

AD Authentication

DESCRIPTION



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 2016, Mitel Networks Corporation

All rights reserved

CONTENTS

1	INTRODUCTION	1
1.1	DESCRIPTION OF AD AUTHENTICATION	1
1.2	PRE-REQUISITES	1
1.3	SUPPORTED AD VERSIONS	2
2	SECURITY.....	3
2.1	SECURE SOCKET LAYER (SSL)	3
2.2	CERTIFICATES	3
2.2.1	SERVER CERTIFICATE	3
2.2.2	ROOT CERTIFICATE	3
2.3	GENERATING CERTIFICATE SIGNING REQUEST (CSR) AND CREATING KEYSTORE	3
2.3.1	CREATING CERTIFICATE BY SIGNING REQUEST FILE	4
2.3.2	CREATING THE KEY STORE BY USING SIGNED CERTIFICATE	5
2.4	STEPS TO GENERATE AND IMPORT CERTIFICATES FOR PM & SNM BY USING LOCAL WINDOWS SERVER AS CERTIFICATE AUTHORITY	9
3	USERS	11
4	CONFIGURATION	12
4.1	CONFIGURE WEB PROTOCOL	12
4.1.1	CONFIGURE WEB PROTOCOL FROM HTTP TO HTTPS WITH SELF-SIGNED CERTIFICATE	12
4.1.2	CONFIGURE WEB PROTOCOL FROM HTTP TO HTTPS WITH UPLOADED SERVER CERTIFICATE	12
4.1.3	TURNING SSL OFF AND BACK ON AGAIN	13
4.2	CONFIGURE SNM AUTHENTICATION METHOD	13
4.3	CERTIFICATE MANAGEMENT FOR AD AUTHENTICATION	14
4.3.1	ROOT CERTIFICATE OR SIGNED SERVER CERTIFICATE	14
4.3.2	ALTERNATIVE TO ROOT CERTIFICATES IN E.G. LAB ENVIRONMENT	14
4.3.3	SEARCH AND DELETE ROOT CERTIFICATES	14
4.4	CONFIGURE AD AUTHENTICATION	15
5	AD AUTHENTICATION MAINTENANCE.....	17
5.1	MODIFYING AD AUTHENTICATION CONFIGURATION	17
5.2	TURNING AD AUTHENTICATION OFF	17
5.3	TURNING AD AUTHENTICATION BACK ON	17
6	AD AUTHENTICATION SCENARIOS.....	18
6.1	SCENARIO 1: PM LOGIN	19
6.2	SCENARIO 2: SNM LOGIN	19
6.3	SCENARIO 3: SNM LOGIN OVER HTTP	20
6.4	SCENARIO 4: PM LOGIN + USE CASE 'ADD EXTENSION'	20
6.5	SCENARIO 5: IN PM "CLICK ON SUBSYSTEM"	21
7	FAULT CASES / EXCEPTIONS	22

1 INTRODUCTION

1.1 DESCRIPTION OF AD AUTHENTICATION

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

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

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

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

1.2 PRE-REQUISITES

- The authentication towards AD is performed over protocol LDAPS. The AD server must therefore be enabled for LDAPS.
- AD authentication is implemented with LDAP authentication method ‘Simple authentication’ (see: <http://msdn.microsoft.com/en-us/library/cc223499.aspx>). As this requires that the user password is sent in clear text, AD authentication is only allowed when the entire web server PM is running on is configured for SSL (HTTPS).
- The AD server must be configured for SSL on the LDAP(S) interface.
- An SNM defined as subsystem for PM configured for AD authentication will also use the AD authentication feature when it is configured for PM authentication method (i.e. not “Linux”). See further in Scenario 2: SNM Login
- Subsystems configured with PM authentication method must also be configured for SSL.
- Subsystems not configured for SSL must use Linux authentication method. I.e. all users that need access must be provided with an own Linux account. Note that this is a high security risk if users get used to log in with AD credentials. See further in Scenario 3: SNM Login over HTTP.
- Auto-login in SNM is disabled upon the action “click on subsystem” in PM. Instead the user needs to be authenticated again, but as long as the SNM server is configured for SSL and PM authentication method, the same user name and password as for the domain (and PM login) will be used.
- All users that should be able to log in to PM and SNM must still be defined as users in the PM database. However, the password associated with each user is not in use as long as AD authentication is enabled.
- The user name or alias used when logging in to PM or SNM with AD authentication must match the one defined and stored in the PM database. This must be considered if the feature “Principal DNS Suffix” is used.

