

MTAS Configuration for Provisioning LDAP MTAS

USER GUIDE

Copyright

© Ericsson AB 2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Overview	3
3	Configuration of Provisioning LDAP Server	5
3.1	Procedure	5
4	Connect to the Provisioning LDAP Server	9
5	Provisioning MTAS MOs	11
6	Configuration Parameters of LDAP Server	13
6.1	Configuration Parameters for MTAS	13
6.2	Procedure	14
7	Access Control	17
7.1	LDAP ACL	17





1 Introduction

This document describes the Lightweight Directory Access Protocol (LDAP) interface of MTAS. It describes the procedure to Instantiate the Provisioning LDAP Server for MTAS, connecting LDAP Server over the COM NBI, Provisioning MTAS Managed Objects (MOs), Configuration Parameter for MTAS and Access Control.

1.1 Prerequisites

This section describes the prerequisites, which must be fulfilled before performing the procedure. It is assumed that the user of this document is familiar with the Operation and Maintenance (O&M) area, in general.

1.1.1 Documents

Before starting any procedure in this document, ensure that the following documents are available:

- *Certificate Management*
- *Ericsson Command-Line Interface User Guide*
- *Managed Object Model (MOM)*
- *MTAS Hardening Guide*
- *vDicos Provisioning LDAP Interface Description*

1.1.2 Conditions

The following conditions must apply:

- The user has the System Security Administrator role.
- An Ericsson Common Command-Line Interface (ECLI) session in Exec mode is in progress.





2 Overview

Configuration data is to be accessed and manipulated through the COM NBLs and provisioning data is to be accessed and manipulated through the provisioning LDAP interface.

MTAS uses a Provisioning LDAP Interface that allows the user to interact with the MTAS by adding, changing, deleting, and searching of certain provisioning data according to the logic of the MTAS.

Provisioning data of MTAS are arranged in a containment hierarchy of MOs. This interface provides standardized access to these data, including filtered search, creation, deletion, and modification of MOs.

Provisioning LDAP Interface can be used for provisioning purposes only. Both “ldap://...” and “ldaps://...” are supported (on different TCP ports), but the TLS must be used with the non-secure “ldap://” case, otherwise the LDAP server refuses the connection request.





3 Configuration of Provisioning LDAP Server

By default, the provisioning LDAP interface is not available for external clients. The provisioning LDAP server can be configured through the Ericsson Common Information Model (ECIM) over the COM NBIs at the following DN:

```
>dn ManagedElement=1,MtasFunction.applicationName=MtasFunction,
MtasSupportFunctions=0,ProvisioningM.applicationName=provisioning,
ProvisioningServer=provisioning
```

The following attributes are available:

- `port`: the port number over which the LDAP server listens (read only)
- `sslPort`: the Secure Socket Layer (SSL) port number over which the LDAP server listens (read only)
- `dnSuffix`: the DN suffix for the provisioning LDAP server (read only)
- `accessControlList`: the LDAP Access Control List (ACL) for the provisioning server
- `nodeCredential`: MO reference to a valid `NodeCredential` instance configured in the `CertM` fragment. The server is not reachable until this attribute is set.
- `trustCategory`: MO reference to a valid `TrustCategory` instance configured in the `CertM` fragment

3.1 Procedure

This section describes the procedure to instantiate Provisioning LDAP server.

3.1.1 Install or Renew Node Credential

For installation or renewal of `NodeCredential` in the `CertM` fragment, refer to *Certificate Management*.

This section demonstrates how to install or renew a node credential directly from a PKCS#12 file containing both a private key and a certificate. It is assumed the valid PKCS#12 file is present in the host.

To install or renew a node credential:

1. Navigate to the `CertM` MO, for example:

```
>dn ManagedElement=1,SystemFunctions=1,SecM=1,CertM=1
```



2. Select the appropriate action:

- Installation, proceed to Step 3.
- Renewal, proceed to Step 6.

