

LDAP-Based Authentication and Authorization Interface

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2016–2018. 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	LDAP-Based Authentication and Authorization in a CBA Environment	1
1.1	Key Features for LDAP-Based Authentication and Authorization	1
1.2	LDAP-Based Authentication and Authorization Concepts	2
1.3	LDAP Lookup Behavior	5
1.4	Target-Based Access Control	9
2	LDAP Object Classes and Attribute Types	13





1 LDAP-Based Authentication and Authorization in a CBA Environment

1.1 Key Features for LDAP-Based Authentication and Authorization

1.1.1 Role-Based Access Control

An access control method where the ME defines permission, that is access, for different management actions in terms of management roles. Each role has own set of rules which determine allowed management actions for the role in the ME.

The roles are assigned to user account in the LDAP server. After the ME has authenticated the user with the LDAP server, it requests the role of the user from the server. The user is then allowed to execute management actions in the ME based on role.

1.1.2 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 (MO).

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.

1.1.3 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`.



1.2 LDAP-Based Authentication and Authorization Concepts

1.2.1 LDAP Client

The ME has two separate LDAP clients, one performing user authentication and another for user authorization. The authentication client is System Security Services Daemon (SSSD), and authorization client is Ericsson proprietary.

If one LDAP server fails, both the 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.

1.2.1.1 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` MO 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 Identifiers (URI) which are configured in ME to reach the LDAP server. That means the attributes `ldapIpAddress` and `fallbackLdapIpAddress` in `Ldap` MO in the MOM.

1.2.2 LDAP Schemas

1.2.2.1 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 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.

1.2.2.2 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 1.3.1 on page 5. For more information on target type, see chapter Section 1.4 on page 9.

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 1.2.2.3 on page 3.

The authorization scope is used by the ME as described in Section 1.3.2 on page 6.

1.2.2.3 Ericsson Role Aliases Schema

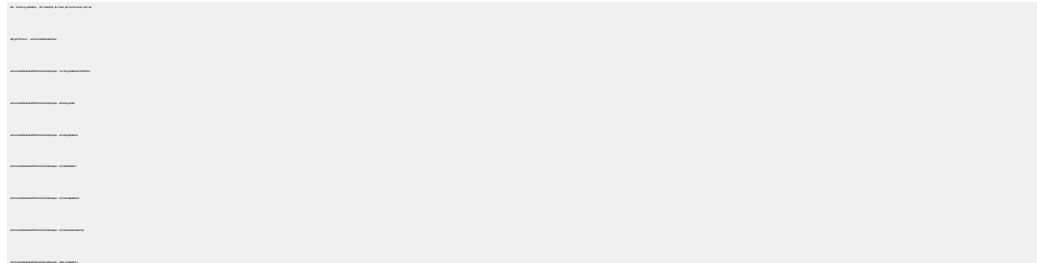
The ME supports LDAP objectclass `ericssonRoleAlias` which includes a multi-value role attribute enabling the resolution of an alias role into a real role. This resolution is meaningful to the system to which the user has logged on.

The ME expects that each real role in `ericssonRoleAlias` is equal to an `ericssonUserAuthorizationScope` (see Section 1.2.2.2 on page 3) 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.



For a definition of the `objectclass` of `ericssonRoleAlias`, see Section 2 on page 13.



Example 1 Ericsson Role Alias with Example Roles in LDIF

1.2.3 LDAP Account Management

Describes the LDAP user account attributes supported by the ME and required in the LDAP server.

1.2.3.1 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
uid	Key attribute for user queries. Mandatory
uidNumber	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
ericssonUserAuthenticationScope	The semantics and the behavior using this attribute are described in Section 1.3 on page 5 and Section 1.4 on page 9. Optional.
ericssonUserAuthorizationScope	The semantics and the behavior using this attribute are described in Section 1.3 on page 5 and Section 1.4 on page 9. 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.

