



A MITEL
PRODUCT
GUIDE

MiVoice MX-ONE

Installing MX-ONE Provisioning Manager - Installation Instructions

Release 7.7
9/1531-ANF 901 15 Uen L

May 2024

Notices

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), its affiliates, parents, or 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 2024, Mitel Networks Corporation

All rights reserved

Contents

1 Introduction.....	1
1.1 Installation Scenarios.....	1
1.2 Installation Using mxone_maintenance Script.....	1
2 Prerequisites.....	2
2.1 StandAlone Installation.....	2
2.2 Coexistence Installations on Server 1.....	2
3 Considerations.....	3
4 Security.....	4
5 Preparations.....	5
5.1 Obtaining a Digital Certificate.....	5
6 Installation.....	6
7 Accessing MX-ONE Provisioning Manager.....	8
8 MX-ONE Provisioning Manager Start and Stop.....	9
9 Upgrade.....	10
9.1 Upgrade of Standalone PM (7.5 SP1 or above).....	10
10 Migrating 5.x or 6.x Manager Provisioning Data to 7.x PM.....	11
11 Migrating from D.N.A. to MX-ONE Provisioning Manager.....	12
11.1 Migration Scenarios.....	12
11.2 Migrating from D.N.A. to MX-ONE Provisioning Manager.....	12
11.2.1 Exporting User and Department Data in D.N.A.....	13
11.2.2 Backing Up Data in MX-ONE Provisioning Manager.....	13

11.2.3 Importing D.N.A. Data in MX-ONE Provisioning Manager.....	14
11.3 Migrating from D.N.A. to MX-ONE PM in Environments.....	14
11.3.1 Exporting User and Department Data from D.N.A.....	15
11.3.2 Importing D.N.A. Data to CMG.....	15
11.3.3 Downloading and Installing the CMG Export Registry File.....	15
11.3.4 Exporting Data from CMG.....	16
11.3.5 Backing Up Data in MX-ONE Provisioning Manager.....	19
11.3.6 Adding CMG as a Subsystem in MX-ONE Provisioning Manager.....	19
11.3.7 Creating Locations for CMG Customer Groups in MX-ONE PM.....	19
11.3.8 Importing CMG Data in MX-ONE Provisioning Manager.....	19
11.4 Migrating to MX-ONE PM from Environments.....	20
11.5 Backing Up Data in CMG.....	21
11.6 Important Post-Migration Considerations.....	21

12 Post Installation..... 22

13 Uninstallation.....23

14 Log Files..... 24

15 Fault Recovery..... 25

16 Increasing Heap Memory Size in Jboss Configuration File..... 26

17 Generating a Certificate Signing Request.....27

18 Downloading the Certificate(s) of third-party servers..... 34

This chapter contains the following sections:

- [Installation Scenarios](#)
- [Installation Using mxone_maintenance Script](#)

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.

1.1 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.

1.2 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

This chapter contains the following sections:

- [StandAlone Installation](#)
- [Coexistence Installations on Server 1](#)

The prerequisites depends on the installation type.

2.1 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 CONFIGURING MIVOICE MX-ONE*.

Follow the instructions during the installation. When running `net_setup` command, choose to configure the server for Other Server.

2.2 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*.

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.

Provisioning Manager can run in HTTP and HTTPS. By default, the system is configured in HTTPS and TLS 1.3.

Provisioning Manager and Service Node Manager support both RSA and ECDSA digital signature algorithms. However, the ECDSA key is not available when a Self-Signed certificate is created.

For information about how to generate a Certificate Signing Request (CSR), see [Generating a Certificate Signing Request](#) on page 27 - how to generate a Certificate Signing Request, which has to be used by Provisioning Manager and Service Node Manager.

This chapter contains the following sections:

- [Obtaining a Digital Certificate](#)

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

5.1 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 `webserver_config` command and then chooses to modify web server protocol + HTTPS.

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`, select the 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** in each of these dialog boxes to continue the installation, or select **No** to exit the installation.
4. Wait until the software is installed.
5. Follow the on-screen instructions.
6. Enter **first 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.

