

# LDAP-Based Authentication and Authorization Interface

---

## INTERWORK DESCRIPTION

**Copyright**

© Ericsson AB 2016, 2017. 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

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Concepts</b>	<b>3</b>
<b>3</b>	<b>LDAP Client</b>	<b>5</b>
3.1	LDAP Transport Layer Security	5
<b>4</b>	<b>LDAP Schemas</b>	<b>7</b>
4.1	Standard Schema	7
4.2	Extended POSIX Account Schema	7
4.3	Ericsson Role Aliases Schema	8
<b>5</b>	<b>LDAP Account Management</b>	<b>9</b>
5.1	Extended POSIX Account Management	9
<b>6</b>	<b>LDAP Lookup Behavior</b>	<b>11</b>
6.1	LDAP Authentication Behavior	11
6.2	LDAP Authorization Behavior	11
6.3	LDAP Referral Chase	16
<b>7</b>	<b>Target-Based Access Control</b>	<b>17</b>
<b>8</b>	<b>LDAP Object Classes and Attribute Types</b>	<b>21</b>





# 1 Introduction

This document describes the following:

- The Managed Element (ME) Lightweight Directory Access Protocol (LDAP) client capabilities
- The LDAP configuration supported by the ME and required in the LDAP server for interworking
- The ME LDAP lookup behavior





## 2 Concepts

### Target-Based Access Control

The LDAP client in the ME provides support to have different management roles for an O&M user depending on the type of ME.

To be able to categorize the MEs this way, the nodes must be configured with one or more target type identities using the attribute `targetType` in *UserManagement* Managed Object.

For example, the network can span several countries and it is needed to let an O&M user act as “admin” in one country, but only as “operator” in another. For more information, see Section 7 on page 17.

### Roles Grouping, Role Aliases

The LDAP client in the ME supports grouping of management roles. Different types of MEs have its own set of roles, because definition of roles is often done locally on the individual ME.

For example, the role “administrator” has been specified as “admin” on one node and “adm” on another. To make administration of equal or similar roles easier, the LDAP client supports the concept of role alias. For example, the alias “admin” can be assigned to “admin”, “adm”, and “administrator”.







## 3 LDAP Client

This section describes the LDAP client capabilities supported by the ME.

The ME has two separate ldap clients, one performing user authentication and another for user authorization. The authentication client is sssd, and authorization client is Ericsson proprietary.

If one LDAP server fails, the both LDAP clients in ME connect to a backup LDAP server. For the behavior of authenticating client, see sssd documentation. In authorization client an LDAP bind attempt is time-limited to 11 seconds. If no response is received within this time, the client immediately attempts to bind to the next server in the list.

The ME can use directory server-enforced password policy control.

Password changes are handled in compliance with RFC 3062.

Only LDAP version 3 is supported.

LDAP clients work only with the LDAP server, which supports ORDERING matching rule for uidNumber and gidNumber attributes. For example, the version of the OpenLDAP server must be at least 2.4.25.

### 3.1 LDAP Transport Layer Security

For LDAP over Transport Layer Security (TLS), the ME uses either LDAPS protocol or `StartTLS` operation according to RFC 4513.

The TLS ciphers offered by the ME are configurable. For that, see *Tls Managed Object* in the Managed Object Model (MOM).

The X.509 certificate that the LDAP server sends to the ME to set up TLS must be constructed properly: The `subjectAltName` (or `subject`) field in the certificate must contain the Uniform Resource Identifier(s) (URI) which is/are configured in ME to reach the LDAP server. That means the attributes `ldapIpAddress` and `fallbackLdapIpAddress` in *Ldap Managed Object* in the MOM.





## 4 LDAP Schemas

This section describes the LDAP schemas supported by the ME.

### 4.1 Standard Schema

The ME supports authentication and authorization based on the POSIX<sup>®</sup> account and the POSIX group schemas, according to RFC 2307.

Authentication is supported according to RFC 2307.

Authorization requires that the following conventions are followed:

- The ME expects that each defined security role is expressed as a POSIX group entry, and that a security role is equal to the attribute `cn` of a POSIX group.
- Each Northbound Interface (NBI) user who is to act in the specified role must be included in the multi-valued attribute `memberUid` of the POSIX group.

### 4.2 Extended POSIX Account Schema

The ME supports a standard POSIX account schema extended with the following attributes:

- `ericssonUserAuthenticationScope`
- `ericssonUserAuthorizationScope`

The authentication scope extension enables the Security Administrator to define for which target type or types a user is to be authenticated. The authentication scope is used by the ME, as described in Section 6.1 LDAP Authentication Behavior on page 11. For more information on target type, see chapter Section 7 on page 17.