Example:

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

The “Principal DNS Suffix” is configured as **mydomain.com**.

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

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

See further chapter: [Configure AD authentication](#).

1.3 SUPPORTED AD VERSIONS

Windows Server 2008 R2 (64 bit)

Windows Server 2012 (64 bit)

2 SECURITY

2.1 SECURE SOCKET LAYER (SSL)

The server, on which PM is installed, needs to be configured for SSL (HTTPS). End users will be using HTTPS when accessing the application web page. The same applies for web services between PM and SNM. Also the AD communication with LDAP shall be encrypted over SSL.

To configure SSL/HTTPS, use command **webserver_config**. See further chapter [Configuration](#).

2.2 CERTIFICATES

The use of certificates is all about trust. We need to be able to trust the other party we connect to and communicate with. Due to this we will need two different kinds of certificates when running AD authentication: one as a server (Server Certificate) to be able to run the web application over HTTPS, and another one (Root Certificate) as a client when we connect to the AD server.

2.2.1 SERVER CERTIFICATE

The server certificate is used for the purpose of other (clients) to trust the PM when connecting over HTTPS. This could either be a self-signed certificate or a certificate signed by a Certificate Authority (CA). See further chapter [Configure web protocol](#).

2.2.2 ROOT CERTIFICATE

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

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

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

However, in a more complex environment it is more common that the AD connection is made through a broadcast via the domain controller or by addressing a sub domain or even the entire domain. In those cases it would be inconvenient to store the server certificates for all possible transfer servers the connection will need to verify as trustworthy. Instead a proper root certificate that can verify the signature on each server's server certificate should be imported. See further chapter [Certificate management for AD authentication](#).

2.3 GENERATING CERTIFICATE SIGNING REQUEST (CSR) AND CREATING KEYSTORE

This section explains how to use the *webserver_config* utility to generate the Certificate Signing Request (CSR).

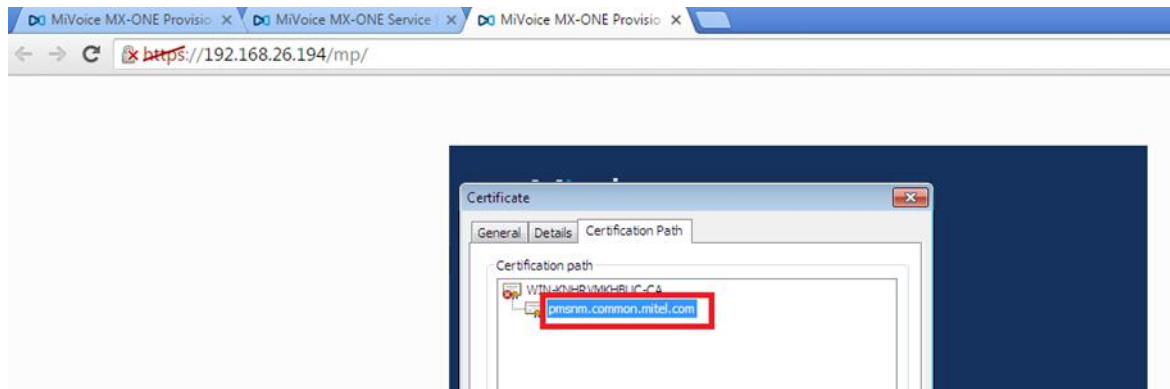
Once you receive the Signed Certificate from the Certificate Authority, the section also describes how to create the Keystore.

```
Manager Applications Configuration Tool
Configure web server
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
x A Configure web protocol to http or https.
x B Set SNM to authenticate to PM or Linux
x C Configure AD authentication
x D Root Certificate Management
x E Check Configuration
x F Collect Diagnosis
x G Re-start webservice (Applications PM, SNM and CSTA)
x H Change TLS Level for HTTPS
m

< OK >      < Exit >
```

[illegible][illegible]