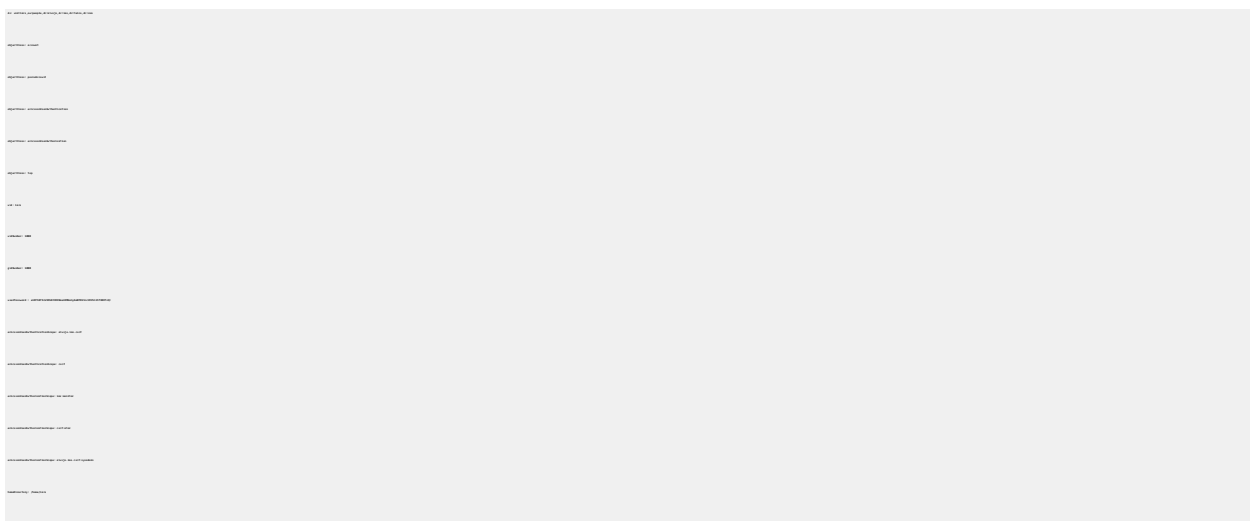
For a description of the LDAP-specific syntax and matching rules of attribute `attributetypes`, see Section 2 on page 13.

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 2 on page 13.



Example 2 Ericsson Extended POSIX Account

1.3 LDAP Lookup Behavior

1.3.1 LDAP Authentication Behavior

When ME is authenticating the user, it searches for a 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 if no target type is configured in the ME. If TBAC is disabled, the ME allows access to all users having a valid password.

1.3.2 LDAP Authorization Behavior

Depending on its configuration, the ME can use the following profile filters when an LDAP search for authorization is performed:

- POSIX_GROUPS
- ERICSSON_FILTER
- FLEXIBLE

For more information on profile filters, refer to `Ldap` MO in the MOM.

1.3.2.1 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

1.3.2.2 ERICSSON_FILTER Profile Filter

When the ERICSSON_FILTER profile filter is used, it is possible to use target types and role aliases in the LDAP server to control the authorization profile of the user. Role aliases can be used without using target types, but use of target types affects how role aliases are selected in the ME. The use of target types in general is explained in Section 1.4 on page 9.

Without target based access control enabled, the ME uses the role aliases as follows:

- 1 The ME reads the values of the attribute `ericssonUserAuthorizationScope` in the extended POSIX account entry for the user.
- 2 If `roleAliasBaseDn` attribute is not configured in the ME, then stop here.
- 3 The ME looks for possible role alias entries from the subtree specified by `roleAliasBaseDn`.
- 4 For each found role alias entry, the ME compares the values read in step 1 (the roles) against the RDN (role) of the role alias entry. If there is a match, the roles in the alias entry are added to list of user roles.



Example 4 Lookup of Role Alias in ERICSSON_FILTER

1.3.2.3 FLEXIBLE Profile Filter

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

1.3.3 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 the `Ldap` MO. 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`.

1.4 Target-Based Access Control

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, to allow only 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.