The authorization scope enables the security manager to specify the following:

- The role or roles the user has in the system, which the user has logged on to, when no “target type” prefix is configured.
- The role or roles the user has in the system, which the user has logged on to, when the “target type” prefix is configured.
- The alias role or roles the user has in the system, which the user has logged on to. There is no syntactic difference between a role and an alias role. If

alias roles are used, then the role aliases schema must be also included in the LDAP server, see Section 4.3 Ericsson Role Aliases Schema on page 8.

The authorization scope is used by the ME as described in Section 6.2 LDAP Authorization Behavior on page 11.

## 4.3 Ericsson Role Aliases Schema

The ME supports LDAP objectclass `ericssonRoleAlias` which includes a multi-value role attribute enabling the resolution of an alias role into a real role. This resolution is meaningful to the system to which the user has logged on.

The ME expects that each real role in `ericssonRoleAlias` is equal to an `ericssonUserAuthorizationScope` (see Section 4.2 Extended POSIX Account Schema on page 7) in the multi-value role attribute in `ericssonRoleAlias` entry. The `ericssonRoleAlias` entry must not contain a nested alias role (`ericssonRoleAlias` entry cannot refer to another `ericssonRoleAlias` entry).

An example of an Ericsson role alias with example roles in LDAP Data Interchange Format (LDIF) is shown in Example 1. The user entry

```
dn: role=sysadmin, dc=cominf, dc=eei, dc=ericsson, dc=se
objectClass: ericssonRoleAlias
ericssonUserAuthorizationScope: cscfsysadministrator
ericssonUserAuthorizationScope: mtassysadm
ericssonUserAuthorizationScope: ecimtopadmin
ericssonUserAuthorizationScope: ecimfmadmin
ericssonUserAuthorizationScope: ecimsnmpadmin
ericssonUserAuthorizationScope: ecimsecmreadonly
ericssonUserAuthorizationScope: sbg:readonly
```

*Example 1 Ericsson Role Alias with Example Roles in LDIF*

For a definition of the objectclass of `ericssonRoleAlias`, see Section 8 on page 21.



## 5 LDAP Account Management

This section describes the LDAP user account attributes supported by the ME and required in the LDAP server.

### 5.1 Extended POSIX Account Management

The Ericsson extended POSIX account has mandatory and optional attributes. The attributes described in Table 1 must be configured when defining LDAP user accounts.

*Table 1 Attributes for Ericsson Extended POSIX Account*

Attribute	Description
<code>uid</code>	Key attribute for user queries. Mandatory
<code>uidNumber</code>	The <code>uidNumber</code> attributes of the LDAP accounts are to be assigned to users so that collision with local accounts is avoided. To leave space for system and password-aged local accounts, the POSIX accounts in LDAP are to use <code>uidNumber</code> greater than, or equal to, 1000. Mandatory
<code>ericssonUserAuthenticationScope</code>	The semantics and the behavior using this attribute are described in Section 6 on page 11 and Section 7 on page 17. Optional.
<code>ericssonUserAuthorizationScope</code>	The semantics and the behavior using this attribute are described in Section 6 on page 11 and Section 7 on page 17. Optional

The ME does not use the `gidNumber` information of the POSIX accounts when roles are determined for the user. However, it is recommended that the LDAP accounts and their groups are assigned in a way that they do not collide with local groups. To leave space for system groups, the POSIX accounts and groups in LDAP are to use `gidNumber` greater than, or equal to, 500.

For a description of the LDAP-specific syntax and matching rules of attribute `attributetypes`, see Section 8 on page 21.

The mandatory and optional Ericsson extended POSIX account attributes that are not mentioned here are not used by the ME.



### Example of Ericsson Extended POSIX Account

Example 2 is based on RFC 2307 and RFC 2798 in LDIF according to RFC 2849.

For a description of the objectclasses of `ericssonUserAuthentication` and `ericssonUserAuthorization`, see Section 8 on page 21.

```
dn: uid=lars,ou=people,dc=alvsjo,dc=ims,dc=telco,dc=com
objectClass: account
objectClass: posixAccount
objectClass: ericssonUserAuthentication
objectClass: ericssonUserAuthorization
objectClass: top
uid: lars
uidNumber: 1000
gidNumber: 1000
userPassword:: e1NTSEF9ck9ZbEJIRXNaek9Mbm1ybmRFNVlncUVVS1l5TURKTzQ=
ericssonUserAuthenticationScope: alvsjo.ims.cscf
ericssonUserAuthenticationScope: cscf
ericssonUserAuthorizationScope: ims:monitor
ericssonUserAuthorizationScope: cscf:ator
ericssonUserAuthorizationScope: alvsjo.ims.cscf:sysadmin
homeDirectory: /home/lars
```

*Example 2 Ericsson Extended POSIX Account*



## 6 LDAP Lookup Behavior

This section describes the ME LDAP lookup behavior.

