

User Management Authorization

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

1	Understanding User Management	1
1.1	Key User Management Concepts	1
1.2	User Authorization	3
1.3	Permission Types	3
1.4	Default Roles	4
2	User Management Authorization Procedures	5
3	Rules for Default Roles	6





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)

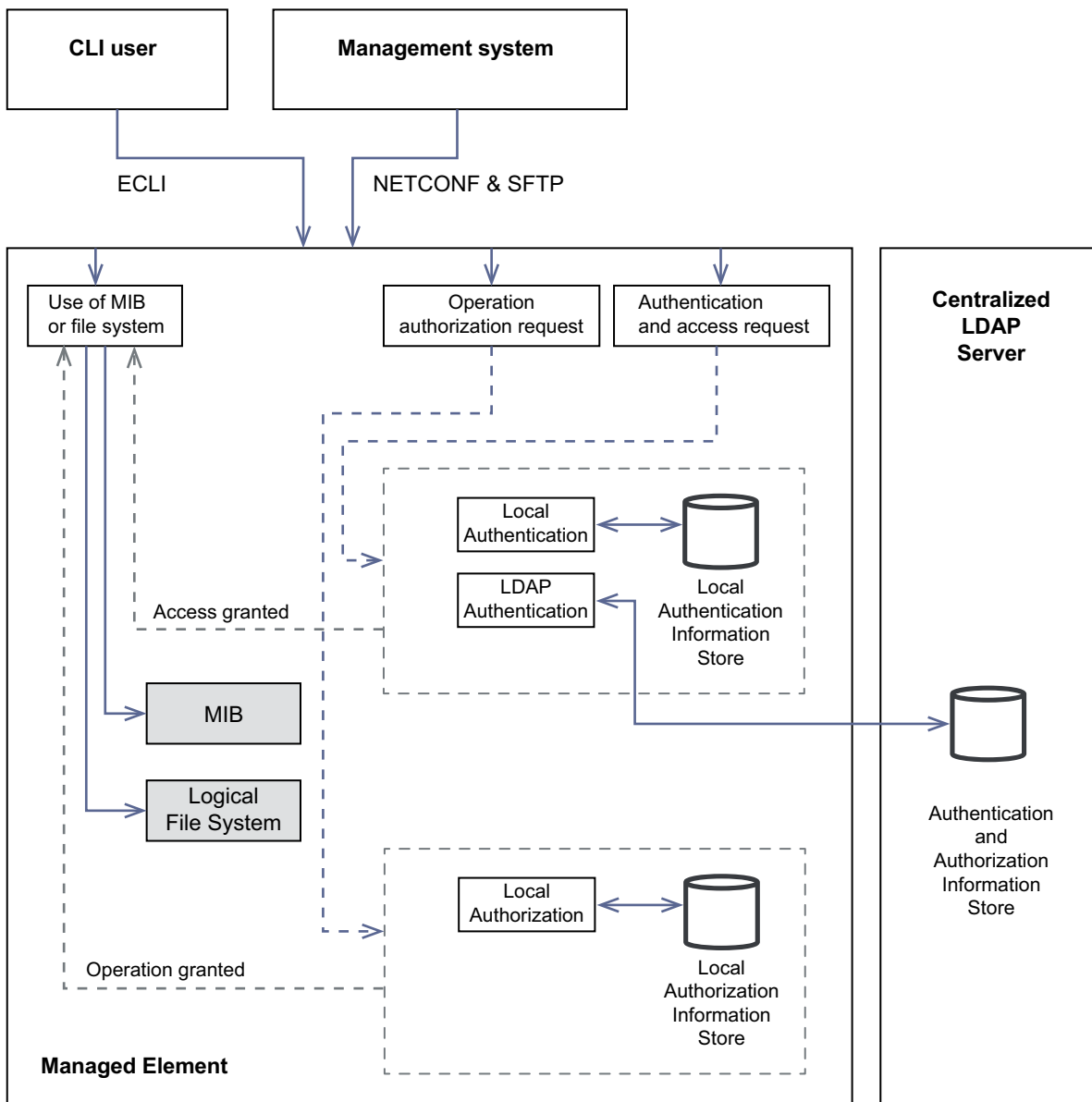


Figure 1 User Management Overview

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 Authorization

Before user authorization occurs, the ME queries the roles of the users.