1



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

SAN – DNS Names: Subject Alternate DNS Names

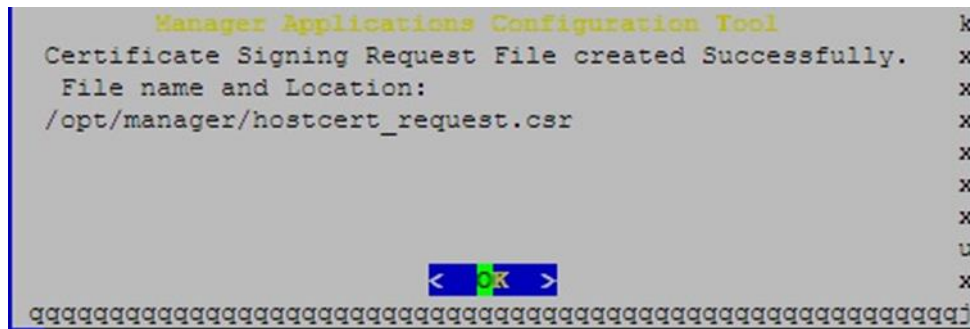
Ex: pm.common.com, snm.common.com

SAN – IP Addresses: Subject Alternate IP Addresses

Ex: 192.168.2.1, 192.168.2.3

Once you have filled the form click “OK”. The system will generate the Certificate Signing Request (CSR) File and locate it at “/opt/manager/hostcert_request.csr”.

You have to copy this file to the local system and share it with Certificate Authority (CA) for them to provide the Signed Certificate.



2.3.2 CREATING THE KEY STORE BY USING SIGNED CERTIFICATE

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

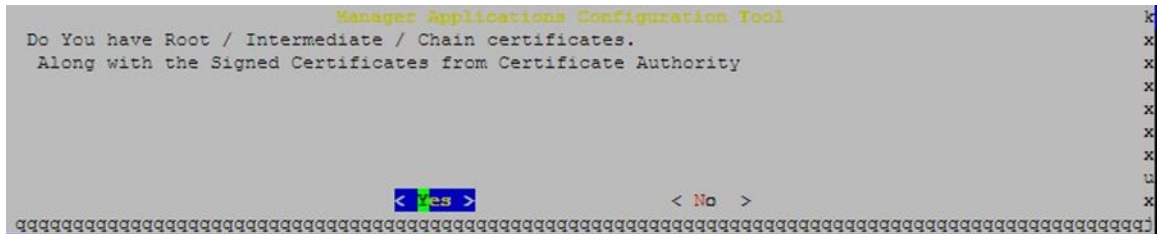
Open **webserver_config** utility.

Then select option “E” – Creating Key Store By using CA Signed Certificate

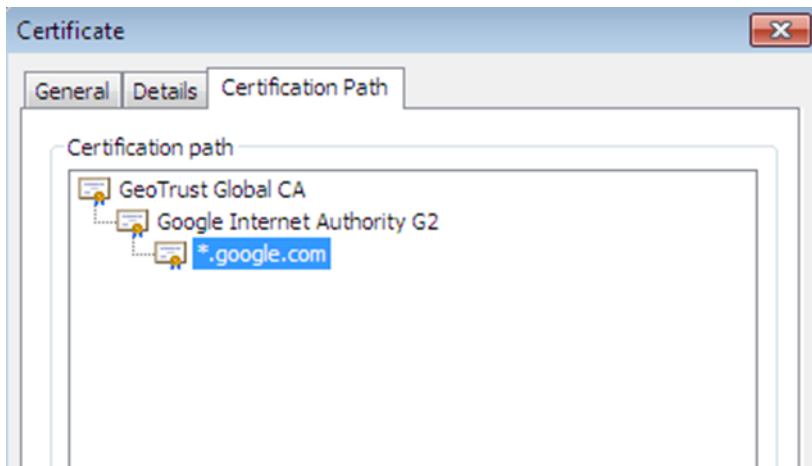


TAB – To move between Directories, Files and Buttons sections

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



What are Root / Intermediate / Chain Certificates?



When you open the certificate like above, here “GeoTrust Global CA” is a Root Certificate, “Google Internet Authority G2” is Chain / Intermediate Certificate, “*.google.com” is a Signed Certificate.

These Root and Signed Certificates will be provided by the Certificate Authority or can be downloaded from their sites.

If there is only Root Certificate, you can use that file directly and ignore the below section otherwise merge all these Root and Chain Certificates into one file.

When you open these Root / Chain Certificates in the notepad, the content may look like below.

