

User Management

DESCRIPTION

Copyright

© Ericsson AB 2016–2019. 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 Authentication	3
1.3	User Authorization	4
1.4	Permission Types	4
1.5	Default Roles	5
1.6	Backup and Restore of Local User Data	6
2	Basic User Management Procedures	7
3	User Management-Related Alarms	13
4	Rules for Default Roles	15





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)

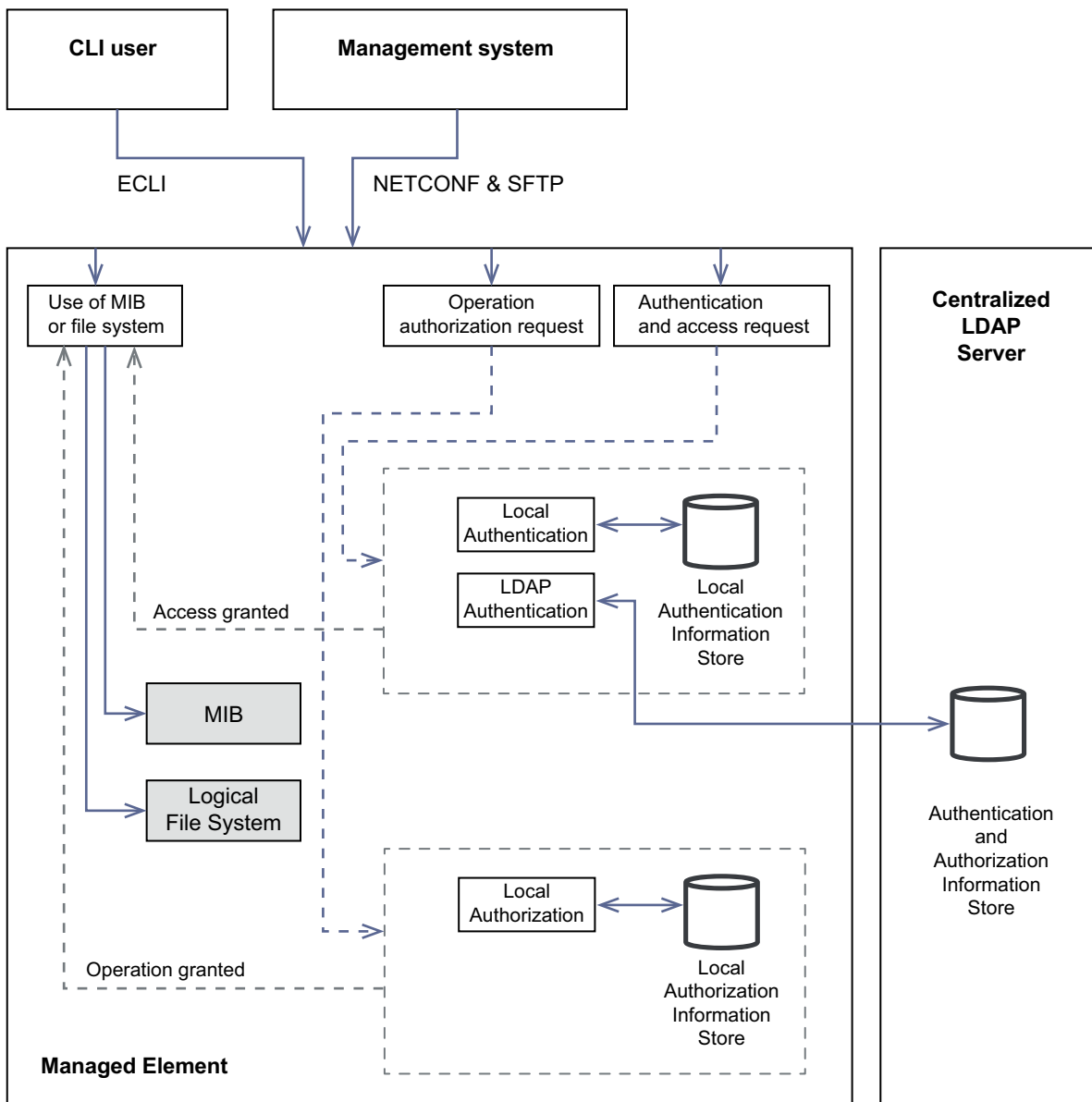


Figure 1 User Management Overview

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.