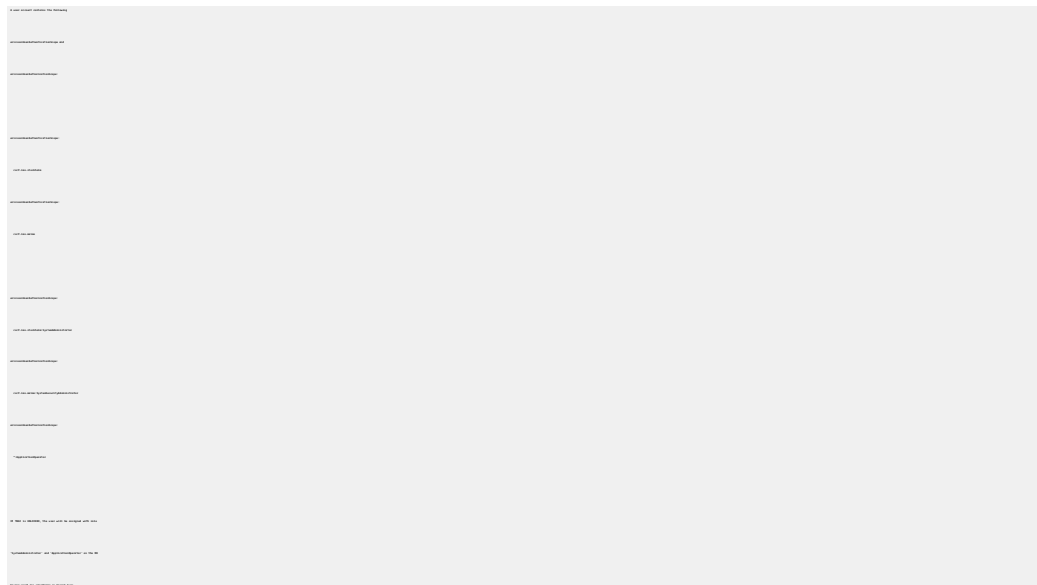


Table 2 describes how the roles and role aliases are handled in different configuration scenarios. The entry `<target>` is the target type for the node where the user is being authorized. The entry matches only with a node having the same target type. The `"*"` is a wildcard that matches all node target 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 1.2.2.3 on page 3.

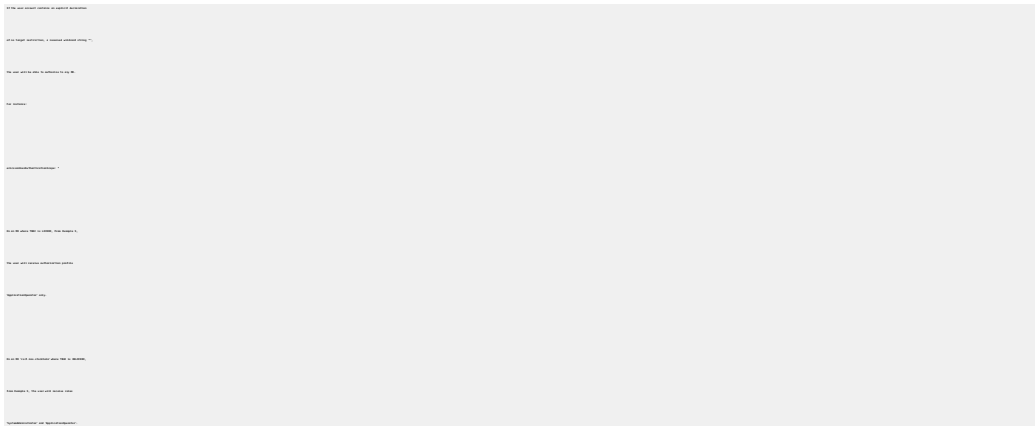
Note: The roles and role aliases are accepted in different manner in certain scenarios.

Table 2 Local Role and Role Alias Resolution

Entry	TBAC OFF (LOCKED)	TBAC ON (UNLOCKED) EricssonFilter version 1	TBAC ON (UNLOCKED) EricssonFilter version 2
<code><target> ":" <role></code>	Not Accepted	Accepted when the target matches.	Accepted when the target matches.
<code><target> ":" <role alias></code>	Not Accepted	Accepted when the target matches.	Accepted when the target matches.
<code><role></code>	Accepted	Accepted	Not Accepted
<code><role alias></code>	Accepted	Accepted	Accepted
<code>"*" ":" <role></code>	Accepted	Accepted	Accepted
<code>"*" ":" <role alias></code>	Accepted	Accepted	Accepted



Example 5 TBAC Configuration



Example 6 TBAC Configuration without Target Restriction



2 LDAP Object Classes and Attribute Types

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.

Example 7 LDAP Object Classes and Attribute Types