3. Enter Config mode:

```
(CertM=1) >configure
```

4. Select the existing `NodeCredential` MO if it is present and proceed to Step 7, else create a `NodeCredential` MO:

```
(config-CertM=1) >NodeCredential=provLdap
```

5. Commit the change:

```
(config-NodeCredential=1) >commit
```

6. Select the existing `NodeCredential` MO to which the PKCS#12 container file is to be installed:

```
(CertM=1) >NodeCredential= provLdap
```

7. This step assumes that the PKCS#12 file is encrypted with password `c_pw`.

Install the certificate:

```
(NodeCredential= provLdap) >installCredentialFromUri  
--uri  
sftp://hostuser1@host1/home/hostuser1/node06stNodeCred  
ential1.p12 --uriPassword  
hostuser1pw --credentialPassword c_pw --fingerprint  
ba:41:ac:4f:b3:00:10:98:28:47:36:b1:eb:d9:66:33:69:05  
:7d:c2
```

The system returns true or false. If false, go to Step 8.

8. Verify that the certificate installation has been completed successfully:

```
(config-NodeCredential=1) >show enrollmentProgress  
result=SUCCESS  
resultInfo="installed from the container file"
```

If an error occurs during the execution of the action, attribute `enrollmentProgress` shows `result=FAILURE` and `resultInfo` shows the cause of the failure.

3.1.2 Instantiate the Provisioning LDAP Server

To instantiate the Provisioning LDAP server, the `nodeCredential` MO of `ProvisioningServer` must refer to a valid `NodeCredential` instance configured in the `CertM` fragment.



To instantiate the Provisioning LDAP server:

1. Navigate to the `ProvisioningServer=provisioning` MO, for example:

```
>dn  
ManagedElement=1,MtasFunction.applicationName=MtasFunction,MtasSupportFunctions=0,ProvisioningM.applicationName=provisioning,ProvisioningServer=provisioning
```

2. Enter Config mode:

```
(ProvisioningServer=provisioning)>configure
```

3. Refer to a valid `NodeCredential` instance configured in the `CertM` fragment:

```
(config-ProvisioningServer=provisioning)>  
nodeCredential=ManagedElement=1,SystemFunctions=1,SecM=1,CertM=1,NodeCredential=provldap
```

4. Commit the change:

```
(config-ProvisioningServer=provisioning)>commit
```

5. Verify that the Provisioning LDAP server is instantiated, see Section 4 on page 9.





4 Connect to the Provisioning LDAP Server

The provisioning LDAP server offers the following connection methods:

1. Secure connection

The connection is established over SSL. SASL PLAIN authentication is used.

Example:

```
ldapsearch -H ldaps://<vip_address>:<ssl-port>  
-b "<base_dn>" -Y plain -O none -U <username> -w  
<password>
```

Note: The server refuses authentication using BIND (-D option).

2. Non-secure connection with Transport Layer Security (TLS)

Although the channel itself is not encrypted, the security is still guaranteed as the server requires that the transport must be done using TLS.

Example:

```
ldapsearch -H ldap://<vip_address>:<port>-b "<base_dn>"  
-Y plain -O none -Z -U <username> -w <password>
```

Note: The server refuses authentication using BIND (-D option).





5 Provisioning MTAS MOs

Parameter Description for Provisioning MTAS MOCs document describes the Managed Object Model (MOM) of the MTAS regarding provisioning MOs. Provisioning-related MOs are not accessible through the COM NBI, so Provisioning LDAP must be used for CM instead. Example in this section demonstrates how to use it.

Example 1: Configure the Dialed Number Mapping (DNM) Administrative State using Provisioning LDAP

The DNM service is enabled by setting the `mtasDnmAdministrativeState` attribute in the `MtasDnm` MO to 1 (Unlocked). If the `mtasDnmAdministrativeState` is set to 0 (Locked), no DNM service is provided by the MTAS.

1. Prepare the `DNM_Example1.ldif`:

```
dn: MtasDnm=0,MtasMmt=0,MtasServices=0,applicationName=
MtasFunction,nodeName=jambala
changetype: modify
replace:mtasDnmAdministrativeState
mtasDnmAdministrativeState: 1
```

2. Perform the LDAP modification operation:

```
ldapmodify -H ldaps://<vip_address>:<ssl_port> -Y plain
-U <username> -w <password> -O none -f DNM_Example1.ldif
```

3. Verify the changes:

```
ldapsearch -H ldaps://<vip_address>:<ssl_port>
-Y plain -U <username> -w <password> -O none -b
"MtasDnm=0,MtasMmt=0,MtasServices=0,applicationName=Mta
sFunction,nodeName=jambala"
```

Example 2: Add the `MtasCommonDataAccNetwTypeAccInfo` using Provisioning LDAP

The `MtasCommonDataAccNetwTypeAccInfo` defines the mobile cells present in the network. It represents the Access Info based on P-Access-Network-Info (PANI) header format.