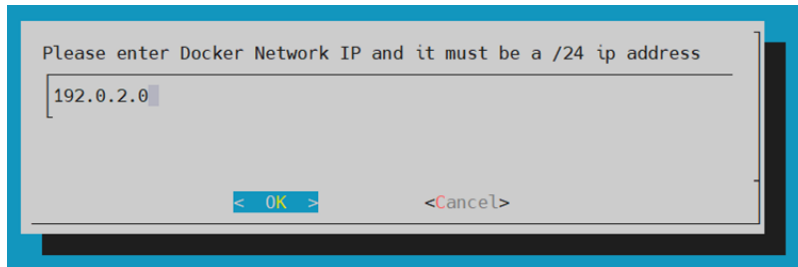
10. Enter a password that needs to be associated with the certificate.
11. Reconfirm the password.
12. Enter a valid IP address or FQDN details for the certificate generation.
13. Select a bit size for the certificate (2048 or 4098)
14. Select a digest bit size for the certificate (SHA256 or SHA384 or SHA512). A popup screen appears showing the certificate generation is completed.

Note:

The RSA self-sign certificate is valid for 60 days only. The user needs to change the certificate manually after 60 days.

15. Select **Yes** to do a restart or select **No** to restart the system later.

16. Enter the IP address for the Docker network. The default IP address is 192.0.2.0.



i Note:

As we transitioned from a monolithic service to a microservice architecture, we isolated each service from one another. To achieve this, we use Docker, which offers the capability to package and execute applications within loosely isolated environments known as containers. This isolation and security enable you to run multiple containers simultaneously on a given host. Containers are lightweight and encompass all the necessary components for running an application, eliminating the need to depend on the host's installed software. You can seamlessly share containers while you work, ensuring that everyone you share them with receives an identical container that functions in the same manner.

i Note:

- Docker requires an IP network for internal service communication. The user must provide an IP address domain in the format /24, reserving the entire range of 255 IP addresses for the Docker network. The IP domain address must be provided in the format XX.XX.XX.0; for example, 192.0.2.0. The first IP address in the given network (XX.XX.XX.1) serves as the Docker network gateway IP address. Docker IP domain need not to be same as the PM/SNM server IP domain.
- For the Docker network IP reservation, it is recommended to avoid using any IP addresses from the range already allocated to the Docker network. Doing so could disrupt communication between containers and potentially result in the unavailability of certain services in PM/SNM. To ensure smooth operation, we strongly advise reserving the entire range of 255 for the Docker network.

17. To configure protocol (HTTP/HTTPS + certificate), run the `webserver_config` command when the installation is completed.

Accessing MX-ONE Provisioning Manager

7

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

To overcome security issues and to prevent unauthorized access, the IP address or FQDN on which PM/ SNM is addressed has to be added as trusted IPs. This is achieved using the option available in *Webseal IP management*, *webserver_config* command or *sudo mxone_maintenance > webmanagement*. For example; if in a redundancy setup, an alias IP is configured, this also must be added as a trusted IP or the server's FQDN on which the PM is reached. If the WebSEAL IP is not configured when trying to access Provisioning Manager and Service Node Manager, an error message will be displayed to the user, for example; '404 - Not Found'.

MX-ONE Provisioning Manager Start and Stop

8

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 CSTAPhaselll.

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`

This chapter contains the following sections:

- [Upgrade of Standalone PM \(7.5 SP1 or above\)](#)

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_config` command 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 **mpManagerPostgresDump.<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](#) on page 6 and follow the on-screen instructions.

9.1 Upgrade of Standalone PM (7.5 SP1 or above)

From version 7.5 SP1, the PM and SNM have been modernized and now use the Docker for containerization. It is not possible to directly upgrade a standalone PM server running with a version below 7.5 SP1. User must install the PM along with the MX-ONE, as the docker configuration is part of the complete build package from version 7.5 SP1.

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

10

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

11

This chapter contains the following sections:

- [Migration Scenarios](#)
- [Migrating from D.N.A. to MX-ONE Provisioning Manager](#)
- [Migrating from D.N.A. to MX-ONE PM in Environments](#)
- [Migrating to MX-ONE PM from Environments](#)
- [Backing Up Data in CMG](#)
- [Important Post-Migration Considerations](#)

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.

