a manual `data_backup` is done.

UNSAFE-GDSX-MODE

get a functionality that is generally very stupid, but that is needed for some GDS-X tests. This mode jeopardizes system stability. Never use this mode except for some specific GDS-X tests. Never use this mode in production systems.

3.3.3 DATA BACKUP ALARM

The alarm code 1-37, Data backup needed, run `data_backup`, will be raised when the amount of uncommitted changes (the differences between the LDAP data and the most recent LDIF file) becomes dangerously large.

3.4 MIRROR CONFIGURATION TO MIVOICE MX-ONE SERVICE NODE 1

3.4.1 GENERAL

When creating a configuration mirror, all data backups and configuration files on each MX-ONE Service Node are stored on MX-ONE Service Node 1.

The command `config_mirror` creates a data storage in the directory `/mxone/mirror` on MX-ONE Service Node 1. The data from MX-ONE Service Node 1 itself and all other data needed to reconfigure the system is also stored in this directory.

A safety backup of the configuration mirror should be made. For more information, see 3.5 Safety Backup on page 9.

For each MX-ONE Service Node, there is a directory on MX-ONE Service Node 1 containing a data backup together with all necessary configuration files.

The command `config_restore` restores a configuration mirror by distributing the data backups and the configuration files from MX-ONE Service Node 1 to all MX-ONE Service Nodes (including MX-ONE Service Node 1 itself).

When done, the complete system can be restored by running the command `data_restore`.

3.4.2 CREATE A CONFIGURATION MIRROR

Use the command `config_mirror` to create a configuration mirror on MX-ONE Service Node 1. The command is executed on MX-ONE Service Node 1.

Note: The command `config_mirror` is very CPU and memory intensive and can easily lead to too slow responses on traffic events and result in MX-ONE Service Node calls throttled alarms. If possible ensure that The command `config_mirror` is always run at low traffic times.

3.4.3 RESTORE A CONFIGURATION MIRROR

When there is inconsistency in the exchange data in the system and in the data backup it may be necessary to restore from a configuration mirror.

Use the command *config_restore* to restore a configuration mirror from MX-ONE Service Node 1 to all MX-ONE Service Nodes. The command is executed on MX-ONE Service Node 1.

3.5 SAFETY BACKUP

3.5.1 GENERAL

When having created a configuration mirror, a safety backup of the information should be made from MX-ONE Service Node 1.

It is possible to specify what information that should be included in the safety backup and also what device the safety backup should be written to. Any mounted storage device can be used. For tape recorders, it is also possible to specify if the tape should be rewound before and after the safety backup is performed.

If there is an inconsistency in the MX-ONE Service Node data, the safety backup can be restored to MX-ONE Service Node 1. After having restored the configuration mirror to all Servers, the MX-ONE Service Node data backup can be restored.

Note: If possible ensure that memory intensive processes, such as safety backup, are always set to run at low traffic time.

3.5.2 MAKE A SAFETY BACKUP

The default is to backup the directories */etc/opt/eri_sn* and */eri_sn/mirror*. It is possible to add more directories to the safety backup (see step 3 below).

1. Make sure that the data backup and config-mirror is made on the system.
2. On Server 1, change user to root.
3. Open the file */etc/opt/eri_sn/<version>/safety_backup.conf* where <version> is the version of MX-ONE Service Node, in an editor.
4. Check the values for the keys **Device** and **Rewind**. Update if necessary.
5. Check the information in the **Include** line. Update if necessary.
6. Save the file.
7. Run the safety backup script by entering the command **eri_sn_safety_backup**.

3.5.3 RESTORE FROM A SAFETY BACKUP

If there is an inconsistency in the MX-ONE Service Node data (for example, mismatch between exchange data and configuration files), or if the MX-ONE Service Node has reported a missing or faulty exchange data file or configuration file, it is necessary to restore from a safety backup.

It is recommended to restore all the files from the backup since only restoring a subset of files is likely to cause inconsistency. The safety backup should match the installed MX-ONE Service Node programs.

1. Make the safety backup accessible from MX-ONE Service Node 1.
2. Check the safety backup and make sure that the files that need to be restored are available in the backup.
3. On Server 1, change the working directory to / (root directory).

Note: It is very important to change the current working directory to / (root) to prevent the safety backup from being restored in the wrong directory. The safety backup will always be restored to the current working directory (according to the pwd printout).

4. List the files in the safety backup with the command **tar -t --file=xxx**, where xxx is the safety backup file.

It is possible to find the differences between the safety backup and the file system with the command **tar -d --file=xxx** (current working directory must be /). For more information about tar, use the command **tar -help**

5. To restore all the files from the backup and overwrite the existing files, enter the command: **tar -x -p --overwrite -v --file=xxx**
6. Restore the configuration mirror from MX-ONE Service Node 1 to all MX-ONE Service Nodes by the command *config_restore*. For more information, 3.4.3 Restore a Configuration Mirror on page 9.
7. Restart the **xinetd** service on all MX-ONE Service Nodes with MX-ONE Classic Stackable media gateways. Use the command **/etc/init.d/xinetd restart**.
8. Restore the data backups by the command *data_restore*. For more information, 3.2.3 Restore From a Data Backup on page 7.
9. Enter the command **start --system** to coordinate the system.
10. Enter the command **restart --system** to restart the system.

3.6

SCHEDULE AUTOMATIC BACKUP

3.6.1

GENERAL

Include the backup commands (*data_backup* and *config_mirror*) in the table for scheduled commands on MX-ONE Service Node 1, **crontab**, to activate automatic backup of the MX-ONE system.