1. Prepare the `DNM_Example2.ldif`:

```
dn: MtasCommonDataAccNetwType=3GPP-E-UTRAN-FDD,MtasCom
monData=0,applicationName=MtasFunction,nodeName=nodeN
ame=jambala
changetype: add
objectClass: MtasCommonDataAccNetwType
```



```
MtasCommonDataAccNetwType:3GPP-E-UTRAN-FDD
```

2. Perform the LDAP add operation:

```
ldapadd -H ldaps://<vip_address>:<ssl_port> -Y plain -U  
<username> -w <password> -O none -f DNM_Example2.ldif
```

3. Verify the changes:

```
ldapsearch -H ldaps://<vip_address>:<ssl_port> -Y plain  
-U <username> -w <password> -O none -b  
"MtasCommonDataAccNetwType=3GPP-E-UTRAN-FDD,MtasCommonD  
ata=0,applicationName=MtasFunction,nodeName=jambala"
```

Example 3: Add the MtasCommonDataPaniTranslationProfile using Provisioning LDAP

The MtasCommonDataPaniTranslationProfile defines the wildcarding profiles. The wildcarding is used during the mobile cell lookup process.

1. Prepare the DNM_Example3.ldif:

```
dn: MtasCommonDataPaniTranslationProfile=3GP  
P-UTRAN-FDD&utran-cell-id-3gpp, MtasCommonDat  
aPaniTranslationProfiles=0, MtasCommonData=0,  
applicationName=MtasFunction,nodeName=jambala  
objectClass: MtasCommonDataPaniTranslationProfile  
mtasCommonDataPaniTranslationProfileRule: 10:/(.*)/3G  
PP-UTRAN-FDD&\1/  
MtasCommonDataPaniTranslationProfile:3GPP-UTRAN-FDD&ut  
ran-cell-id-3gpp
```

2. Perform the LDAP add operation:

```
ldapadd -H ldaps://<vip_address>:<ssl_port> -Y plain -U  
<username> -w <password> -O none -f DNM_Example3.ldif
```

3. Verify the changes:

```
ldapsearch -H ldaps://<vip_address>:<ssl_port> -Y plain  
-U <username> -w <password> -O none -b  
"MtasCommonDataPaniTranslationProfile=3GPP-U  
TRAN-FDD&utran-cell-id-3gpp, MtasCommonDataP  
aniTranslationProfiles=0, MtasCommonData=0,  
applicationName=MtasFunction,nodeName=jambala"
```



6 Configuration Parameters of LDAP Server

This section describes the configuration parameters for MTAS and examples to modify it.

6.1 Configuration Parameters for MTAS

This section describes the parameters introduced for MTAS of the provisioning server.

6.1.1 LDAP_PROVISIONING_PORT

This parameter sets the port number over which the LDAP server listens, see Table 1. For more Information, refer to *MTAS Hardening Guide*.

Table 1 LDAP_PROVISIONING_PORT

Value Range	Default Value	Type	Unit	Activation
0-65535	17323	Unsigned 16-bit integer ⁽¹⁾	N/A	Within one minute

(1) Make sure that it does not conflict with other open ports on the host.

6.1.2 LDAP_PROVISIONING_SSLPORT

This parameter sets the SSL port number over which the LDAP server listens, see Table 2. For more Information, refer to *MTAS Hardening Guide*.

Table 2 LDAP_PROVISIONING_SSLPORT

Value Range	Default Value	Type	Unit	Activation
0-65535	17423	Unsigned 16-bit integer ⁽¹⁾	N/A	Within one minute

(1) Make sure that it does not conflict with other open ports on the host.

6.1.3 LDAP_PROVISIONING_DNSUFFIX

This parameter is the DN suffix for the provisioning LDAP server, see Table 3.