11.1 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 [Migrating from D.N.A. to MX-ONE Provisioning Manager](#). 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 PM in Environments including CMG](#).
- 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.

11.2 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).

11.2.1 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

11.2.2 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**.

11.2.3 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](#) on page 13.

11.3 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.

11.3.1 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 these 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 Department Data in D.N.A. on page 12](#)

11.3.2 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.

11.3.3 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.

11.3.4 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`.

Figure 1: Edit tab

Server: EUA2 DBID: 01

File Command ?

Program: EXPORT_MP

Program path: export.exe

Parameters: -n EXPORT_MP

Wait: 0

Max restarts: 0

Start order: 0

Enabled: ☒

Desktop: ☐

State: Running

Start time: 08-05-06 11:09

Errors: 0

Additional parameters

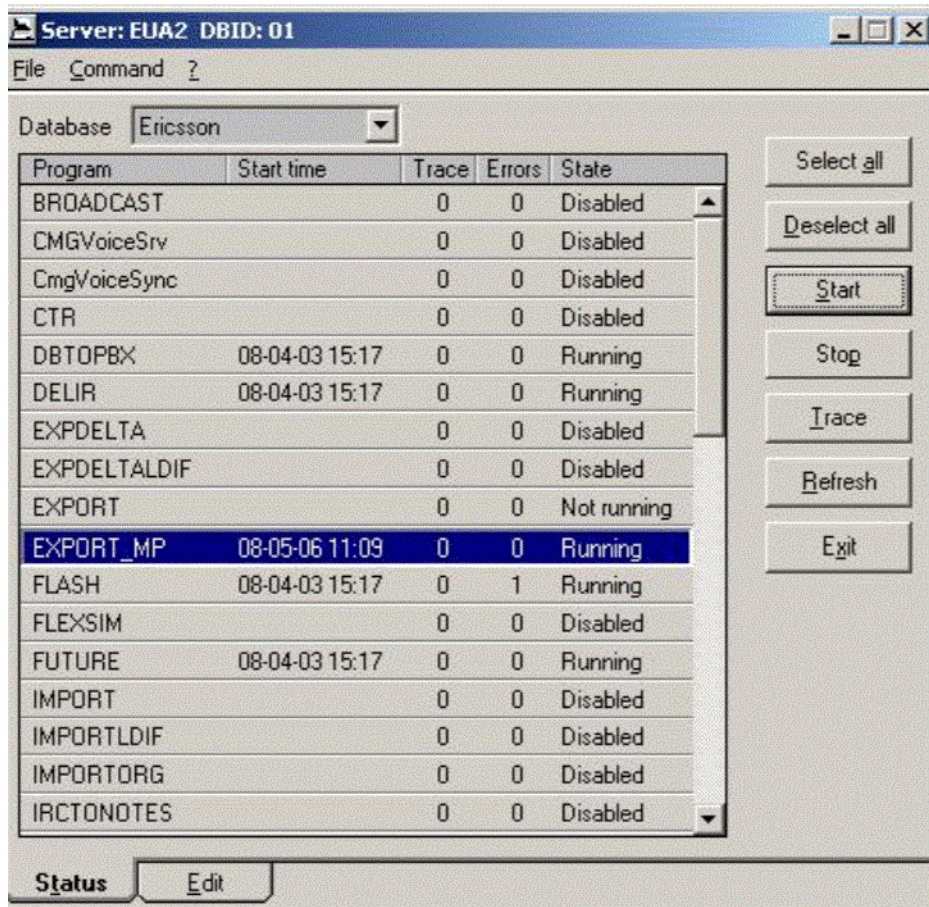
Group	Name	Value
Config	FileSpec	MPExport.txt

Buttons: Save, New, Delete, Previous, Next

Bottom tabs: Status, **Edit**

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

Figure 2: Status tab



5. 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.

11.3.5 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**.

11.3.6 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 subsystem 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.

11.3.7 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**.

11.3.8 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.
5. 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](#) on page 19.

Note:

See [Important Post-Migration Considerations](#) on page 21 on page 16 for important information on how to manage user data in environments including MX-ONE Provisioning Manager and CMG.

11.4 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 [Downloading and Installing the CMG Export Registry File on page 15](#)

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

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.

11.5 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*.