Crontab uses the editor specified by certain environment variables. Use the command **man crontab** to find out which environment variables. To check the environment variables, use the command **echo \$variablename**. If the editor is unfamiliar, it is possible to change it.

For more information, such as the format of the crontab command, see the online reference manual pages for crontab. Use the command **man 5 crontab**.

It is recommended to be MX-ONE Service Node Administrator user (mxone_admin) when executing the crontab command.

For security reasons the scheduling of safety backups (using the command *eri_sn_safety_backup*) needs to be done by root user.

3.6.1.1

Activate Automatic Backup

1. Enter the command **crontab -e** to open an editor.
2. Add lines containing when to run scheduled commands. The first 5 fields specify when to run the command and the remaining field what command to run (see examples below). It is recommended to allow at least 30 minutes between the different jobs.

The fields must be separated by at least one space. Use a header line (starting with #) to make the information easier to read.

3. Save the file and close the editor. Crontab installs the new table for scheduled commands.
4. If necessary, update the safety backup configuration. For more information, 3.5.2 Make a Safety Backup on page 9.

Example 1:

Make a data backup every night at 01:25.

#min	hour	day	month	weekday	command
30	01	*	*	*	/opt/eri_sn/bin/mdsh -c data_backup

Example 2:

Make a data backup every night at 01:25 and generate an alarm if data back fail.

#min	hour	day	month	weekday	command
30	01	*	*	*	/opt/eri_sn/bin/mdsh -c data_backup ; if [\$? != 0] ; then /opt/eri_sn/bin/alarm -i -C 1 -D 10000 --alarm-severity 3 --alarm-text "Automatic data backup failed" ; fi

Example 3:

Make a data backup every Thursday night (4th day of week) and Sunday night (7th day of week) at 00:45.

#min	hour	day	month	weekday	command
45	00	*	*	4,7	/opt/eri_sn/bin/mdsh -c data_backup

Example 4:

Make a data backup every Monday (1st day of week) and Friday (5th day of week) at 22:00. Create a configuration mirror every Friday at 23:00.

#min	hour	day	month	weekday	command
00	22	*	*	1,5	/opt/eri_sn/bin/mdsh -c data_backup
00	23	*	*	5	/opt/eri_sn/bin/mdsh -c config_mirror

Example 5:

Make a data backup every night at 02:00. Create a configuration mirror every Sunday night (7th day of week) 02:30.

#min	hour	day	month	weekday	command
00	02	*	*	*	/opt/eri_sn/bin/mdsh -c data_backup
30	02	*	*	7	/opt/eri_sn/bin/mdsh -c config_mirror

Example 6:

Make a safety backup every Sunday night at 03:00. Note that you must be root user.

#min	hour	day	month	weekday	command
00	03	*	*	7	/opt/eri_sn/bin/eri_sn_safety_backup

3.6.1.2*Change Scheduled Automatic Backup*

1. Enter the command **crontab -e** to open an editor.
2. Update the lines specifying when the commands are scheduled with new time and date.
3. Save the file and close the editor. Crontab installs the new table for scheduled commands.

3.6.1.3*Deactivate Automatic Backup*

1. Enter the command **crontab -e** to open an editor.
2. Remove the lines containing scheduling of commands.
3. Save the file and close the editor. Crontab installs the new table for scheduled commands.

4 SYSTEM START, RESTART AND RELOAD

4.1 GENERAL

Note: Do not mix up the system start/restart/reload with the Linux start/restart/reload.

Start/Restart phase 1

The system (or program unit) is cleared from traffic and the system information is cleared.

Start phase 1.3

System configuration data is updated.

Start phase 1.5

System information (other than system configuration data, for example, links between program units) are updated.

Start/restart phase 2

The system (or program unit) is prepared for traffic.

Start after data restore

The system updates data to match exchange data restored from backup (for example, an extension that was added after the last backup occasion is removed).

Event	Start Phase 1	Restart Phase 1	Start Phase 1.3	Start Phase 1.5	Start Phase 2	Restart Phase 2	Start After Data Restore
Initial start	1-All		2-All	3-All	4-All		
Data restore							1-All
Data backup							
Restart program unit		1-PU in question		2-All		3-PU in question	
(Restart MX-ONE Service Node)		(1-All PU in MX-ONE Service Node)		(2-All)		(3-All PU in MX-ONE Service Node)	
Restart system		1-All		2-All		3-All	
System start (also called coordination start)			1-All	2-All			
Reload program unit/Program unit termination		1 - PU in question		2-All		3-PU in question	4-All
Recovery from Media Gateway error				3-All		2-All PU in MX-ONE Service Node	

Note: A start after data restore is preceded by restore of exchange data from backup. The numbers (1/2/3/4) indicate the start phase sequence.

4.1.1

START

A program unit must have status **Halfstarted** or **Started** to perform a start. A start does not affect the traffic.

4.1.2

RESTART

A program unit must have status **Alive**, **Halfstarted** or **Started** to perform a restart. At a restart of one program unit, connections may be disrupted depending on the function of the program unit.

At a system restart (restart of all program units in the system), all traffic is stopped.

4.1.3

RELOAD

The program unit is terminated. The program unit is reloaded from the hard disk and the data for the program unit are restored from the backup. The program unit is restarted. Restore of data in the entire system and start after data restore follows.

