

# User Management Authentication

## DESCRIPTION

**Copyright**

© Ericsson AB 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

<b>1</b>	<b>Understanding User Management</b>	<b>1</b>
1.1	Key User Management Concepts	1
1.2	User Authentication	3
<b>2</b>	<b>User Management Authentication Procedures</b>	<b>3</b>
<b>3</b>	<b>User Management Authentication-Related Alarm</b>	<b>9</b>





# 1 Understanding User Management

## 1.1 Key User Management Concepts

User Management provides a management interface to configure the following on the Managed Element (ME):

- Local user authentication
- Lightweight Directory Access Protocol (LDAP) authentication
- Local authorization for maintaining local Policy Information Point (PIP)

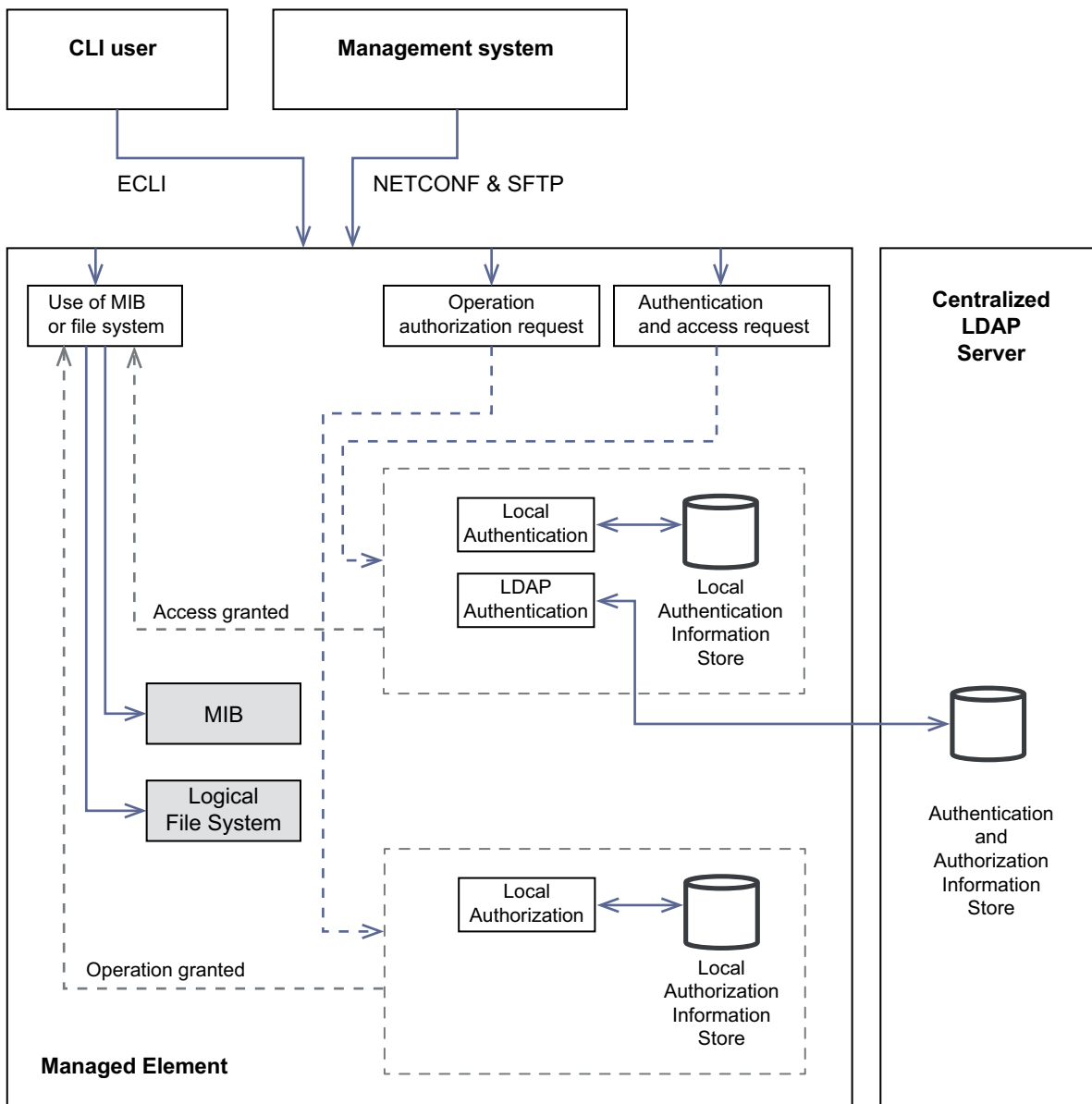


Figure 1 User Management Overview

This instruction assumes that the ME has already been installed and initially configured. The initial configuration includes the necessary settings for the authentication and authorization of users.

Authentication is used for checking user credentials and user access. Role-Based Access Control (RBAC) authorization is used to ensure correct user access privileges. The ME supports management of local users and authentication and supports the LDAP protocol for centralized user authentication. For centralized authentication, Target-Based Access Control (TBAC) can be applied over RBAC. Authentication and authorization are performed according to the organization authorization policy.



The local authentication method is always available to ensure that the operator cannot be inadvertently denied access to the managed element. It is recommended to create enough local accounts to mitigate connectivity issues to centralized authentication. The managed element supports centralized authentication by the LDAP protocol. Centralized authentication is preferred for daily operations to keep a consistent user base over a network of managed elements.

The local authentication method is always performed. If local authentication fails to find a user, the authentication continues with centralized LDAP authentication. The order of authentication methods cannot be changed.

## 1.2 User Authentication

The user initiates a session which triggers user authentication. For the authentication to be successful, a user account must be configured either locally by Local Authentication, or centrally in an external LDAP server. The first configured account is the Local Authentication administrator, which is defined at site deployment.