11.6 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*.

Figure 3: Post-Installation menu

```
lqqqqProvisioning Manager Post-Install Configurationqqqqqqk
x
x This utility is for performing individual tasks in      x
x Provisioning Manager.                                x
x
x You can use the UP/DOWN arrow keys to navigate and    x
x spacebar to select.                                  x
x
x Please choose your option!                             x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x      [ ] 01 Database check                          x x
x x      [ ] 02 Database backup                        x x
x x      [ ] 03 Database restore                      x x
x x      [ ] 04 Provisioning Manager Re-install       x x
x x      [ ] 05 Unlock user                          x x
x x      [ ] 06 Set user password                    x x
x x      [ ] 07 View user privileges                 x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq] x
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x      < OK >      < Exit >
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq]
```

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**.

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

```
sudo mp_uninstall
```

Log files are created automatically and can be found in directory `/var/log/mxone_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`

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

Increasing Heap Memory Size in Jboss Configuration File 16

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_MODULES_SYSTEM_PKGS -  
Djava.awt.headless=true"
```

```
JAVA_OPTS="$JAVA_OPTS -Djboss.modules.policy-permissions=true"
```

```
JAVA_OPTS="$JAVA_OPTS -Djboss.as.management.blocking.timeout=600"
```

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**.

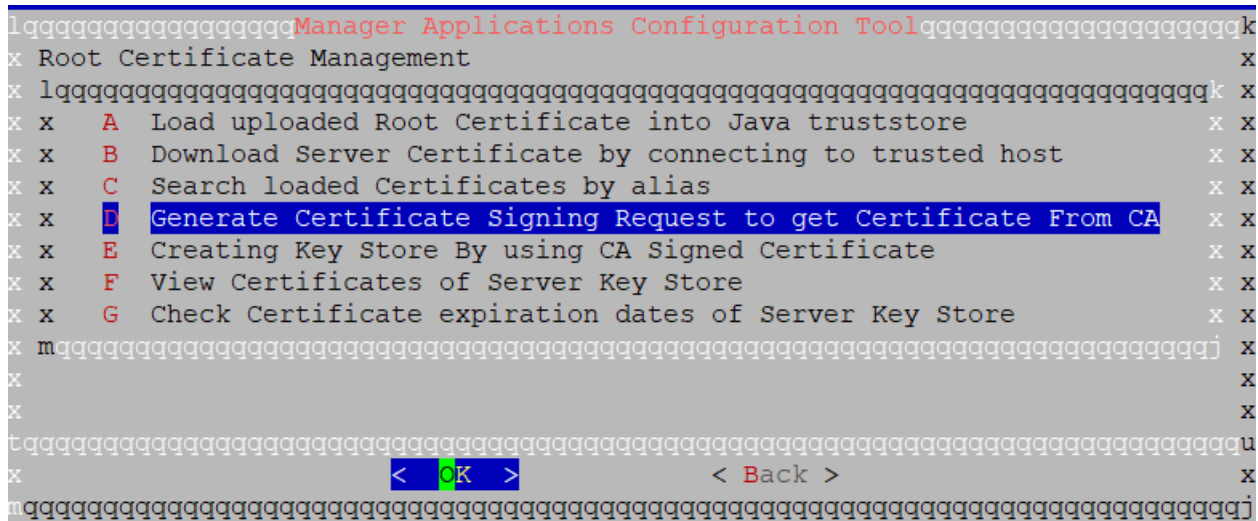
17