4.1.4 PROGRAM UNIT STATUS

Status	Meaning
Not loaded	There is no program unit loaded in the system with program unit number or name.
Terminated on purpose	The program unit was terminated due to a command initiated reload.
Terminated	The program unit was terminated due to: <ul style="list-style-type: none"> • System action, for example, a program unit is executing a job too long and program unit is forced to terminate. • Program error, such as segmentation fault.
Alive	The program unit is loaded, but data have not been restored and start or restart is not executed.
Half started	The program unit has failed to restore data or complete one or several start phases or both.
Started	The program unit has completed all start phases and data from backup was successfully restored.

4.1.5 PROGRAM UNIT TYPE

The characteristics of the program unit is specified in a 32-bit variable, the **Type** variable. Each bit indicates a certain characteristic. Every bit set indicates that the program unit has the characteristic. Only bits described in the table below are used by the system.

Type variable (hexadecimal value)	Characteristics
0x00000080	Alarm sending
0x00000100	Has cross address checking function
0x00000200	Necessary for the traffic in the system
0x00000400	Necessary supervision program unit which contains automatic fault recovery measures
0x00000800	Common function
0x00001000	Device handling program unit
0x00002000	Device handling program unit dealing with auto initiated device
0x00004000	Program unit requiring information whether the MX-ONE Service Node, where the program unit is located, is isolated
0x00008000	Program unit capable of handling external synchronization
0x00040000	Cannot be removed by command
0x00080000	Does not have exchange data

Example: If the Type variable has the value 0x00000180, the program unit is alarm sending and has cross address checking function.

4.1.6 SUBSYSTEM LEVEL (TYPEEXT)

The function of the program unit at subsystem level is specified in a 32 bits variable, the TypeExt variable. The TypeExt variable consists of the sub-variables described in the table below.

TypeExt sub-variable	Bit(s) in variable	Meaning
PCSUBSYST	B0-B3	Indicates which subsystem the program unit belongs to.
PCPUTYPE	B4-B8	Indicates if a device or unit belongs to a certain type. (Commonly used to mark the presence of optional programs or blocks.) The value of this sub-variable varies for the different subsystems.
PCHANDLERINTERFACE	B13	The program unit has an interface to a handler unit.
PCDISTRIBUTIONINTERFACE	B14	The program unit has an interface to a distribution unit.
PCHWINTERFACE	B15	The program unit has an interface to hardware (that is, it is a device board handling program unit).

4.2 START AND RESTART SYSTEM

To start the system, enter the command *start* and specify system.

start --system

To restart the system, enter the command *restart* and specify system.

restart --system

4.3 RESTART PROGRAM UNIT

To restart a program unit, enter the command *restart* and specify the program unit.

restart -u XAMPLE -I 1

restart --unit XAMPLE --Lim1

4.4 RELOAD SYSTEM

All the program units in the system are reloaded. A valid backup must be available before attempting to reload.

To reload the system, enter the command *reload* and specify system.

reload --system

4.5 RELOAD PROGRAM UNIT

The program unit is terminated. The program unit is reloaded from the hard disk. Exchange data of the program unit is restored from the backup. The program unit is restarted. Restore of data in the entire system and start after data restore follows. A valid backup must be available before attempting to reload.

To reload a program unit, enter the command *reload* and specify the program unit.

reload -unit XAMPLE

4.6 SHUT DOWN SYSTEM

1. Enter the command *media_gateway_start* and specify shutdown to shutdown the Media Gateway.
2. Enter the command */etc/init.d/eri_sn stop* to shutdown the MX-ONE Service Node.

Note: Must be executed with root privileges.

5

USING THE RECOVERY IMAGE

In case you need to reinstall your system and restore data, follow the instructions below.

Note: The Recovery Image procedure deletes everything on the server, including existing data backups. If you intend to reuse any files, such as configuration files and data backups that exist on the server that you are going to do a recovery on, then you must transfer these files and data backups to another location (for example, to a USB memory stick).

In the following instructions the phases of waiting for the system to boot and transfer files are skipped. In some steps an estimated time is given.

5.1

CREATE A BOOTABLE USB-STICK

To create a bootable USB-stick:

1. Download the Recovery Image from the Knowledge Base. Check the md5 sum of the file before using it. If not correct, download again.
2. On a Windows PC open the ISO image with a proper program such as daemon tools.
3. The USB stick MUST be formatted with fat32.
4. Copy the content (not the ISO image) from the Recovery Image to a USB-stick.
5. Install bootloader on the USB drive, from command prompt in Windows. (Make sure you are running the command prompt as administrator in Win 7 & above).

`X:syslinux.exe --directory /boot/x86_64/loader [--force] --mbr --active X:`

Replace X: with the drive letter the USB drive shows up as (DO NOT USE C:). If it seems like nothing happened, it is usually done.

Note: A file named *ldlinux.sys* may appear on the USB drive, that is normal.

6. Rename `common.xml` to `common_dvd.xml`
7. Rename `common_usb.xml` to `common.xml`

The USB should now in theory be bootable.

When booting from USB: Select USB as boot device in BIOS.

A startup screen will show up:

- type *install* to start the installation.

5.2

SET HW CLOCK

Before using the Recovery Image it is necessary to set the server hardware clock to a relatively accurate current time. Enter BIOS mode. Set the current date. Save and exit.

Note: If the clock is too far off the recovery will fail.

5.3

RECOVERY IMAGE FOR MIVoice MX-ONE SERVICE NODE

One recovery image is provided for the recovery of a MX-ONE Service Node Mitel ASU Lite, ASU or Mitel ASU-II.

Note: SW RAID 1 is used if Mitel ASU and ASU-II have two hard disc drives.