The administrator account is used for initial and recovery scenarios when authentication to regular O&M accounts is inaccessible. The administrator account is to be used to create the first local user accounts with appropriate authorization. The administrator account cannot be locked and its use must be limited to recovery scenarios.

When adding user accounts, naming must serve as a unique identity. Naming collisions can result in unexpected authentication behavior, as the user trying to authenticate with that name is mapped to the account first found with that name. The operator must ensure that usernames are globally unique, in the scope of both local and central authentication, to match expected authentication behavior.

In centralized LDAP authentication, a primary and a secondary LDAP server is supported. The LDAP authentication first tries against the primary server and then the secondary server.

## 2 User Management Authentication Procedures

User Management supports the following operations for an administrator with the System Security Administrator role.

### General

- Configure legal notice



The legal notice presented before user authentication on certain interfaces can be changed to comply to domestic legal requirements. The procedure [Configure Legal Notice](#) provides further details on how to perform this operation. Also refer to the appropriate documentation of the interface to learn if the legal notice is applicable.

- Change logon Failure Delay

The delay after a failed password logon attempt can be changed. The procedure [Configure Login Failure Delay](#) provides further details on how to perform this operation.

## Local Authentication

- Create, change, and delete user account

An O&M user account can be created and modified to give access to the system. It includes a username and a password or an SSH public key used for identification and authorization. The procedures in [Create User Account](#), [Change User Account](#), and [Delete User Account](#) provide further details on how to perform these operations.

- Reset password for user account

A reset password operation must be performed by the administrator when the user account is locked because of the password expiry. The procedure in [Reset Password for User Account](#) provides further details on how to perform this operation.

- Remove password from user account

The password can be removed if the user account is configured to use key based authentication. This removal of the password liberates the user account from password management requirements. The procedure [Remove Password from User Account](#) provides further details on how to perform this operation.