Table 3 LDAP_PROVISIONING_DNSUFFIX

Value Range	Default Value	Type	Unit	Activation
String in the following format: "nodeName=<node_name>"	nodeName=jambala	String	N/A	Within one minute



6.2 Procedure

Example in this section demonstrates the procedure to configure the LDAP_PROVISIONING_DNSUFFIX parameter.

To configure parameter LDAP_PROVISIONING_DNSUFFIX:

1. Log on to the target system as root:

```
ssh root@[OAM ip]
```

2. Select the appropriate action based on the result of below command:

```
SC-1:~ # vdicos-envdata-get LDAP_PROVISIONING_DNSUFFIX
```

If the result is `error - object or attribute does not exist`, then proceed to Step 3 else proceed to Step 4.

3. Create the parameter:

```
SC-1:~ # vdicos-envdata-create LDAP_PROVISIONING_DNSUF  
FIX
```

4. Set the parameter:

```
SC-1:~ # vdicos-envdata-set LDAP_PROVISIONING_DNSUFFIX  
"nodeName=Node1"
```

5. Connect to the COM CLI on the OAM IP address:

```
SC-1:~ # ssh -p 830 -t -s root@[OAM ip] cli
```

6. Navigate to the ProvisioningServer=provisioning MO, for example:

```
>dn  
ManagedElement=1,MtasFunction.applicationName=MtasFunct  
ion,MtasSupportFunctions=0,  
ProvisioningM.applicationName=provisioning,Provisioning  
Server=provisioning
```

7. Enter Config mode:

```
(ProvisioningServer=provisioning)>configure
```

8. Delete the current accessControlList:

```
(config-ProvisioningServer=provisioning)>no  
accessControlList
```

9. Configure the new accessControlList:

```
(config-ProvisioningServer=provisioning)>accessControl  
List="to
```



```
dn.subtree=\"nodeName=Node1\" by dn=gidNumber=0+uid  
Number=0,cn=peercred,cn=external,cn=auth manage by  
anonymous auth by users manage by * none"
```

10. Commit the change:

```
(config-ProvisioningServer=provisioning)>commit
```





7 Access Control

On the provisioning LDAP interface, authentication is performed according to the PAM configuration and access control is determined by the LDAP ACL.

The LDAP ACL is defined by the `accessControlList` attributes of the `ProvisioningServer=provisioning` MO.

7.1 LDAP ACL

This section demonstrates the procedure to check the current ACL and how to update the ACL.

7.1.1 Show the Current ACL

To check the current ACL:

1. Navigate to the `ProvisioningServer=provisioning` MO, for example:

```
>dn
ManagedElement=1,MtasFunction.applicationName=MtasFunction,MtasSupportFunctions=0,
ProvisioningM.applicationName=provisioning,ProvisioningServer=provisioning
```

2. Show the current ACL:

```
(ProvisioningServer=provisioning)>show accessControlList
accessControlList
"to dn.subtree=\"nodeName=jambala\" by
dn=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth manage by anonymous auth by users manage by * none"
(ProvisioningServer=provisioning)>
```

7.1.2 Update the ACL

To update the ACL which controls the `MtasDnm` MTAS MOC to read only:

1. Navigate to the `ProvisioningServer=provisioning` MO, for example:

```
>dn
ManagedElement=1,MtasFunction.applicationName=MtasFunction,MtasSupportFunctions=0,
ProvisioningM.applicationName=provisioning,ProvisioningServer=provisioning
```



2. Enter Config mode:

```
(ProvisioningServer=provisioning)>configure
```

3. Delete the current `accessControlList`:

```
(config-ProvisioningServer=provisioning)>no  
accessControlList
```

4. Configure the new `accessControlList`:

```
(config-ProvisioningServer=provisioning)>accessControl  
List="to  
dn.subtree=\"MtasDnm=0,MtasMmt=0,MtasServices=0,applica  
tionName=MtasFunction,nodeName=jambala\" by users read"
```

```
(config-ProvisioningServer=provisioning)>accessControl  
List="to  
dn.subtree=\"nodeName=jambala\" by dn=gidNumber=0+ui  
dNumber=0,cn=peercred,cn=external,cn=auth manage by  
anonymous auth by users manage by * none"
```

5. Commit the change:

```
(config-ProvisioningServer=provisioning)>commit
```