1. Boot the server from the USB.
2. Press F3-key to change display resolution to 800X600.
3. Select **Installation** from the menu. If no selection is made in the boot choice menu the default installation type is executed automatically, for example, boot from hard disk.

The installation starts installing LINUX and the MX-ONE Service Node software during approximately 25-30 minutes. After installation is complete the message "Please Reboot System now" will be shown.
4. Logon as user root with password changeme, then type command reboot and press Enter. Wait for system to reboot.
5. The server is now in the same default status as it was when delivered from the factory (Turnkey).
6. Select **Yes** when the following message is displayed: *Welcome to MX-ONE. You have to configure your system before starting the MX-ONE. Do you want to configure your server now?*
7. Continue with installation and configuration of the system, see the installation instructions for *INSTALLING AND CONFIGURING MIVoice MX-ONE* section NETWORK AND SYSTEM CONFIGURATION.

6

LICENSE HANDLING

6.1

GENERAL

The MX-ONE is currently shipped with a 20 days trial license file. This means that the exchange can be set up fully functional during installation without any other license file.

Note: If no commercial license file is installed within 20 days, the MX-ONE Service Node will not function. Contact your local dealer/distributor to get access to the Aastra Connect and register you in the system to get a license file.

The MX-ONE Service Node contains a license server to prevent unauthorized use of system resources.

Each license consists of a license tag of up to 40 characters, the product number for licenses, the number of currently used licenses, and a maximum number of licenses. The maximum number of licenses must not be exceeded unless the trial period is activated. The trial period will allow an unlimited use of all licensed sales objects for a limited period of time.

The principle for license handling in the MX-ONE Service Node is that a unique MX-ONE Service Node hardware ID is checked towards an encrypted license file. If the license file does not include the correct hardware ID, it will not be possible to change customer data controlled by licenses.

6.2

REGISTER AND RECEIVE A LICENSE FILE

Do as follows:

Note: Contact your local dealer/distributor to get access to Aastra Connect.

1. Open **Mitel Connect**, <https://connect.mitel.com/connect>. The **Mitel Connect** is displayed.
2. Type your user name in the field **User Name**.
3. Type your password in the field **Password**.
4. Click **Login**. The welcome page is displayed.
5. Select **Licenses & Services**. The **Mitel Licenses & Services** page is displayed.
6. **Type or Paste** the **voucher number** you got via e-mail in the field **Voucher** under **Register voucher**.

Note: You can search the voucher number if you do not know the voucher ID, but have order information such as Mitel order number or partner order number.

7. Click **Register voucher**. The step **Voucher input** is displayed. Under **Voucher contents** you will see all information of your voucher registration.

Note: The progress line on the top, guides you in the registration flow, green boxes indicates successful entering information.

Note: You can create more than one voucher at a time.

8. Click **Next**. The step **System data** is displayed.
9. Type the **license number (for MX-ONE, hwid=Hardware ID)** in the field **EID/Serial***, for example hwid 12345-12345-12345-12345, 29 characters.

Note: Note! For a new system you have to type a new hwid, and for an add-on you have to type an already registered hwid.

10. Check the information under **Ownership Information** and **Feature changes**.

Feature changes

Part number	Part name	Registered	Quantity	
			Voucher	Sum
86L00004AAA-A	MX TS Telephony System 5.0	0	1	1
FAL1045302	MX TS IP extension 1 port	0	10	10
FAL1049028	MX TS Gateway	0	1	1
FAL1046789	MX TS 1 User	0	10	10
Basic	MX TS Telephony System SWB	0	1	1
Basic	MX TS Telephony User SWB	0	10	10
Basic	MX TS Gateway SWB	0	1	1

Figure 2: The step Feature changes

11. Click **Confirm input**. The step **Processing message** is displayed.

Progress

Processing message

Please check your entries.

If you confirm the selected licenses, the new license code will be generated. No undo!
Please go back to the selection page, if you want to modify your inputs.

System data

IPA no.:
 EID / Serial: 345621-214356
 Product type: MX-ONE
 Release: 5.x

Figure 3: The step Confirm changes

12. Click **Confirm & Generate License Key**. The **license file** generates and sends to you via **e-mail**.

License Generated

Your license file/code has been generated successfully.

IPA no.: SN-80391

The file has been sent to your e-mail address: teliapartner@gmail.com

[» Download the current license file](#)

Figure 4: Confirmation of generated License file

Note: For more information of how you register, search and download license files, please see help in **Mitel Connect**.

6.3 INSTALL LICENSE FILE

1. Print the hardware ID of the MX-ONE Service Node by typing the command ***license_status -s***.
Format for the hardware ID is: **<5 hexadecimal digits>-<5 hexadecimal-digits>-<5 hexadecimal digits>-<5 hexadecimal digits>-<5 hexadecimal digits>** (the format may change without prior notice in future releases).
- Note:** The hardware ID is the same as the “Exchange” line in the license file.
2. Order and register a license file in Aastra Connect.
3. Transfer the license file to the MX-ONE Service Node’s file system. e.g. */local/home/mxone_admin/*
4. Key command ***sudo -H /opt/mxone_install/bin/mxone_maintenance*** to start MX-ONE Maintenance Utility.
5. Select option license and select install license file:
 - If the MX-ONE Service Node is running, the new license file is installed and activated
 - If the MX-ONE Service Node is not running, start the MX-ONE Service Node with the new license file by typing: ***/etc/init.d/eri_sn start***
6. Enter the command ***license_status*** to verify that the license file is activated correctly.

6.4 PRINT LICENSE FILE

Enter the command ***license_print -file <full path + file name>*** to print the encrypted license file to view the license information.