For local users, the roles are stored in the user account configuration.

The user access rights depend on defined authorization rules that specify the permissions to a set of resources within the ME. The authorization rules are grouped into roles. A role is equivalent to the user occupation within an organization, for example, system administrator. A user can have one or more roles.

The ME supports some predefined roles, see Section 1.4 Default Roles on page 4. Custom roles can also be configured over the Northbound Interface (NBI).

The authorization rules are all defined locally on the ME. Therefore, the user authorization is a local authorization. Custom rules corresponding to customer roles can be configured over the NBI.

Authorization rules provide different access levels to the MIB and the ECLI commands. Authorization rules are defined by permission types, see Section 1.3 Permission Types on page 3.

1.3 Permission Types

Rules for access can be specified for Managed Objects (MOs), their attributes and actions. The execution of the ECLI commands and the NETCONF operations is not subject to authorization. However, the rules affect the result of the ECLI commands and the NETCONF operations that operate on MOs.

Table 1 Permission Types and Access Levels

Permission Type	Description
No access (NO_ACCESS)	The user has no read, write, or execute rights to the MOs, attributes, or actions
Execute (X)	The user can execute all actions in the MOM



Table 1 Permission Types and Access Levels

Permission Type	Description
Read (R)	The user can read MOs and get attribute values
Read and execute (RX)	The user can read MOs, get attribute values, and execute all actions in the MOM
Read and write (RW)	The user can create and delete MOs as well as get and set attribute values
Read, write, and execute (RWX)	The user can create and delete MOs, set, and get attribute values, as well as execute all actions in the MOM

When a user with an authorization profile wants to access resources of the ME, the access request is authorized against matching security rules. The rules are checked in the following order:

- 1 All negative rules (with the NO_ACCESS permission) are evaluated. If a match is found, access is denied.
- 2 All positive rules (with X, R, RX, RW, and RWX permissions) are evaluated until a match is found; the corresponding access is granted. If no match is found, access is denied.

1.4 Default Roles

The ME supports several predefined default roles. These roles and the corresponding rules cannot be modified. The detailed permissions for each role are described in Section 3 on page 6.

Default permissions to the ME are granted automatically to all users and are expressed through the role named “Self”.

Table 2 Predefined Default Roles

Default Role	Description
Self	Used for default authorization permissions.
System Administrator	Responsible for the administration of all non-security-related attributes and capabilities of an ME, including features, configuration parameters, and monitoring.
Local Authentication Administrator	Responsible for the administration of the local user accounts at initial or recovery scenarios. Dedicated to the Administrator Account to limit its use.
System Security Administrator	Responsible for the administration of all security-related attributes and capabilities of an ME, including user accounts and authorizations.



Table 2 Predefined Default Roles

Default Role	Description
System Read Only	Can view most non-security-related attributes and capabilities of an ME, including features, configuration parameters, and monitoring.
Managed Function Application Administrator	Responsible for the administration of all non-security-related attributes and capabilities of the Managed Function, including features, configuration parameters, and monitoring.
Managed Function Application Security Administrator	Responsible for the administration of all security-related attributes and capabilities of the Managed Function, including user accounts and authorizations.
Managed Function Application Operator	Can view some non-security-related attributes and capabilities of the Managed Function, including features, configuration parameters, and monitoring.

2 User Management Authorization Procedures

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

Local Authorization

— View roles and rules

The administrator can view the roles retrieved from the LDAP server and the rules defined in the ME. The understanding of the roles and rules is a prerequisite for solving any authorization issues. The procedure in [View Roles and Rules](#) provides further details on how to perform this operation.

— Lock or unlock local authorization method

The administrator locks the local authorization to give full access to all resources to all users authenticated by LDAP. Locking can be done in maintenance situations. The procedure in [Lock Local Authorization Method](#) provides further details on how to perform this operation.

The administrator unlocks the local authorization to enable the local authorization based on defined rules and roles when the ME is operational or to test the proper execution of local authorization. The procedure in [Unlock Local Authorization Method](#) provides further details on how to perform this operation.



