

LDAP-Based Authentication and Authorization Interface

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2014, 2015. 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
2	LDAP Client	3
2.1	LDAP Transport Layer Security	3
3	LDAP Schemas	5
3.1	Standard Schema	5
3.2	Extended POSIX Account Schema	5
3.3	Ericsson Role Aliases Schema	6
4	LDAP Account Management	7
4.1	Extended POSIX Account Management	7
5	LDAP Lookup Behavior	9
5.1	LDAP Authentication Behavior	9
5.2	LDAP Authorization Behavior	9
5.3	LDAP Referral Chase	11
6	LDAP Object Classes and Attribute Types	13





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 LDAP Client

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

If one LDAP server fails, the LDAP clients must quickly fall over to a backup LDAP server. An LDAP bind attempt is time-limited to 3 seconds. If no response is received within this time, the client immediately attempts to bind to the next server in the list.

The ME offers the strongest cipher first and excludes the Data Encryption Standard (DES) cipher from the available cipher suite.

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

Password changes are handled in compliance with RFC 3062.

Note: Only LDAP version 3 is supported.

2.1 LDAP Transport Layer Security

For LDAP over Transport Layer Security (TLS), the ME uses action `StartTLS` according to RFC 4513.

The LDAP client requires that the configured IP address or Fully Qualified Domain Name (FQDN) of the LDAP server as reference identity is present in the certificate of the LDAP server as one of the following:

- `subjectAltName` values
- `subjectName` field Common Name (cn) value





3 LDAP Schemas

This section describes the LDAP schemas supported by the ME.

3.1 Standard Schema

The ME supports authentication and authorization based on the POSIX[®] 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 equal to the Common Name 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.

3.2 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 5.1 LDAP Authentication Behavior on page 9. For more information on target type, refer to *Security Management for ECLI, NETCONF, and SFTP Users*.

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. In this case, the value of the authorization scope must have the format `<target_type>:<role>`, where colon (:) is a delimiter.
- 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 an alias role is defined, the schema must also include the role aliases schema, see Section 3.3 Ericsson Role Aliases Schema on page 6.

The authorization scope is used by the ME as described in Section 5.2 LDAP Authorization Behavior on page 9.

3.3 Ericsson Role Aliases Schema

The ME supports LDAP class `ericssonRoleAlias`, including 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 is equal to an `ericssonUserAuthorizationScope` (see Section 3.2 Extended POSIX Account Schema on page 5) in the multi-value role attribute, with the restriction that it cannot contain a nested alias role.

An example of an Ericsson role alias with example roles in LDAP Data Interchange Format (LDIF) is shown in Example 1. For a definition of the `objectclass` of `ericssonRoleAlias`, see Section 6 on page 13.

```
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



4 LDAP Account Management

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

4.1 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.
<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.
<code>ericssonUserAuthenticationScope</code>	The semantics and the behavior using this attribute are described in Section 3.2 Extended POSIX Account Schema on page 5.
<code>ericssonUserAuthorizationScope</code>	The semantics and the behavior using this attribute are described in Section 5 on page 9.

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 groups are assigned in way to avoid collision 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 6 on page 13.

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 6 on page 13.



```
dn: uid=lars,ou=people,dc=alvsjo,dc=ims,dc=telco,dc=com
cn: Lars Magnus Ericsson
ericssonUserAuthenticationScope: alvsjo.ims.cscf
ericssonUserAuthenticationScope: cscf
ericssonUserAuthorizationScope: ims:monitor
ericssonUserAuthorizationScope: cscf:ator
ericssonUserAuthorizationScope: alvsjo.ims.cscf:sysadmin
gecos: Lars Magnus Ericsson
gidNumber: 1000
homeDirectory: /home/lars
loginShell: /bin/bash
objectClass: ericssonUserAuthentication
objectClass: ericssonUserAuthorization
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
shadowInactive: -1
shadowLastChange: 13159
shadowMax: 99999
shadowMin: 0
shadowWarning: 7
sn: Ericsson
uid: lars
uidNumber: 1000
userPassword:: e1NTSEF9ck9ZbEJIRXNaek9Mbml5bmRFNVlncUVVS1l5TURKTzQ=
```

Example 2 *Ericsson Extended POSIX Account*



5 LDAP Lookup Behavior

This section describes the ME LDAP lookup behavior.

5.1 LDAP Authentication Behavior

If target types are specified when 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 configured target type.

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.

5.2 LDAP Authorization Behavior

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

- `POSIX_GROUPS`
- `ERICSSON_FILTER`
- `FLEXIBLE`

For more information on profile filters, refer to *Security Management for ECLI, NETCONF, and SFTP Users*.

5.2.1 `POSIX_GROUPS` Filter Type

For the `POSIX_GROUPS` filter type, the ME retrieves all instances of `posixGroup` in which the current NBI user is a member.

For a specification of the convention with which the POSIX groups are looked up, see Section 3.1 Standard Schema on page 5.



5.2.2 ERICSSON_FILTER Filter Type

For the `ERICSSON_FILTER` filter type, 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 3.2 Extended POSIX Account Schema on page 5.

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 `ericssonUserAuthorizationScope` of the extended POSIX account and takes an intersection with the local node types.
 - b. The ME takes the resulting set of Step a and filters the roles from attribute `ericssonUserAuthorizationScope` of the extended POSIX account that have a prefix matching a target type or explicit wildcard.

Also, if attribute `version` in managed object *EricssonFilter* is set to 1, the roles without any target type qualifier are also filtered. If the attribute is set to 2, the roles are not filtered. As shown in Example 3, if `ims.South` is a configured target type, the ME filters roles as follows:

- Administrator, Supervisor, and operator for the user if version is 1.
- Administrator and Supervisor for the user if version is 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 3.3 Ericsson Role Aliases Schema on page 6.
3. The ME repeats Step 1 to filter the roles based on target type qualifiers for role alias objects.

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

Example 3 Filter Roles



5.2.3 FLEXIBLE Filter Type

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

5.3 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`.





6 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 4, 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 4 *LDAP Object Classes and Attribute Types*