6.5 LICENSE USAGE REPORTS

6.5.1 GENERAL

The purpose of the feature License Usage Reports is to enable an easy way to keep track of how licensed resources are utilized over time.

Daily peak values and snapshots of currently seized licenses are periodically taken and archived for future use.

The reports are generated at 10:00, 14:00 and periodically every programmed number of hours. The minimum interval is 1 hour, maximum 24 hours.

After midnight the previous day's peak value and reports are packed into a package of daily reports. The reports can be automatically mailed to one or more predefined mail addresses in intervals of 1 day or longer. The mail interval starts at the beginning of, and ends at the end of, each month when a mail is also generated if an interval is programmed.

Reports can also be automatically erased after a programmable length of time.

Each report contains an encrypted authentication checksum to prevent manipulation. Reports can be manually generated or erased at any time with command.

Reports are stored on the MX-ONE Service Node main server under directory `/var/opt/eri_sn/<version>/usage_report`.

Note: There are no alarms generated if reports are not possible to archive due to disk space shortage or other disk problems.

The command *license_report* is used to manage this function, see command description *TECHNICAL REFERENCE GUIDE, UNIX COMMANDS* for details.

The function is controlled by a license.

Set a license report mail address, with a report interval of 2 hours, and a mail interval of 14 days. If not set, a default time interval and Mitel mail address will be valid.

license_report -mail-address administrator@mitel.com -report-interval 2 -mail-interval 14

6.5.2

CUSTOMER GROUP LICENSE REPORTS

If the function usage report is active and the system have customer group data initiated, usage data for each such group will be generated.

Each time a license is seized the generation is done via command "customer_report". The command will generate certain predefined licenses. These licenses are feature levels, terminals and groups. This command is not be used from command line.

The peak value license usage for each group will be kept and included in the daily package of reports.

If customer group is to be charged for license usage, an individual "finance ID" can be assigned per customer group.

7

MEDIA GATEWAY UNIT

The Media Gateway Unit is a hardware based media gateway, see the *MGU DESCRIPTION* and *MGU2 DESCRIPTION*.

7.1

SETUP MEDIA GATEWAY ETHERNET PORTS

For more information, see the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE*.

7.2

INITIATION OF MGU

See the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE*.

7.3

VIRTUAL BOARDS

For information on virtual boards, please see the parameter description for *BRDID*, in *Technical Reference Guide, MML parameters*.

7.4

UPDATE AND UPGRADE OF MGU SOFTWARE

The Media Gateway Unit comes fully functioning, with a bootable Linux Operating System and with an operable version of the MGU software, which will be started at power on. It may be necessary to upgrade the MGU to a newer version. This MGU firmware update/upgrade has to be initiated manually.

For more information, see the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE* or see the installation instructions for *UPGRADING AND UPDATING*.

When the firmware has been updated or upgraded, the Media Gateway is restarted automatically. After restart, the new firmware is installed on the Media Gateway.

7.5

START AND RESTART MEDIA GATEWAY

The Media Gateway Unit is automatically started and connected to the MX-ONE Service Node once it is powered on.

7.6

LED INDICATIONS IN THE MEDIA GATEWAY

There is a LED indication on the Media Gateway Unit's front panel: green light indicates OK, and red light not OK. See the *MGU DESCRIPTION* or *MGU2 DESCRIPTION* for details.

8 MEDIA SERVER

The Media Server is a software based media gateway, with functionality similar to the MGU, see the *MEDIA SERVER DESCRIPTION*.

8.1 INITIATION OF MEDIA SERVER

See the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE*.

8.2 UPDATE AND UPGRADE SOFTWARE

The Media Server software is installed on the Service Node server or any server where the MS shall run, and is automatically started at startup of the operating system. Upgrading of the MS will be performed by upgrading or updating the MX-ONE Service Node via the *mxone_maintenance* tool.

For more information, see the installation instructions for *INSTALLING AND CONFIGURING MIVOICE MX-ONE* or see the installation instructions for *UPGRADING AND UPDATING*.

8.3 START AND RESTART MEDIA SERVER

The Media Server is automatically started and connected to the MX-ONE Service Node once it is powered on.

9

INTER-MEDIA GATEWAY RTP COMMUNICATION

9.1

GENERAL

In an MX-ONE system with several Media Gateways with local MX-ONE Service Nodes, it is necessary to set up RTP resources for inter-Media gateway communication to be able to make calls between the Media Gateways without using IP trunks.

The *rtp_resource* handling commands can be used for viewing RTP resources for an MX-ONE. For more information, see *TECHNICAL REFERENCE GUIDE, UNIX COMMANDS* for details.

When connecting a TDM device to an IP device, the RTP resource will be booked in the same gateway where the TDM device is situated.

When connecting two IP devices with forced gateway, or of a auxiliary device towards a IP device, the order to try to book the RTP resources will be in the following order.

- 1) Media Server in the same IP domain as at least one of the IP devices.
- 2) Any Media Server.
- 3) Media Gateway in the same IP domain as at least one of the IP devices.
- 4) Any Media Gateway.

At multiple choices the load will be distributed equally.

9.2

PRINT RTP RESOURCE INFORMATION

Print RTP resource information for a MX-ONE Classic. Use the command ***rtp_resource -lim 1,2*** to print information for Media Gateway 1 and 2.

Print codec information for the MX-ONE Classic. Use the command ***rtp_resource -lim 1,2 -info*** to print information for Media Gateway 1 and 2.