— Create, change, and delete custom roles and custom rules

The administrator can create or change custom roles and custom rules when the predefined roles and rules do not match the needs of the organization authorization policy. The procedures in [Create Custom Role](#), [Change Custom Role](#), [Create Custom Rule](#), and [Change Custom Rule](#) provide further details on how to perform these operations.

The administrator can delete custom roles and custom rules when they are no longer needed by the organization authorization policy. The procedures in [Delete Custom Role](#) and [Delete Custom Rule](#) provide further details on how to perform these operations.

Note: Local authorization must be used to understand the default roles the product delivers, and using roles in assigning authorization for users. Customization of roles and rules are possible by adding extra roles over the default ones.

3 Rules for Default Roles

The detailed permissions for the default roles are described in the following tables. “Deny” indicates the default behavior when no permission rule is defined.



Table 3 Self-Permissions

MOM Fragment						Permission	Scope	
Managed Element						R	Only the MO but not the attributes (enables navigation in the ECLI)	
	System Functions							
		Backup and Restore Management				Deny	Not Applicable	
		Fault Management						
		File Management						
		License Management						
		Performance Management						
		Security Management				R	Only the MO but not the attributes (enables navigation in the ECLI)	
			User Management					
				LocalAuthenticationMethod				R for matching MO (=user id)
				AdministratorAccount				
					SshPublicKey		RWX	
				UserAccountM			R	Only the MO but not the attributes (enables navigation in the ECLI)
					UserAccount		R for matching MO (=user id)	
			SshPublicKey		RWX	The MO, its attributes, and actions		
		Software Inventory Management				Deny	Not Applicable	
		Software Management						
		System Management						
		Transport						
Equipment								



Table 4 LocalAuthenticationAdministrator Permissions

MOM Fragment				Permission	Scope		
Managed Element				R	Only the MO but not the attributes (enables navigation in the ECLI)		
	System Functions						
		Backup and Restore Management		Deny	Not Applicable		
		Fault Management					
		File Management					
		License Management					
		Performance Management					
		Security Management					
			User Management		R	Only the MO but not the attributes (enables navigation in the ECLI)	
				LocalAuthenticationMethod		RWX	The MO, its attributes, actions, and child MOs
				LocalAuthorizationMethod		R	The MO, its attributes, and child MOs
		Software Inventory Management		Deny	Not Applicable		
	Software Management						
	System Management						
	Transport						
	Equipment						



Table 5 System Administrator Permissions for Default Roles

MOM Fragment			Permission	Scope	
Managed Element			RWX	The MO, its attributes, and actions	
	System Functions			RWX	The MO, its attributes, actions, and child MOs
		Backup and Restore Management			
		Fault Management			
		License Management			
		Performance Management			
		File Management		FileGroup=InServicePerformance: R	
				FileGroup=SoftwareManagement : RWX	
		Security Management		R	Only the MO but not the attributes (enables navigation in the ECLI)
			Certificate Management	R	The MO, its attributes, actions, and child MOs
	Software Inventory Management		RW		
	Software Management		RWX		
	System Management				
	Transport		RWX	The MO, its attributes, and actions	
Equipment		Deny		Not Applicable	



Table 6 System Security Administrator Permissions for Default Roles

MOM Fragment			Permission	Scope	
Managed Element			R	Only the MO but not the attributes (enables navigation in the ECLI)	
	System Functions				
		Backup and Restore Management		Deny	Not Applicable
		Fault Management		R	The MO, its attributes, actions, and child MOs
		File Management		Deny	Not Applicable
		License Management			
		Performance Management			
		Security Management		RWX	The MO, its attributes, actions, and child MOs
			Certificate Management		
		Software Inventory Management		R	
		Software Management		Deny	Not Applicable
		System Management			
	Transport				
	Equipment				

Table 7 System Read-Only for Default Roles

MOM Fragment			Permission	Scope	
Managed Element			R	The MO, its attributes, and actions	
	System Functions			Deny	The MO, its attributes, actions, and child MOs
		Backup and Restore Management			
		Fault Management			
		File Management			
		License Management		R	The MO, its attributes, actions, and child MOs
		Performance Management			
		Security Management		Deny	Not Applicable
		Software Inventory Management		R	The MO, its attributes, actions, and child MOs
		Software Management		R	
		System Management			
	Transport		Deny	The MO, its attributes, and actions	
Equipment		Not Applicable			