- Create SSH Public Key, Change SSH Public Key, and Delete SSH Public Key

User authentication is possible with SSH public key. If SSH public key is configured, it is recommended to remove the password from the account. SSH public key management is described by procedures in [Create SSH Public Key](#), [Change SSH Public Key](#), and [Delete SSH Public Key](#).

- Create, change, and delete account policy

The purpose of an account policy is to limit the accessibility of unused accounts. Account policies can be created and modified. The account policy setting locks an account if the account dormant time is set to be measured and the account dormant time runs out. All non-password related properties of user account are associated with account policy. The procedures in [Create Account Policy](#), [Change Account Policy](#), and [Delete Account Policy](#) provide further details on how to perform these operations.





- Create, change, and delete password policy

Security and usability with passwords are achieved by password management policies and the possibility to enforce strong passwords. The procedures in [Create Password Policy](#), [Change Password Policy](#), and [Delete Password Policy](#) provide further details on how to perform these operations. Strong passwords must be chosen to prevent brute-force password attacks. The procedure in [Change Password Quality Configuration](#) provides further details on how to perform this operation.

- Set user roles for user account

A user account is assigned one or several roles to enforce the access control to the node resources. For instance, the node resources can be the MO tree, CLI commands, or NETCONF operations. The procedure in [Set User Roles for User Account](#) provides further details on how to perform this operation.

- Lock user account administratively and unlock administrative lock for user account

The administrator can lock and unlock a user account. In managing the user access, the user can be locked out by the administrator, for example, if the user for some reason no longer is approved for having access. The procedures in [Lock User Account Administratively](#), and [Unlock Administrative Lock for User Account](#) provide further details on how to perform these operations.

- Unlock Operational Lock for User Account

A user account can also be locked by system, which can be unlocked by administrator. The reasons for a user account to be locked by the system could be, for example, because of an account or password policy, or because of too long user inactivity or password expiry. The procedure in [Unlock Operational Lock for User Account](#) provides further details on how to perform this operation.

- Change the alarm configuration for the administrator account

The specific Administrator account cannot be locked. As a measure to detect irregular logon activity to this account, the account can emit an alarm if the alarming threshold is reached. The number of failure attempts as a threshold can be configured. The procedure in [Change Administrator Account](#) provides further details on how to perform this operation.

**Note:** Local authentication operations must be used if the system does not support centralized authentication, or to configure centralized authentication and to define fallback accounts, in case the centralized user management service becomes inaccessible.

## LDAP Client Configuration in the ME

- View LDAP configuration



The administrator can check the current LDAP configuration. The understanding of the LDAP configuration is a prerequisite for solving any authentication issues. The procedure in [View LDAP Configuration](#) provides further details on how to perform this operation.

- Lock or Unlock LDAP authentication method

In maintenance situations, the administrator can lock the LDAP authentication to prevent users from accessing the ME, when it is not fully operational. When the LDAP authentication method is locked, only local authentication and emergency access to the ME is possible. The procedure in [Lock LDAP Authentication Method](#) provides further details on how to perform this operation.

The administrator unlocks the LDAP authentication to enable user LDAP authentication when the ME is operational or to test the proper execution of LDAP authentication. The procedure in [Unlock LDAP Authentication Method](#) provides further details on how to perform this operation.

- Configure LDAP basic connection

To get a clear text unsecure connection to an LDAP authentication server, the IP address and the port number of the server must be configured. Search operations to the server require a base Distinguished Name (DN). All LDAP user object must be accessible from this DN. Optionally a fallback IP address can be configured.

The procedure in [Configure LDAP Basic Connection](#) provides further details on how to perform this operation.

It is strongly recommended to secure the LDAP connection by using TLS.

- Configure referral chasing

LDAP referral shows that the LDAP server does not have the requested object and returns a possible location where the requested object could be found. The ME then follows the referrals returned to fetch the actual requested object.

Referral chasing is only to be configured if the LDAP server is known to return LDAP referrals from the searches on the base DN, which is configured as part of the [Configure LDAP Basic Connection](#) operation. When a referral is used to redirect user authentication, the referral can only point back to a different DN of the same server.