For more information on the LDAP interface, see [LDAP-Based Authentication and Authorization Interface](#).

The User Management managed area, `UserManagement`, can be found in the Managed Object Model (MOM). For general information about the MOM, Managed Object Classes (MOCs), cardinality, and related concepts, see [Managed Object Model User Guide](#).

1.2 User Authentication

The user initiates a session that triggers user authentication. User authentication is based on password or SSH public key. 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.

All authentication attempts, whether successful or not, are recorded in the ME security log.

For more information, see [Audit Information](#).

A successful user authentication triggers a user authorization.



1.3 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.

For LDAP, the ME performs additional checks whether the user can access the ME based on POSIX parameters (uidNumber) and TBAC attribute of the user account. For roles, three different LDAP profile filters are supported for search: flexible filter, POSIX groups filter, and Ericsson roles filter. The Ericsson roles profile filter is used together with the Ericsson Operations Support System (OSS) solution. If the Ericsson roles profile filter is used, the authorization can be selective based on the target type. In some networks, it can be required to let a user have different management roles on different MEs. For example, the network can span several countries, and it can be needed to let a user act as “admin” in one country, but only as “operator” in another. This function is part of the TBAC functionality.

To facilitate the management of LDAP user accounts, it is possible to create role alias objects in the LDAP server, to group different authorization roles, and that can be referred from individual user accounts. When the ME queries the user roles, it translates the alias roles found in the user account to the roles contained by the alias object. The roles that were found in the alias role are used by the ME for user authorization.

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 root user is not allowed to be used for Operations, Administration, and Maintenance (OAM) NBI activities. The operator needs to create users according to their needs, and assign different roles to them.

The ME supports some predefined roles, see Section 1.5 Default Roles on page 5. 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 1.4 Permission Types on page 4.

1.4 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.
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.

1.5 Default Roles

The ME supports several predefined default roles as described in Table 2. These roles and the corresponding rules cannot be modified. The detailed permissions for each role are described in Section 4 on page 15.

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

Table 2 Default Roles

Default Role	Description
CSCF Application Administrator	Responsible for the administration of all non-security-related attributes and capabilities of the CSCF Function, including features, configuration parameters, and monitoring.
CSCF Application Operator	Can view some non-security-related attributes and capabilities of the CSCF Function, including features, configuration parameters, and monitoring.



Table 2 Default Roles

Default Role	Description
CSCF Application Security Administrator	Responsible for the administration of all security-related attributes and capabilities of the CSCF Function user accounts and authorizations.
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.
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.
System Read Only	Can view most non-security-related attributes and capabilities of an ME, including features, configuration parameters, and monitoring.
System Security Administrator	Responsible for the administration of all security-related attributes and capabilities of an ME, including user accounts and authorizations.
System Troubleshooter	Responsible for troubleshooting-related activities, including backup and restore, file management, performance management, and viewing all non-security-related attributes and capabilities of an ME.

1.6 Backup and Restore of Local User Data

Information related to user accounts expires over time. Backup taken of configuration data could have been done at a time when different accounts were used. The users can have also changed their passwords after the configuration data backup. This can result in a state after restoration where the valid users before the backup restoration cannot access the ME after the restoration, because of expired passwords or invalid accounts, or can access the ME with different authorization.

It is strongly recommended to create a backup immediately after any change in the password of the administrator account. It is also recommended to create regular backups of User Account information frequently.

User account information classifies as system data in backup and restore procedures.



2 Basic User Management 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 see the appropriate documentation of the interface to learn if the legal notice is applicable.

- Change Login 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 keys. 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 provide the access to control 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 be also 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 Authentication

— 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 MIB 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 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

LDAP authorization to get roles needs an authorization filter to be set up.

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 for performing these operations.

The Ericsson LDAP filter has two incompatible versions, version 1 and version 2, each describing different ME authorization behavior. 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.

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

The differences between version 1 and version 2 are described in detail in [LDAP-Based Authentication and Authorization Interface](#).

The procedure in [Configure Ericsson Filter Version](#) provides further details on how to perform this operation.

— Configure TLS for LDAP

The administrator needs to install certificates for TLS. For server only authentication, a trust category is required; for mutual authentication, a node



credential must also be deployed. For the information on how to deploy certificates, see [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.

It is possible that the administrator needs 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.