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

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

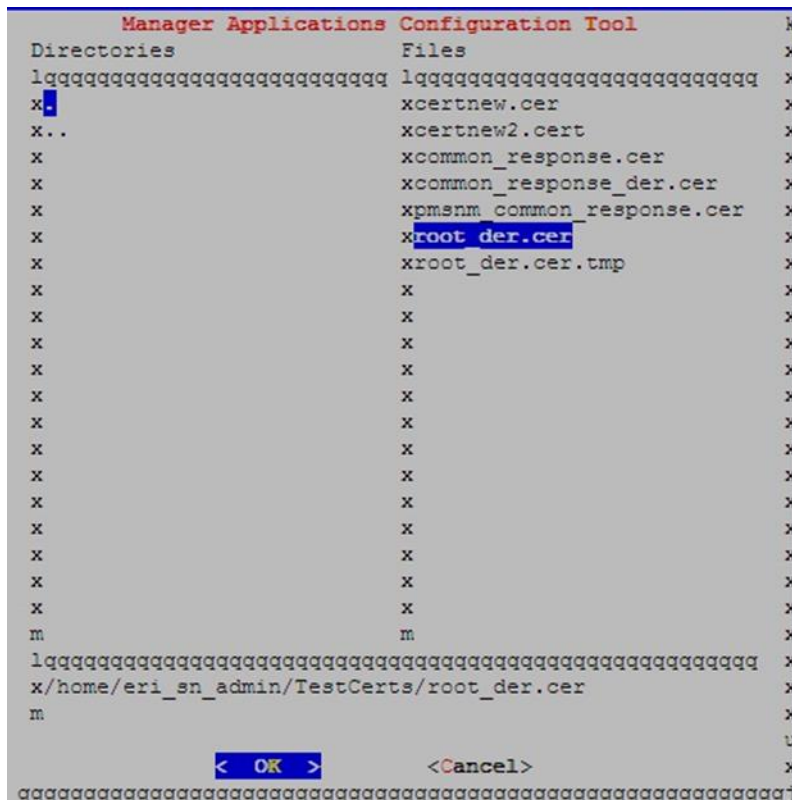
```
-----BEGIN CERTIFICATE-----
Root Certificate Information
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Chain Certificate Information
-----END CERTIFICATE-----
```

Then select the Root / Chain Certificate file

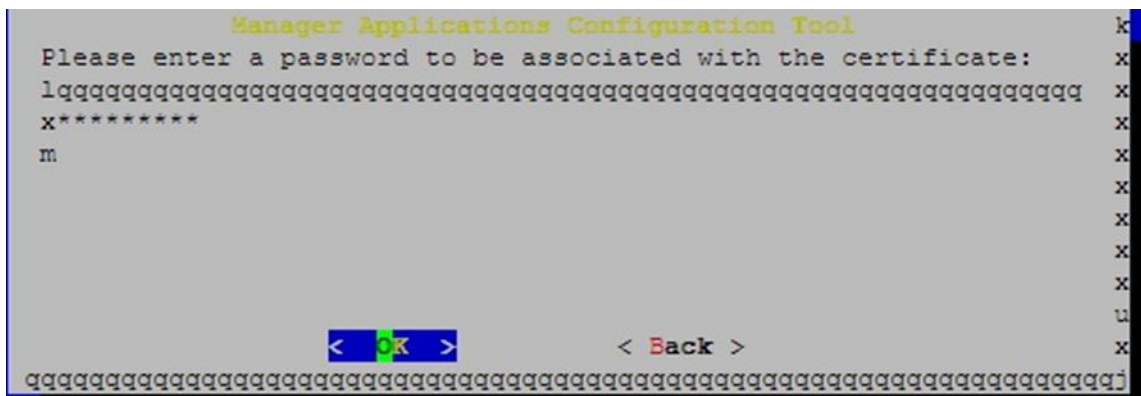
Instructions:

TAB – To move between Directories, Files and Buttons sections

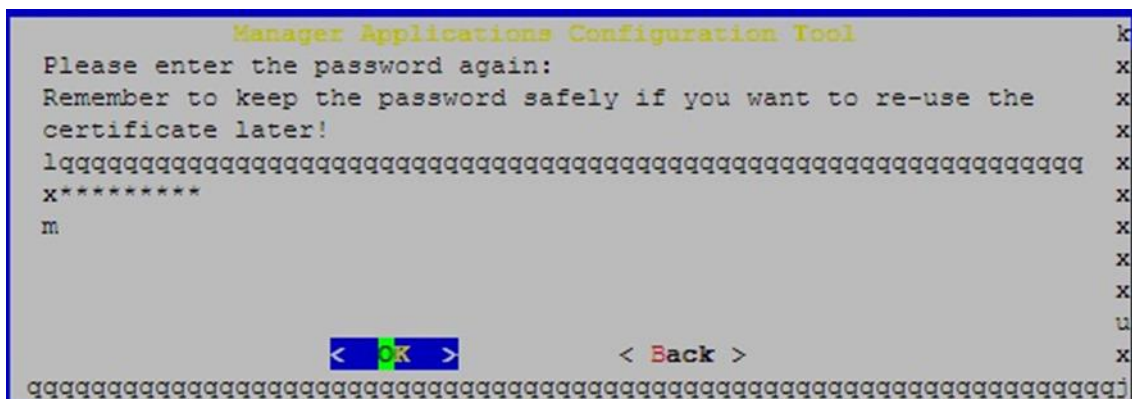
Space – Select **the Directory** / Files