The procedure in [Configure Referral Chasing](#) provides further details on how to perform this operation.

- Configure bind name and password for LDAP authentication

The administrator can configure the bind name and password required for password-based simple bind LDAP authentication. The change of bind name and password can also be triggered by the organization security policy. The



procedure in [Configure LDAP Simple Bind](#) provides further details on how to perform this operation.

#### — Configure LDAP authorization filter

Authorization filter must be set up to enable LDAP server to provide authorization profile (a.k.a roles) of the user accounts. LDAP authentication does not use this information, but it is forwarded to Local Authorization function which enforces access control to the node resources based on the profile.

The ME supports the following authorization filter types:

- Ericsson filter, built-in LDAP filter that allows for RBAC and TBAC.
- POSIX filter, standard POSIX group filter which treats groups as RBAC roles.
- Flexible filter, which allows for interpreting an arbitrary attribute of an arbitrary object as RBAC role.

Only one filter type can be selected, and the recommended alternative is the Ericsson filter.

The procedures in [Configure Ericsson LDAP Filter](#), [Configure POSIX LDAP Filter](#), and [Configure Flexible LDAP Filter](#) provide further information for performing these operations.

The Ericsson LDAP filter has two incompatible versions, version 1 and version 2, each describing different ME authorization behavior. The differences between version 1 and version 2 are described in detail in [LDAP-Based Authentication and Authorization Interface](#).

The default is version 2, which has better security properties. If an old installation with version 1 is upgraded, it retains version 1 until configured to use version 2. The procedure in [Configure Ericsson Filter Version](#) provides further details on how to perform this operation.

**Note:** The version 1 is deprecated and is not to be used in new installations.

#### — Configure TLS for LDAP

In order to use TLS for LDAP, the administrator needs to install certificates for TLS. To authenticate the LDAP server, a trust category is required; to authenticate also the LDAP client (ME), a node credential must also be deployed. For the information on how to deploy certificates, refer to [Certificate Management](#).

The administrator needs to change the certificate settings for LDAP TLS in the following situations:

- The ME node credential for LDAP TLS has been reinstalled by certificate management.



- Another trust category for LDAP TLS must be used.

The administrator may need to change the default cipher suite for changed security requirements or compatibility with network peers.

The procedures in [Configure TLS for LDAP and SSH and TLS Protocol Management](#) provide further details on how to perform this operation.

#### — Configure Target-Based Access Control (TBAC)

The administrator needs to change the TBAC settings when the current settings no longer match the operator organization needs, for example, in the following situations:

- The ME needs to become part of a different geographical domain.
- The ME needs to become part of a different functional domain.
- The ME needs to become part of a different competence domain.

In order to apply TBAC, the user accounts or the role aliases in the LDAP server must be set up with authorizations that are scoped to specific ME target types. To set up these authorization roles and for the description of the corresponding authorization decision logic, refer to [LDAP-Based Authentication and Authorization Interface](#).

The procedure in [Configure Target-Based Access Control](#) provides further details on how to perform this operation.

#### — Configure role aliases for RBAC

When role aliases are used then the ME must know the LDAP base DN where the alias objects reside: The role aliases base DN needs to be configured in the ME.

The procedure in [Configure Role Aliases for RBAC](#) provides further details on how to perform this operation.

To configure role alias objects in the LDAP server and for the description of the corresponding role resolution logic, refer to [LDAP-Based Authentication and Authorization Interface](#).

**Note:** LDAP authentication must be configured if there is a centralized user management service accessible with the LDAP protocol. For security, deploying it with TLS is highly recommended.



### 3 User Management Authentication-Related Alarm

Table 1 User Management Authentication-Related Alarm

Alarm	Description
Local Authentication, Authentication Failure Limit Reached	The number of failed password logon attempts on the administrator account exceed the threshold passwordMaxFailure within the time interval passwordFailureCountInterval.