Using the `webserver config` command in `mxone_maintenance`, the user can generate a Certificate Signing Request (CSR) that can be used by Provisioning Manager and Service Node Manager.

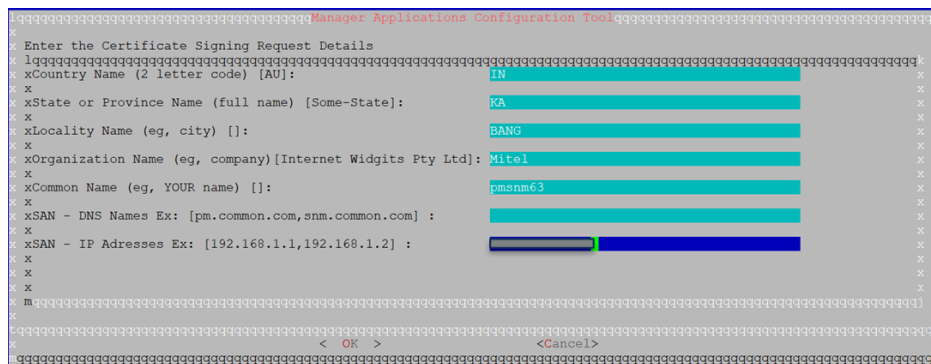
1. Enter the `webserver_config` command. The following screen appears.

9/1531-ANF 901 15 Uen L

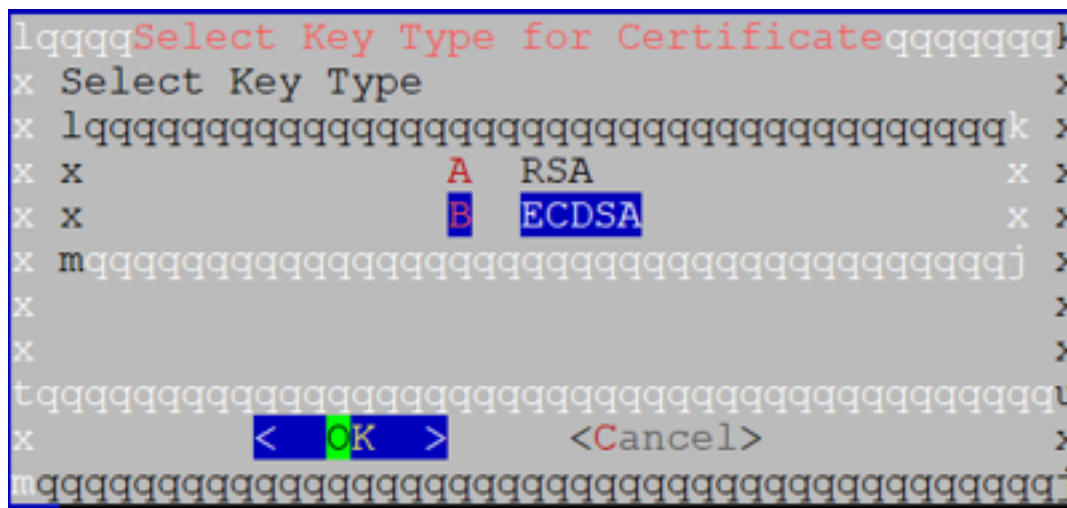
2. Select **Root certificate Management** and click **OK**. The following screen appears.



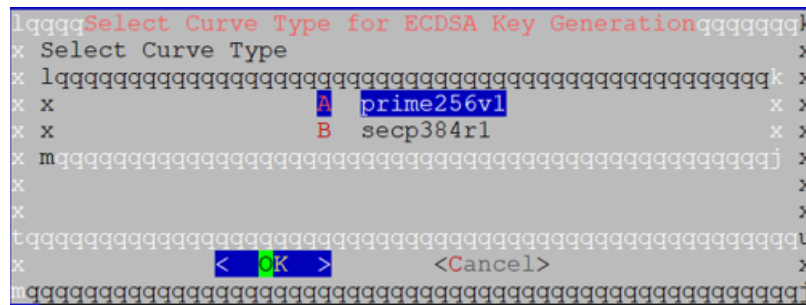
Select **Generate Certificate Signing Request to get Certificate From CA** and click **OK**. The following screen appears.



3. Enter the CSR details and click **OK**. The following screen appears.



4. Select **ECDSA** as key type and click **OK**. The following screen appears.



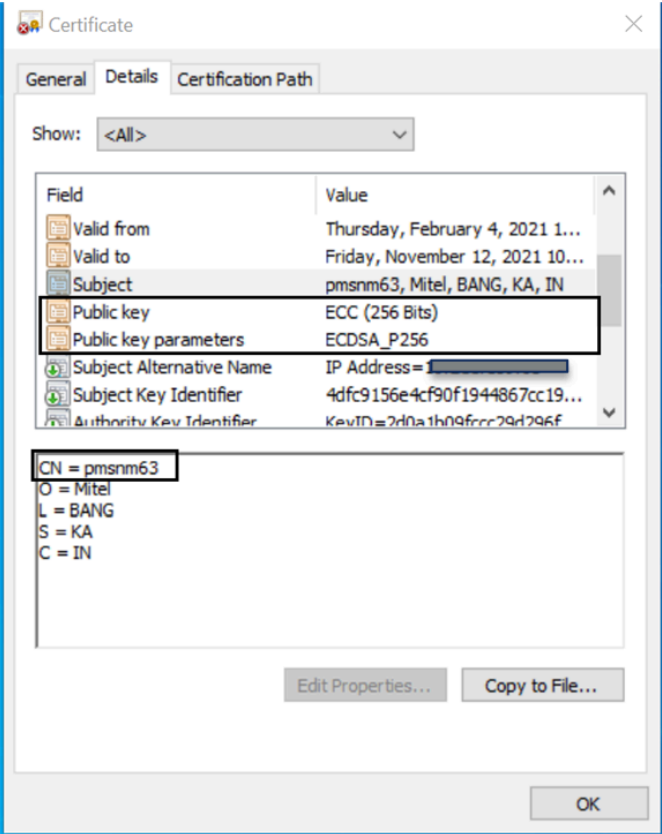
5. Select **Curve Type** (similar to selecting bit size in case of RSA). An ECDSA private key is generated.

Note:

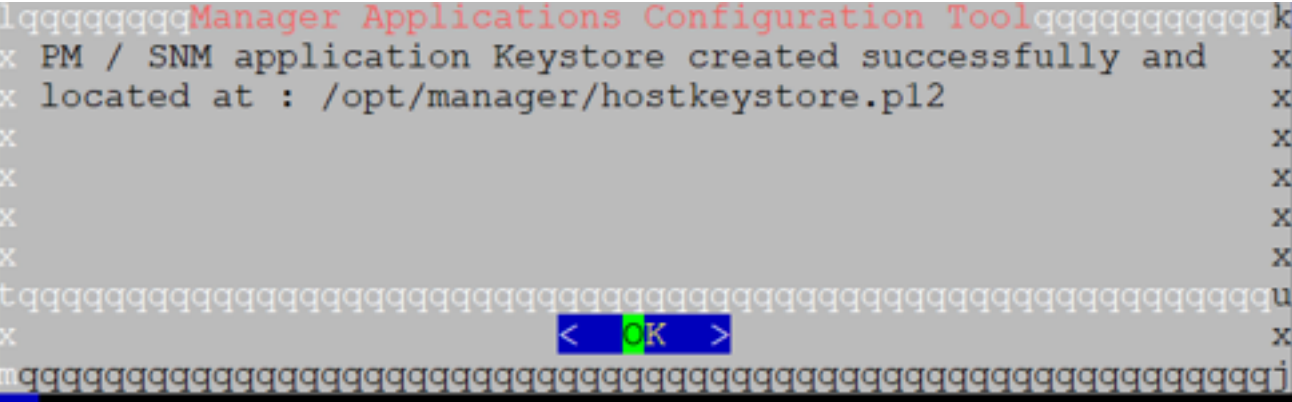
Private key and CSR files are generated in: /opt/manager/ directory