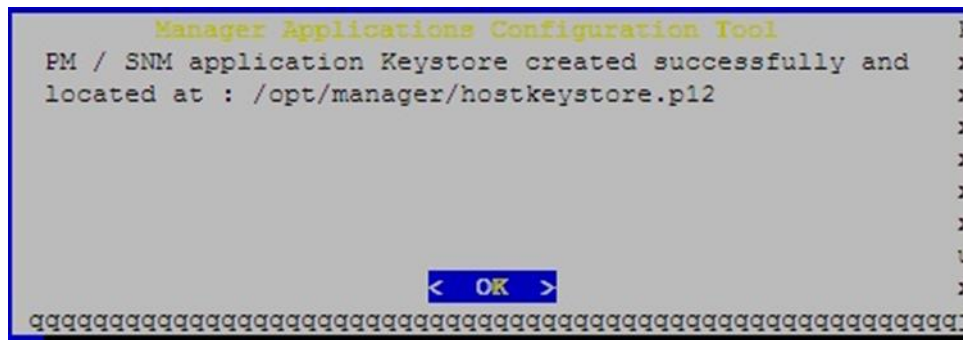
Then enter the password to create the Key Store



Re-Enter the same password for Validation



Then System creates the Key Store File and locates at “/opt/manager/hostkeystore.p12”



You can use this file and enable the HTTPS.

Webserver_config → Configure web protocol to enable HTTP or HTTPS → Change to HTTPS / Keep HTTPS → Certificate is uploaded to file System → select the created Key Store file from “/opt/manager/hostkeystore.p12”.

2.4 STEPS TO GENERATE AND IMPORT CERTIFICATES FOR PM & SNM BY USING LOCAL WINDOWS SERVER AS CERTIFICATE AUTHORITY

Do as follows:

1. Generate certificate requests by using IIS for PM and SNM.
2. Upload the certificate request to “certsrv” application.
3. Issue the certificates by using MMC .
4. Download the Issued certificates from “certsrv” application.
5. Complete the certificate request by using IIS.
6. Generate the PFX files for PM and SNM with private key to use as a keystore.
7. Follow below steps to enable SSL for PM and SNM applications.
 - a. Open Webserver_config utility
 - b. Select “Configure web protocol to HTTPS”
 - c. Select “Change to HTTPS”
 - d. Select “ Certificate is uploaded to file system”
 - e. Select the “.PFX” file which was generated in Step 6.
8. Follow below steps to exchange the certificates between PM, SNM, AD and CMG
 - a. Open Webserver_config utility
 - b. Select “Root Certificate Management”
 - c. Select “Load Upload Root Certificate into Java truststore”.
 - d. Select the certificate of other system, Provide the alias name.

Ex : If we are executing above steps in PM, then we have to select the certificate of SNM. Which we have downloaded from Step 4

In case if the Other system is AD or CMG, then have to get the AD or CMG certificates from AD or CMG servers by using MMC tool.

Importing the certificate of PM/SNM, AD and or CMG is applicable for Co-Existing system (PM/SNM are in same server) also.

We can import the certificate by connecting to other system directly by selecting “webservice_config” -> Root Certificate Management -> Download Certificate by connecting to trusted host -> Enter the Other Server Name / IP, Port and alias names.

9. At AD or CMG side, have to import the server Certificate of PM by using MMC tool to the “trusted people” section.
10. Import the Root Certificate of PM to AD or CMG by using MMC tool to “trusted Certificate Authority” Section.



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

3 USERS

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

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

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

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

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

4 CONFIGURATION

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

All necessary configuration scripts are available through the command **webserver_config**.