Print busy RTP resources for a MX-ONE Classic. Use the command ***rtp_resource -lim 3 -print busy*** to print information for node 3.

10

MIVOICE MX-ONE SERVICE NODE USER ADMINISTRATION

After a first time setup there is only one user on the MX-ONE Service Node and this user (root) has no restrictions. The commands in the MX-ONE Service Node are divided into eight levels, and it is recommended to analyze the need of several administrator levels on the server.

For more information about command levels, see the command description for *COMMANDS IN MX-ONE SERVICE NODE*.

For more information about user accounts on the Linux server, see the operational directions for *USER ACCOUNT MANAGEMENT*.

11

SYNCHRONIZATION

11.1

GENERAL

The synchronization function is used to receive synchronization from an external source, give sync to the system, display the external sources and rate the preferred source with class and priority.

Perform a re-synchronization after the sources are defined. If no source is specified, the Media Gateway or the MX-ONE Classic is using the internal clock.

Use the command *trsp_synchronization* to display external synchronization sources, define the external synchronization sources and re-synchronization of external synchronization sources in the Media Gateway.

Class "a" represents the highest quality on a synchronization source and class "d" the lowest quality. Priority "1" is chosen first and "3" last. The chosen synchronization source is the source defined with the best class. If several sources are defined with same class, priority is used.

11.2

DEFINE SYNCHRONIZATION SOURCES

1. Display the external synchronization sources for media gateway 2A.
trsp_synchronization -mgw 2A
2. Rate the preferred sources with class and priority.
trsp_synchronization -bpos 2A-0-00 -class b -prio 1
3. Re-synchronize after the sources are defined.
trsp_synchronization -resync -mgw 2A

11.3

DEACTIVATE SYNCHRONIZATION SOURCES

1. Reset not preferred synchronization sources **-class no** and **-priority no**.
trsp_synchronization -bpos 1B-0-00 -class no -prio no
2. Re-synchronize after the sources are defined.
trsp_synchronization -resync -mgw 1B

11.4

LBP22

LBP22 backplane is inter-connecting the PCM-sync pin of mag 0 and mag1 on bpos x-x-00. Therefore, 2 sync receiving boards (e.g. GJUL or TLUX), each located on x-x-00 in mag0 and mag1 would interfere with each other, causing the sync to become disturbed. This would cause sync problems for the system, particular for DECT systems. Entire media gateway synchronization will be disturbed including a connected Group switch. To avoid the conflict, moving one of them to a different position is a must. Any other combination of boards in these positions will not have any impact.

12 BLOCKING, DEBLOCKING

12.1 GENERAL

The blocking function is used for repairing. Ongoing traffic is not terminated but no new traffic is permitted for the devices that are blocked.

An alarm is generated when a device is blocked.

The deblocking function is used to cancel (erase) manual blockings and all types of system generated blockings or fault markings.

12.2 BLOCK A DEVICE

To block a device, use the command *block*.

block -bpos 1A-2-20

12.3 DEBLOCK A DEVICE

To deblock a device, use the command *deblock*.

deblock -bpos 1A-2-20

12.4 LIST BLOCKED OR DISTURBANCE MARKED DEVICES

To list blocked and disturbance marked devices, use the command *block_list*.

block_list -lim 1

13

ALARM HANDLING AND SNMP

For more information, see the operational directions for *ALARM HANDLING* and see the operational directions for *MIVOICE MX-ONE SNMP SUPPORT, ALARM NOTIFICATION AND EMERGENCY CALL EVENTS*.

14 SERVER HARDENING

The MX-ONE has been endowed with a set of configurations aiming to increase the system's security, reliability and resiliency to a number of malicious attacks.

14.1 IPTABLES

IPTables is a packet filter built into the Linux kernel. The filter has been configured to prevent that certain services running on the server for the MX-ONE Service Node, necessary for the server's correct functioning, can be reached from the corporate network (eth0). The following services have been blocked for incoming connections on eth0:

- vat
- postgresql
- clvm-cfg
- kerberos
- nfs
- sunrpc
- rmiregistry
- daytime
- tftp

Additionally, ICMP echo reply messages (ping) are limited to one response per second.

To display the actual IPTables configuration, type **iptables -L**

To remove a rule, for instance the one blocking the daytime protocol on eth0, type **iptables -D INPUT -i eth0 -p udp -m udp -dport daytime -REJECT**

For more information about how to configure IPTables, refer to the IPTables manual pages, type **man iptables**.

14.2 SSH CONFIGURATION

The MX-ONE is configured to not accept any SSH connection logging in as root. In case root privileges are required, it is necessary to log on as another user and then to use the command **su -**. The SSH configuration is saved in the **/etc/ssh/sshd_config** file.

14.3 SECCHK

Seccheck is a security tool used by the Suse Linux Enterprise Server Operating System. Seccheck comprises three scripts that are run respectively each day, each week and each month (as cron jobs). In case something is detected that might indicate a security breach, a mail is sent to the root user with a description of the problem.

The seccheck scripts are stored in the **/usr/lib/secchk** directory.

The seccheck script can also be run manually by typing:

- **/usr/lib/secchk/security-daily.sh** or
- **/usr/lib/secchk/security-weekly.sh** or
- **/usr/lib/secchk/security-monthly.sh**

The weekly and monthly seccheck scripts are very CPU and memory intensive and can easily lead to too slow responses on traffic events and result in **MX-ONE Service Node calls throttled** alarms. If possible ensure that these checks are always run at low traffic times. Check the settings in `/etc/cron.d/seccheck` on when the checks are executed. For operations where degrading of the telephony throughput is not acceptable or for other reasons the checks can be removed.