### 6.1 LDAP Authentication Behavior

When ME is authenticating the user, it searches for an user account entry in LDAP server by matching logon name with the uid attribute in the account entry.

ME searches for account entry candidates with ldap search with configured baseDn, scope=wholeSubtree and filter="(&(&(&(uid=<logon\_name>)(objectclass=posixAccount))(uid=\*))(&(uidNumber=\*)!(uidNumber=0)))", where <logon\_name> is the logon name used by the user.

The ME selects the account entry by comparing the uid attribute with the logon name. The comparison is either in case sensitive or case insensitive. This depends on an integration time configuration option in ME which is not changeable at deployed ME. The default handling is case sensitive. If there is a match, then ME tries to make simple bind to the selected user account entry using the password provided by the user at logon. Successful bind implies successful authentication.

The sshkey based authentication is not supported.

If target types are specified when Ldap authentication and Target Based Access Control (TBAC) are enabled, the ME uses `ericssonUserAuthenticationScope` in extended POSIX accounts to filter out if a user can be authenticated on the node.

For example, `ericssonUserAuthenticationScope: ims.South` in the extended POSIX account of the user enables the ME to authenticate the user if `ims.South` matches a target type configured in the ME.

In addition to authentication of users with matching target type, also explicit wildcard, the asterisk character (\*), in `ericssonUserAuthenticationScope` is accepted. Explicit wildcard is also accepted even if no target type is configured. If TBAC is disabled, the ME allows access to all users having a valid password.

### 6.2 LDAP Authorization Behavior

The ME based on configuration can use the following three profile filters when an LDAP search for authorization is performed:

- `POSIX_GROUPS`



- `ERICSSON_FILTER`
- `FLEXIBLE`

For more information on profile filters, refer to *LdapManaged* Object in the MOM.

### 6.2.1 **POSIX\_GROUPS Profile Filter**

For the `POSIX_GROUPS` profile filter, the ME retrieves all instances of `posixGroup` in which the current NBI user logon name corresponds one of the values of multivalued attribute `memberUid`. The user is granted roles from matching `posixGroup` entries according to `cn` attribute.

See Example 3, where user "lars" has two roles configured: "SystemAdministrator" and "SystemSecurityAdministrator".





```
#
# User Account Entry
#
# Note: only attributes relevant for role handing in POSIX schema are shown.
#
dn: uid=lars,ou=people,dc=alvsjo,dc=ims,dc=telco,dc=com
objectClass: account
objectClass: posixAccount
uid: lars

#
# POSIX Group Entry
#
# Note: only attributes relevant for role handing in POSIX schema are shown.
# This group represents role SystemSecurityAdministrator.
# Only one user "lars" has SystemSecurityAdministrator role assigned.
#
dn: cn=SystemSecurityAdministrator,ou=group,dc=telco,dc=com
objectClass: posixGroup
cn: SystemSecurityAdministrator
memberUid: lars
# Note: gidNumber is not used by the ME
gidNumber: 50000

#
# POSIX Group Entry
#
# Note: only attributes relevant for role handing in POSIX schema are shown.
# This group represents role SystemAdministrator.
# Two users "lars" and "magnus" have SystemAdministrator role assigned
# (user magnus does not have user account entry in this example)
#
dn: cn=SystemAdministrator,ou=group,dc=telco,dc=com
objectClass: posixGroup
cn: SystemAdministrator
memberUid: lars
memberUid: magnus
# Note: gidNumber is not used by the ME
gidNumber: 50001
```

*Example 3 Roles in POSIX Account*

## 6.2.2 ERICSSON\_FILTER Profile Filter

For the ERICSSON\_FILTER profile filter, target types configured for the ME are used when performing the LDAP search. The ME uses `ericssonUserAuthorizationScope` and `ericssonUserAuthenticationScope` from the extended POSIX account, see Section 4.2 Extended POSIX Account Schema on page 7.



The ME follows the following steps:

1. If target types are configured and TBAC is enabled:
  - a. The ME filters the target types for the user from attribute `ericssonUserAuthenticationScope` of the extended POSIX account and takes an intersection with the local node types.
  - b. The ME takes the resulting set of target types and keeps the roles from attribute `ericssonUserAuthorizationScope` of the extended POSIX account that has a prefix matching a target type or explicit wildcard.