4.1 CONFIGURE WEB PROTOCOL

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

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

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

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

4.1.1 CONFIGURE WEB PROTOCOL FROM HTTP TO HTTPS WITH SELF-SIGNED CERTIFICATE

Do as follows:

1. As root, or with sudo privileges, run command **webserver_config**.
2. Select **Configure web protocol to http or https**.
3. Select **[CHANGE TO/KEEP] HTTPS**.
4. Confirm the next two windows by pressing the Type key.
5. Select **Create a self-signed certificate**.
6. Type the password to be associated with the certificate (This is needed in case the certificate shall be re-used later on).
7. Re-type the password.
8. Accept a restart of the web server. The configuration will not take effect before a restart of the web server is done.

4.1.2 CONFIGURE WEB PROTOCOL FROM HTTP TO HTTPS WITH UPLOADED SERVER CERTIFICATE

Do as follows:

11. As root, or with sudo privileges, run command **webserver_config**.
12. Select **Configure web protocol to http or https**.
13. Select **[CHANGE TO/KEEP] HTTPS**.
14. Confirm the next two dialogs by pressing the Type key.
15. Select **Certificate is uploaded to file system**.

16. Use the **Up/Down key**, and **Enter** on the keyboard, to navigate to your certificate file, mark it and press **Enter**.
17. Accept that it is the correct file to be used.
18. Provide the password associated with the certificate.



Note! If an incorrect password is used, the certificate will not function.

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

4.1.3 TURNING SSL OFF AND BACK ON AGAIN

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

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

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

4.2 CONFIGURE SNM AUTHENTICATION METHOD

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

For Linux authentication it is required that the user has a Linux account. This is to be created according to standard Linux procedures via command or using `mxone_maintenance` utility. Log-in as user `mxone_admin`, and key the command `sudo -H /opt/mxone_install/bin/mxone_maintenance` and select option user and follow the instructions on screen.

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



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

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

To set PM authentication method when PM is running on a standalone server, log in to the SNM server.

Do as follows:

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

4.3 CERTIFICATE MANAGEMENT FOR AD AUTHENTICATION

4.3.1 ROOT CERTIFICATE OR SIGNED SERVER CERTIFICATE

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

Do as follows:

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

4.3.2 ALTERNATIVE TO ROOT CERTIFICATES IN E.G. LAB ENVIRONMENT

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

Do as follows:

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

4.3.3 SEARCH AND DELETE ROOT CERTIFICATES

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

To search Java trust store and optionally delete a certificate.

Do as follows:

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

4.4 CONFIGURE AD AUTHENTICATION

The following must be considered before AD authentication is configured:

- How shall the AD server be addressed:
 - IP address
 - Host name
 - Domain name
- Which port number is applicable for LDAPS on the AD server (default is 636)
- Is there a need to define the Base Context DN (Distinguished Name) for AD? This is equal to defining in which part of the AD the user shall be sought. Example:
 CN=Users,DC=mysubdomain,DC=mydomain,DC=org
 To search the entire AD, leave the field blank.
 Please note that the Base Context DN must have a perfect match, and it cannot be verified by any means by the PM configuration tool.
- How the user credentials shall be typed:
 - a useralias only
 - useralias@domain (also commonly known as User-Principal-Name)

If all users that should be able to log in to PM are using the same domain when being authorized in AD, it is possible to assign the domain name as a “Principal DN suffix in the AD authentication configuration. For example:

- All users belong to the same domain, *ourdomain.com*.
- The AD server uses User-Principal-Name when authorizing users, i.e. by default the user e-mail address, e.g. jdoe@ourdomain.com.
- In the AD authentication configuration, define the Principal DN suffix as *ourdomain.com*.
- The users will now use the alias only, e.g. *jdoe* when logging in to PM.



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

- To disable suffixing, just leave the field for attribute **Principal DN suffix** empty.
- Do never Type the character **@**. It will automatically be appended.

Do as follows:

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

Please note that if the server not is configured for SSL/HTTPS, the AD configuration wizard will be interrupted.

5 AD AUTHENTICATION MAINTENANCE

5.1 MODIFYING AD AUTHENTICATION CONFIGURATION

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

Do as follows:

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

5.2 TURNING AD AUTHENTICATION OFF

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

Do as follows:

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

5.3 TURNING AD AUTHENTICATION BACK ON

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

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

6 AD AUTHENTICATION SCENARIOS

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

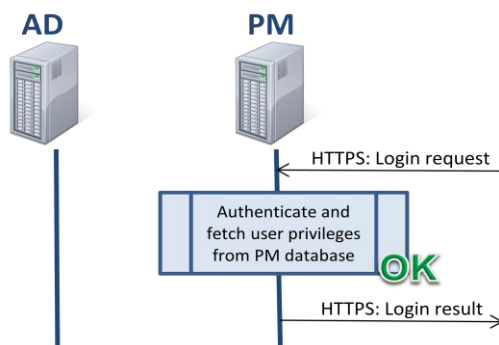
For each login attempt it is checked whether the user is:

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

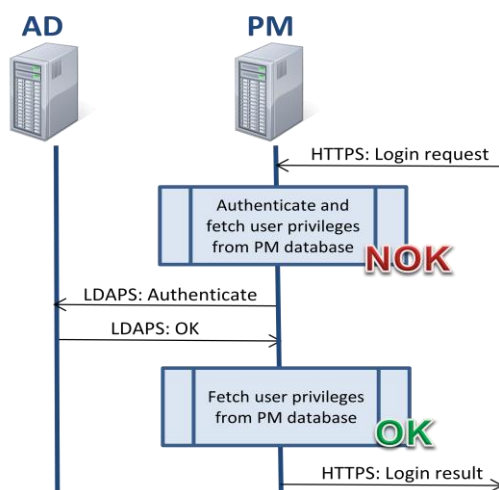
At each login attempt it is first checked if the user can be authenticated in the PM user database. If not, an AD authentication attempt is made and if this is successful the user is authorized from PM user database.

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

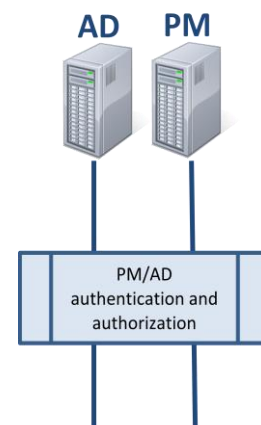
User authenticated and authorized in PM user database:



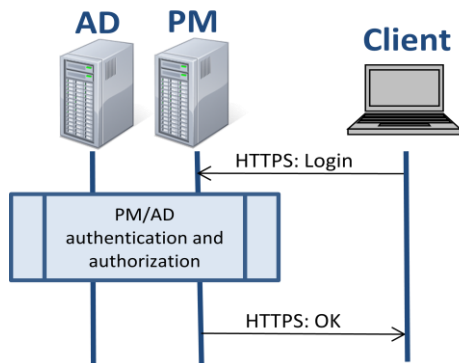
User authenticated in AD and authorized in PM user database:



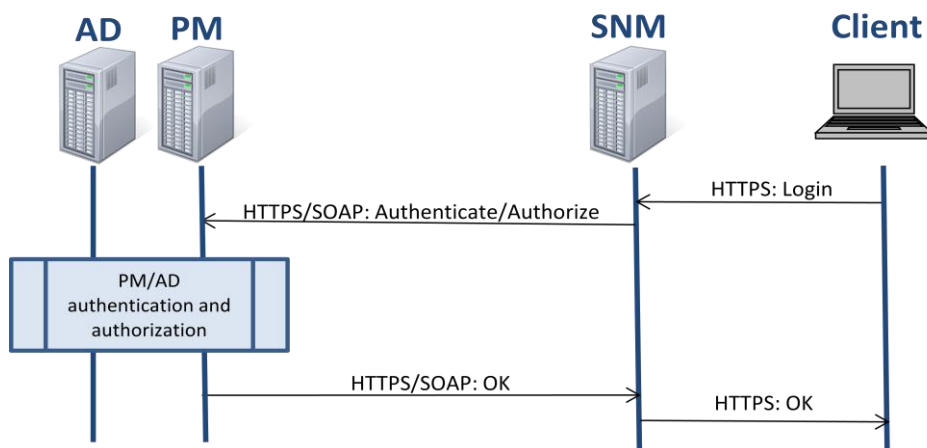
The examples above are in the following scenarios referred to as:



6.1 SCENARIO 1: PM LOGIN



6.2 SCENARIO 2: SNM LOGIN



6.3 SCENARIO 3: SNM LOGIN OVER HTTP

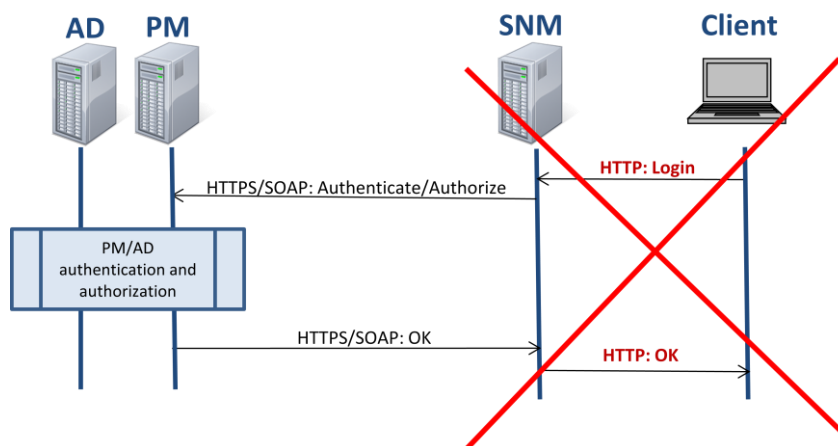


Warning! This scenario shall be avoided!

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

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

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



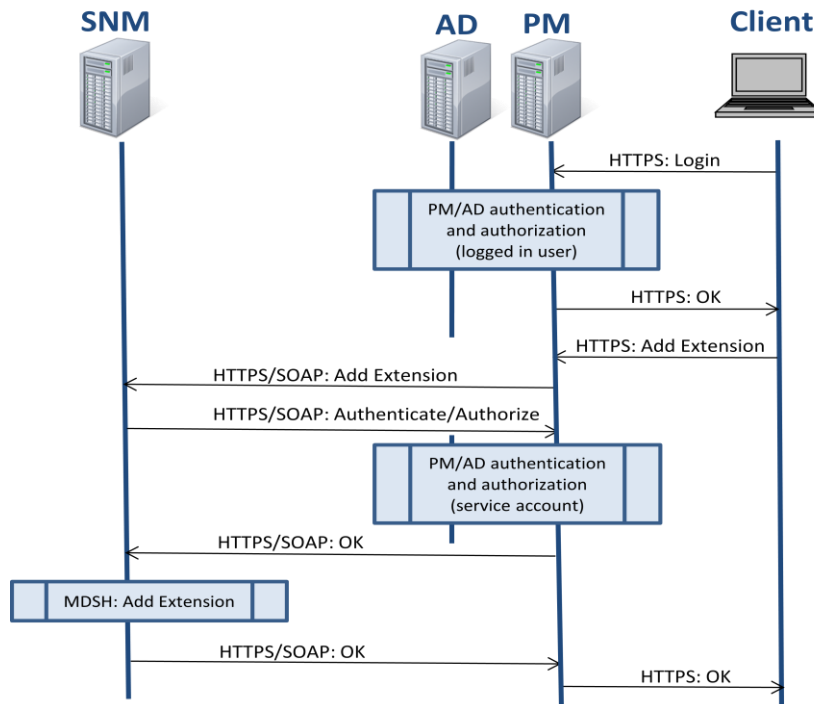
6.4 SCENARIO 4: PM LOGIN + USE CASE 'ADD EXTENSION'

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

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

Note (1): Despite that the "service account" is configured with privileges on a high level, it will not enable any extra features for the logged in PM user.

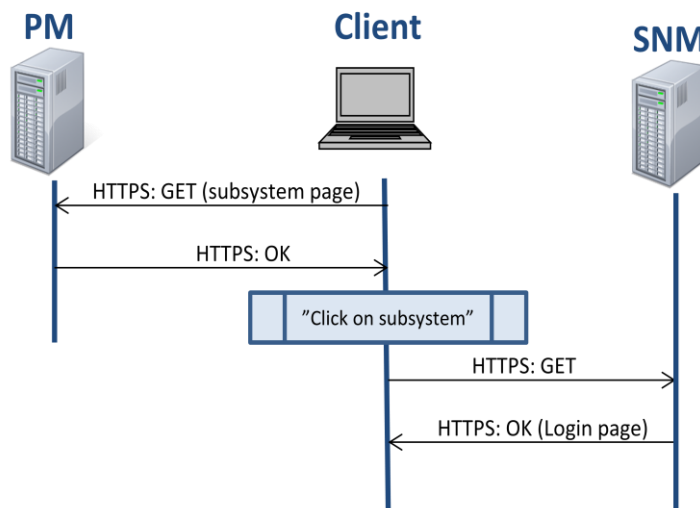
Note (2): It is recommended that the "service account" is created for PM authentication only, and not as an AD user account. Implicit actions in the PM application that require use of the subsystem "service account" will render a lot of authentication requests. It is therefore more efficient to avoid AD authentication.



6.5 SCENARIO 5: IN PM “CLICK ON SUBSYSTEM”

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

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



7 FAULT CASES / EXCEPTIONS

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