To remove the security check do the following:

Log-in as user `mxone_admin`, and key the command `sudo -H /opt/mxone_install/bin/mxone_maintenance` and select option `seccheck` and follow the instructions on screen.

15 FAULT LOCATION

15.1 GENERAL

For more information regarding fault location, see the fault locating instructions for *MIVOICE MX-ONE FAULT LOCATION*.

15.2 TRACE FUNCTIONALITY

The Trace functions in the MX-ONE Service Node is an integrated part of the system. The function consist of the following parts.

- Commands to administer the function – **trace**
- Program unit running on the processor – **LOGGER**
- Components integrated into the signaling mechanisms
- Code components specified in design rules
- Code provided from the designer

The Trace functions make it possible for the administrator to analyze the system performance and trace error conditions. The Trace functions can be used when integrating the system to verify the intended functions or to find problems in a system with traffic.

15.2.1 TRACE TYPES

The MX-ONE handles basically the following types of trace data:

- **Trace error log**
This log is dedicated to trace individual 0. This trace individual is always active and will record any abnormality detected in the MX-ONE. The log is cyclic, that is, overwrites the oldest entries when the log becomes full, filters which signals to store (is set), and it is possible to alter the size of the storage (1 up to 5000 entries, default is 500). The error trace cannot be removed or stopped.
- **Unit trace**
Can be initiated on the MX-ONE program units in one or all MX-ONE Service Nodes.
Exception: LLP and dynamically loaded commands or daemons (for example, board_sw and snmpd). Unit trace is set up by command and has no restrictions on options like filter etc.
- **Sequence trace**
Sequence trace can be initiated in several ways depending on what is known of the function that is to be analyzed. It is possible to start on a specific signal, with or without specific data and to start on a known directory number, or a known EQU position.
Exception: The directory number must be associated to a terminal, that is, not a group number. EQU positions must be an interface, for example, trunk line interface, extension line interface or operator line interface, not auxiliary device interfaces.
Sequence trace is set up by command and has no restrictions on options like filter etc.
- **Hardware trace**
Hardware trace is performed by copying all signals to or from hardware positions.

The trace is started on a complete 32 group in the addressing range. It is possible to exclude individual in the 32 group from the trace by setting a mask. Each signal sent in the HW interface will be recorded twice, once in signal format and once in raw format. This is done to help the debugging of signaling to and from a new interface board. (Filtering can be used to omit the unwanted copy.)

Hardware trace is set up by command and has no restrictions on options like filter etc.

15.2.2

PERFORM A TRACE

15.2.2.1

Initiation

1. Enter the command **trace -display** to check if there are free trace individuals.
2. Initiate the trace by using one of the commands below:
 - Trace started on a specific program unit.
trace -lim -unit
 - Trace started on a specific signal number.:
trace -lim -unit -signo [-byte]
 - Trace started on a specific signal name.
trace -lim -unit -signam [-byte]
 - Trace started on a directory number.
trace -dir
 - Trace started in a equipment position.
trace -equ
 - Trace started on a backplane 32 group.
trace -hwpos [-mask]
 - Trace started on the switch specific functions (LSU/DSU or Media Gateway internal functions).
trace -hwpos -switch [-mask]

15.2.2.2

Modification

It is possible to modify the behavior of the trace individual.

Note: The change command can be used any number of times as long as the trace has not started.

The following can be changed:

- The trace individual
- The trace individual can stop when maximum copies are received or overwrite the oldest
- The size of the trace buffer
- The signals to include or omit in the trace
- The kind of text trace copies to include in the trace
- A stop signal that will stop the trace if included in the trace
- Stop conditions if an error signal is received

- An information text to the trace individual (reminder or message to other users)

Note: Several trace individuals can use the same stop condition.

15.2.2.3

Start Trace

Enter the command **trace -start** to start the trace or traces.

Note: Several traces can be started with the same command.

15.2.2.4

Stop Trace

Enter the command **trace -stop** to stop the traces.

Note: Several traces can be stopped with the same command.

15.2.2.5

Display Trace Status

It is possible to check the status of the traces at any time. Status information can be printed without stating a trace individual. This will give a print of all 16 trace individuals statuses. If only one trace individual is given, only that trace individual will be printed.

If there is no LIM parameter, all buffer counters of the MX-ONE Service Nodes are added and printed. If there is a LIM parameter, the counter from that MX-ONE Service Node is printed. Depending on what type of trace that is initiated, different layouts will be used. All parameters entered are presented. Some additional information like pointers and program units, where a directory number resides, are also printed to help the administrator to identify the right data in the trace printout.

Related command and parameters are **trace -display [-lim]**

15.2.2.6

Print Trace Result

When a trace is stopped it is possible to print the trace result. In a multi Server system, the trace copies will be printed in chronological order. It is possible to print from a specific MX-ONE Service Node with the LIM parameter. It is also possible to print copies containing a certain signal number, or to print a range of copies. To change the printout format a show parameter can be given to omit the parts of the signal that are regarded as irrelevant in the printout format.

Related command and parameters are:

trace -print [-lim] [-from] [-to] [-signo] [-show]

Note: The trace information and status are always printed in the header before the actual trace information, so that the trace setup can be examined when analyzing the result.

15.2.2.7

Clear the Trace Buffer

Enter the command **trace -clear** to clear the content of the trace buffer.

Note: Several traces can be cleared with the same command.