```
PHOENIX:/local/home/mxone_admin # cat /opt/manager/private.key
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEII0ozWHlad74iPyTlrHlvdGfSWKK4uCQ1AzcivduGbyPoAoGCCqGSM49
AwEHoUQDQgAERi4WQtUKjVDI83mxelT3WvFz8CYaZWehT+SsPwD8Ah8rNXdzfQ1H
0SWGos/Q7pt8XKSseHNF/+pEOFbnCHBB8A==
-----END EC PRIVATE KEY-----
PHOENIX:/local/home/mxone_admin #
```

6. Sign the CSR using CA.



7. Add the certificate to your system.



8. Click **OK**. The following screen appears.

[illegible]

9. The Change protocol to https and select a created keystore. Click **OK**. The following screen appears.

```

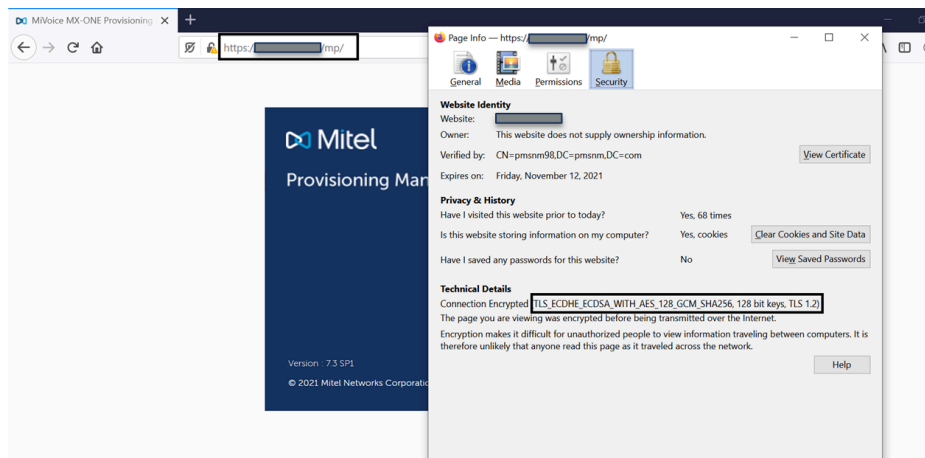
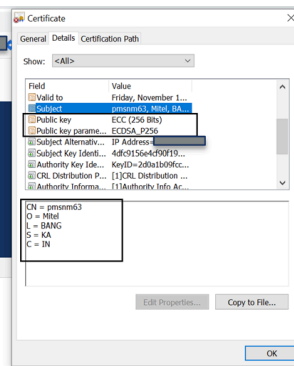
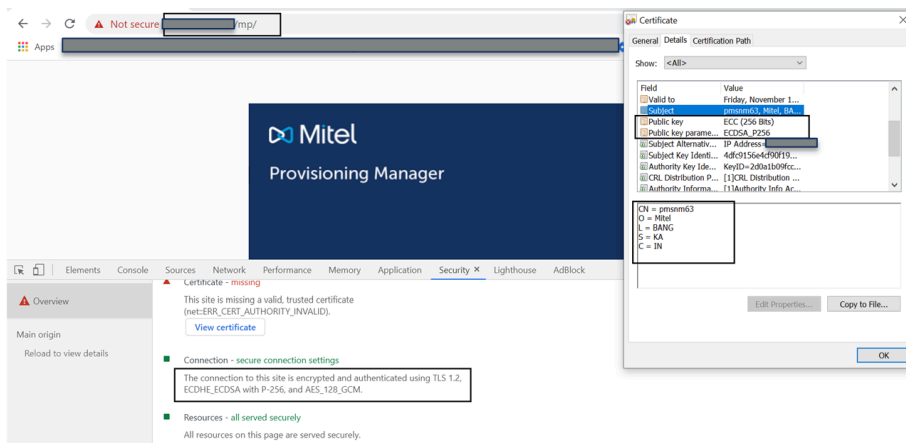
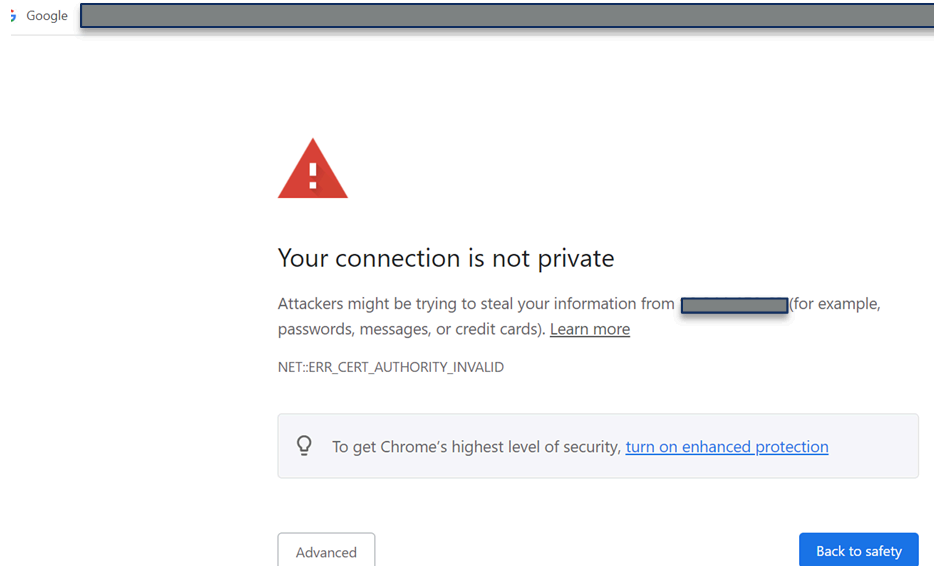
lqqqqSelect the type of TLS encryption qqqqqqqk
x Select the type of TLS encryption x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x A Standard x x