Roles without any target type qualifiers are accepted on *EricssonFilter* *version 1*, but not accepted on *version 2*, as shown in Table 2.

All other roles in the account are ignored.

2. If a role alias base Distinguished Name (DN) is configured, the ME tries to resolve the list of roles gathered in the first step as alias roles. If the ME cannot resolve a role as an alias role, it uses it as it was a resolved role. An alias role is to be specified as described in Section 4.3 Ericsson Role Aliases Schema on page 8.

Aliases without any target type qualifiers are accepted on both *EricssonFilter* versions, as shown in Table 2.

3. The ME repeats Step 1 to filter the roles based on target type qualifiers for role alias objects.

Table 2 describes how the roles and role aliases are handled in different configuration scenarios. The entry `<target>` is the target type for the node where the user is being authorized. The entry matches only with a node having the same target type. The `"*"` is a wildcard that matches all node target types. An entry with no target type is an implicit wildcard and it behaves the same way as the explicit wildcard `"*"`. The `<role>` and `<role alias>` entries are configured in the `ericssonUserAuthorizationScope` as described in Section 4.3 on page 8.

**Note:** The roles and role aliases are accepted in different manner in certain scenarios.



Table 2 Local role and role alias resolution.

Entry	TBAC OFF	TBAC ON <i>EricssonFilter</i> version 1	TBAC ON <i>EricssonFilter</i> version 2
<target> ":" <role>	Not Accepted	Accepted when the target matches.	Accepted when the target matches.
<target> ":" <role alias>	Not Accepted	Accepted when the target matches.	Accepted when the target matches.
<role>	Accepted	Accepted	Not Accepted
<role alias>	Accepted	Accepted	Accepted
"*" ":" <role>	Accepted	Accepted	Accepted
"*" ":" <role alias>	Accepted	Accepted	Accepted



**Note:** The `targetType` attribute must be set to non-empty value when TBAC is ON, see *Configure Target-Based Access Control* for details.

The Example 4 contains one possible LDAP configuration. The following roles are returned for the target type `ims.South`:

- Administrator, Supervisor, and Operator for the user if version is 1.
- Administrator and Supervisor for the user if version is 2. The Operator is expanded if it is defined as a role alias.

```
ericssonUserAuthenticationScope: ims.South
ericssonUserAuthorizationScope: ims.South:Administrator
ericssonUserAuthorizationScope: ims.North:SecurityAdministrator
ericssonUserAuthorizationScope: *:Supervisor
ericssonUserAuthorizationScope: Operator
```

*Example 4 Filter Roles*

### 6.2.3 FLEXIBLE Profile Filter

For the `FLEXIBLE` profile filter, the ME performs an LDAP search as configured in the ME.

## 6.3 LDAP Referral Chase

The ME supports client referral chasing for both authentication and authorization. This applies only if the referral URL refers to the same LDAP server instance while authenticating. This means that if the referral returns the address of a different host, authentication fails.

Client referral chasing can be configured from the NBI by setting attribute `useReferrals` in Managed Object `Ldap`. The attribute can have the following values:

- `true` – Referral chase is enabled.
- `false` – Referral chase is disabled, that is, the LDAP client ignores the URL returned by the referral.

**Note:** The default value is `false`.



## 7 Target-Based Access Control

This chapter provides background information for target-based access control (TBAC).

The LDAP client in the ME supports Target-Based Access Control (TBAC) when `profileFilter` is configured to value `ERICSSON_FILTER` in the ME. Refer to *Ldap* MOC and *ProfileFilter* enumeration.

TBAC configuration of an ME needs a set of target classifiers. The target types of the ME can contain any classifier string for the ME, for example, geographical, such as Stockholm, or network, such as IMS, or functional identifiers, such as CSCF, and any combination of those.

In the LDAP server, the optional Ericsson specific extended POSIX Account schema attributes `ericssonUserAuthenticationScope` and `ericssonUserAuthorizationScope` define if and which privileges the user is granted in the node.

- `ericssonUserAuthenticationScope`

The target qualifier values in `ericssonUserAuthenticationScope` in the LDAP server are intersected by the target types configured in *UserManagement* MO in the ME, in order to only allow the authorizations that are valid in the context of the local Ericsson application. The field of `ericssonUserAuthenticationScope` must be used as an authorization prefilter to preserve that the user does not get authorization escalation to a role which the user was not allowed to authenticate. `ericssonUserAuthenticationScope` allows the use of wildcarded scope to let the user to be authorized on any ME based on its `ericssonUserAuthorizationScope`.