15.2.2.8

Remove a Trace Individual

If a trace individual is not needed any more, free the trace individual by removing the trace configuration and placing the trace individual in idle state. The related command and parameter is: ***trace -remove***

16 SWAP AND REPAIR

16.1 SERVER

For replacement of the server, see the operational directions for *REPLACING MISCELLANEOUS HARDWARE* or see the operational directions for *REPLACING BOARDS IN MIVOICE MIVOICE MX-ONE MEDIA GATEWAYS* section *Replacing Mitel ASU Lite, ASU or Mitel ASU II*.

16.2 MEDIA GATEWAY

For replacement of the Media Gateway, see the operational directions for *REPLACING MISCELLANEOUS HARDWARE* section *REPLACING MEDIA GATEWAY* or see the operational directions for *REPLACING BOARDS IN MIVOICE MX-ONE MEDIA GATEWAYS*.

17

MIVOICE MX-ONE SERVICE NODE FILE STRUCTURE

17.1

FOLDERS

MX-ONE Service Node follows the typical structure of a Linux directory tree:

Table 1 Application executable files, static configuration files and configuration file templates

```
/opt/eri_sn/bin
/opt/eri_sn/etc
/opt/eri_sn/install
/opt/eri_sn/lib
/opt/eri_sn/sbin
/opt/eri_sn/upgrade
```

Table 2 Install packages, scripts, and utilities

```
/opt/mxone_install/bin
/opt/mxone_install/install_sw
/opt/mxone_install/target
```

Table 3 Active configuration files

```
/etc/opt/eri_sn
```

Table 4 Install configuration file

```
/etc/opt/mxone_install
```

Table 5 Reload data and system backup files

```
/var/opt/eri_sn/call_logging
/var/opt/eri_sn/ldap
/var/opt/eri_sn/traffic_recording
/var/opt/eri_sn/usage_reports
/var/opt/eri_sn/xdata
```

Table 6 Miscellaneous log files

```
/var/log/mxone
```

Table 7 Configuration files saved at uninstall

```
/tmp/mxone/mxone_install/savedAtUninstall
```

The directory /opt/eri_sn and the sub directories are write protected. The directories /etc/opt/eri_sn and /var/opt/eri_sn are write enabled.

17.2 CONFIGURATION FILE TEMPLATES

The following file templates are located in the directory /opt/eri_sn/etc:

- alarm_severity.conf
- alarm_text.conf
- awdb.conf
- board_characteristics.conf
- market.conf
- start_order.conf
- sudaem.conf
- swdb.conf

17.3 INSTALLATION AND UPGRADING CONFIGURATION FILES

The following files are located in the directory /etc:

- /etc/opt/mxone_install/serverData.conf
Contains configuration data for servers that is needed by the installation and upgrade. It is changed indirectly by the mxone_maintenance functions

Note: This file should not be updated manually

17.4 ACTIVE CONFIGURATION FILES

The following files are located in the directory /etc/opt/eri_sn:

- /etc/opt/eri_sn/<version>/mitelSIPphones/
- /etc/opt/eri_sn/<version>/sip_user_agents/
- /etc/opt/eri_sn/<version>/certs/
- /etc/opt/eri_sn/<version>/config_mirror.conf
- /etc/opt/eri_sn/<version>/ip_telephony.conf
- /etc/opt/eri_sn/<version>/ldap.conf
- /etc/opt/eri_sn/<version>/ldapLogin.conf
- /etc/opt/eri_sn/<version>/lic.dat
- /etc/opt/eri_sn/<version>/lic_feature_based.dat
- /etc/opt/eri_sn/<version>/lic_traditional.dat
- /etc/opt/eri_sn/<version>/llsp_unit.conf
- /etc/opt/eri_sn/<version>/mdsh.conf
- /etc/opt/eri_sn/<version>/mdsh.rc
- /etc/opt/eri_sn/<version>/safety_backup.conf
- /etc/opt/eri_sn/<version>/sip_trunk_profiles/

- /etc/opt/eri_sn/<version>/sip_user_agents/
- /etc/opt/eri_sn/<version>/status.conf
- /etc/opt/eri_sn/<version>/tls_telephony.conf
- /etc/opt/eri_sn/snmp/

Note: <version> is the version of MX-ONE Service Node.

17.5

RELOAD DATA AND SYSTEM BACKUP FILES

The following files and directories are located in the directory
/var/opt/eri_sn/<version>/xdata/:

- var/opt/eri_sn/<version>/xdata/xdata_z.conf
Configuration of valid backups, where z is the MX-ONE Service Node number. Removing this file will result in a restart with default reload data values if command *restart --system* is executed
- /var/opt/eri_sn/xdata/<version>/xdata_z_yyyymmddhhmm/
Backup directory where yyyy = year, mm = month, dd = day, hh = hour, mm = minute and ss = second when backup was executed. z is the MX-ONE Service Node number.

Note: <version> is the version of MX-ONE Service Node.

17.6

TRANSFER OF PCREGEN FILES FOR RESTORING DATA

Copy the files using text mode for transfer in order to get correct Restore Data. Do not ZIP the Print files.

18

HARD DISK MAINTENANCE

The service node software takes a bit more than 1 GB disk space. When the service node is to be upgraded disk space is needed for the current software, which might need to be restored in a roll back procedure. Disk space is also needed for the new software and during the upgrade procedure disk space is needed for temporary files.

In all **5 GB** of free disk space must be available on the root partition **in each MX-ONE Service Node** before a new version of the service node can be installed. When more disk memory is needed manually remove possible core dump files and unused service node versions.

To remove unused files or packages use the maintenance script:

1. Package handling
2. Remove