x x B High End Encryption x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x x
x x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq u
x < OK > <Cancel> x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj

```

10. Change the TLS version to 1.2 and Click **OK**.

[illegible]

11. Test the certificate in Chrome and Firefox browsers and check whether the cipher is used or not.



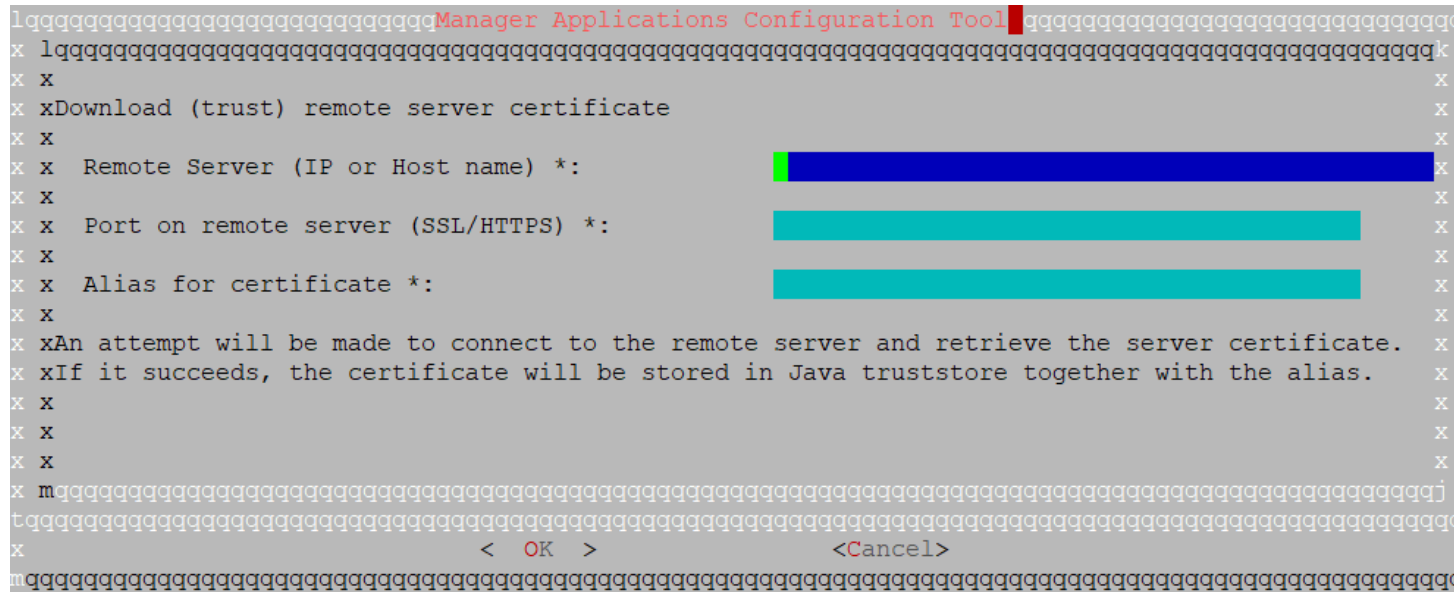
18

The following example shows how to download the certificate.

1. Enter the `webserver_config` command and select **Root certificate Management** and click **OK**. The following screen appears.

[illegible]

2. Select **Download server Certificate** by connecting to trusted host and click **OK**. The following screen appears.



3. Enter the third-party server details and click **OK**.
4. After the above steps are successful, restart jboss.