- `ericssonUserAuthorizationScope`

The attribute can be used for defining authorization profiles (or: categories) the user is a member of. It is a case insensitive string "tuple" of form `<Target Qualifier>:<Authorization Profile>`, where ':' is the separator; `<Target Qualifier>` is the Ericsson node target type identifier, such as 'bsc', 'cscf', classifying the target node type for which the user acquires the `<Authorization Profile>`; `<Authorization Profile>` is the Ericsson application defined profile (for example: a role).

When TBAC is LOCKED in the ME, only the authorization profiles without target qualifiers and with wildcard scope (indicated by '\*' character) are assigned to the user from the user database.

When TBAC is UNLOCKED in the ME, the behavior depends on the `version` attribute in *EricssonFilter* MO configured in the ME. The behavior is described in Table 2

*Table 3 Versioned ericssonAuthorizationScope Behavior*

Version	Authorization of O&M User
1	The authorization profiles with matching target qualifiers, without target qualifiers, and with explicit wildcard scope are assigned to the user from the user database.
2	The authorization profiles with matching target qualifiers and with wildcard scope are assigned to the user from the user database. Authorization profiles with explicit wildcard (indicated by '*' character) can be used for both, role aliases and local roles. Implicit wildcard (no target qualifier) can only be used for role aliases.

A user account contains the following  
ericssonUserAuthenticationScope and  
ericssonUserAuthorizationScope:

```
ericssonUserAuthenticationScope:  
  cscf.ims.stockholm  
ericssonUserAuthenticationScope:  
  cscf.ims.malmo  
  
ericssonUserAuthorizationScope:  
  cscf.ims.stockholm:SystemAdministrator  
ericssonUserAuthorizationScope:  
  cscf.ims.malmo:SystemSecurityAdministrator  
ericssonUserAuthorizationScope:  
  *:ApplicationOperator
```

If TBAC is UNLOCKED, the user will be assigned with role  
'SystemAdministrator' and 'ApplicationOperator' on the ME  
having 'cscf.ims.stockholm' as target type.

#### *Example 5*



If the user account contains an explicit declaration of no target restriction, a reserved wildcard string '\*', the user will be able to authorize to any ME. For instance:

```
ericssonUserAuthenticationScope: *
```

On an ME where TBAC is LOCKED, from Example 5, the user will receive authorization profile 'ApplicationOperator' only.

On an ME 'cscf.ims.stockholm' where TBAC is UNLOCKED, from Example 5, the user will receive roles 'SystemAdministrator' and 'ApplicationOperator'.

### *Example 6*







## 8 LDAP Object Classes and Attribute Types

This section describes the structure, syntax, and matching rules of LDAP `objectclasses` and `attributetypes` supported by the ME and required in the LDAP server. This is according to RFC 4517.

The Object Identifiers (OIDs) are registered in the Ericsson branch of the OID structure.

**Note:** In Example 7, ensure that the syntax exactly includes the tab spaces when it is copied to the LDAP schema file.



```
attributetype ( 1.3.6.1.4.1.193.207.372
    NAME 'ericssonUserAuthenticationScope'
    DESC 'Ericsson User Authentication Scope'
    EQUALITY caseIgnoreIA5Match
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

## Auxiliary Object Class for Ericsson User authentication attributes.
objectclass ( 1.3.6.1.4.1.193.207.374
    NAME 'ericssonUserAuthentication'
    SUP top AUXILIARY
    MAY ( ericssonUserAuthenticationScope ))

attributetype ( 1.3.6.1.4.1.193.207.373
    NAME 'ericssonUserAuthorizationScope'
    DESC 'Ericsson User Authorization Scope'
    EQUALITY caseIgnoreIA5Match
    SUBSTR caseIgnoreIA5SubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

## Auxiliary Object Class for Ericsson User authorization attributes.
objectclass ( 1.3.6.1.4.1.193.207.376
    NAME 'ericssonUserAuthorization'
    SUP top AUXILIARY
    MAY ( ericssonUserAuthorizationScope ))

attributetype ( 1.3.6.1.4.1.193.207.371
    NAME 'role'
    DESC 'Ericsson Role'
    EQUALITY caseIgnoreIA5Match
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

## Auxiliary Object Class for Ericsson Role Aliases
objectclasses: ( 1.3.6.1.4.1.193.207.375
    NAME 'ericssonRoleAlias'
    SUP top STRUCTURAL
    MAY ( role $ ericssonUserAuthorizationScope))
```

**Example 7** *LDAP Object Classes and Attribute Types*