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, see [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, the ME must be able to find the LDAP base DN where the alias objects reside. The LDAP base DN needs to be configured. To configure role alias objects in the LDAP server and for the description of the corresponding role resolution logic, see [LDAP-Based Authentication and Authorization Interface](#).

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

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.



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 User Management-Related Alarms

Table 3 User Management-Related Alarms

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





4 Rules for Default Roles

The detailed permissions for the default roles are described in Table 4 to Table 18. “Deny” indicates the default behavior when no permission rule is defined.



Table 4 Self-Permissions

MOM Fragment					Permissi on	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						
				AdministratorAccount			R for matchi ng MO (=user id)		
					SshPublicKey		RWX	The MO, its attributes, and actions	
					UserAccountM		R	Only the MO but not the attributes (enables navigation in the ECLI)	
				UserAccount			R for matchi ng MO (=user id)		
					SshPublicKey		RWX	The MO, its attributes, and actions	
		Software Inventory Management			Deny	Not Applicable			
		Software Management							
		System Management							
	Transport								
Equipment									



Table 5 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	R	Only the MO but not the attributes (enables navigation in the ECLI)
	User Management		
	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 6 System Administrator Permissions for Default Roles

MOM Fragment			Permission	Scope		
Managed Element				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				
		Log Management			The MO, its attributes, and actions	
	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				
	Software Inventory Management			RW	The MO, its attributes, actions, and child MOs	
	Software Management			RWX		
	System Management					
	Transport				The MO, its attributes, and actions	
Equipment			Deny	Not Applicable		



Table 7 System Read-Only for Default Roles

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



Table 8 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		
	Log Management	R	The MO and its attributes
	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 9 System Troubleshooter Permissions for Default Roles

MOM Fragment		Permission	Scope
Managed Element		R	The MO, its attributes, actions, and child MOs



MOM Fragment		Permission	Scope
	CSCF Functions	RWX	The MO, its attributes, actions, and child MOs
	System Functions	R	The MO, its attributes, actions, and child MOs
	Backup and Restore Management	RWX	The MO, its attributes, actions, and child MOs
	Fault Management	R	The MO, its attributes, actions, and child MOs
	File Management	RWX	The MO, its attributes, actions, and child MOs
	License Management	R	The MO, its attributes, actions, and child MOs
	Performance Management	RWX	The MO, its attributes, actions, and child MOs
	Security Management	R	The MO, its attributes, actions, and child MOs
	Certificate Management		
	Software Inventory Management		
	Software Management	RWX	The MO, its attributes, actions, and child MOs
	System Management	R	The MO, its attributes, actions, and child MOs
	Transport	RWX	The MO, its attributes, actions, and child MOs
	Equipment	R	The MO, its attributes, actions, and child MOs

Table 10 CSCFApplicationAdministrator Permissions

MOM Fragment	Permission	Scope
Managed Element	R	Only the MO but not the attributes (enables navigation in the ECLI)



MOM Fragment		Permission	Scope
	CSCF Function	RWX	The MO, its attributes, actions, and child MOs
	System Functions	R	Only the MO but not the attributes (enables navigation in the ECLI)
	Backup and Restore Management	RWX	The MO, its attributes, actions, and child MOs
	Fault Management	R	
	File Management	R	Only the MO but not the attributes (enables navigation in the ECLI)
	Logical FS	R	
	FileGroup Policy	RWX	The MO, its attributes, actions, and child MOs
	Performance Management	RWX	
	Software Inventory Management	R	
	Software Management	R	SwM,* The MO, its attributes, actions, and child MOs
		RWX	SwM,UpgradePackage,* The MO, its attributes, actions, and child MOs



Table 11 CSCFApplicationSecurityAdministrator Permissions

MOM Fragment			Permission	Scope
Managed Element			R	Only the MO but not the attributes (enables navigation in the ECLI)
System Functions			R	
		Fault Management	R	The MO, its attributes, actions, and child MOs
		File Management	R	Only the MO but not the attributes (enables navigation in the ECLI)
		Logical FS	R	
		FileGroup Policy	RWX	The MO, its attributes, actions, and child MOs
		Security Management	R	SecM The MO, its attributes, actions, and child MOs
			RWX	SecM,UserManagement,LocalAuthorizationMethod,Role=CSCF_Application_Administrator,* The MO, its attributes, actions, and child MOs
			RWX	SecM,UserManagement,LocalAuthorizationMethod,Role=CSCF_Application_Operator,* The MO, its attributes, actions, and child MOs
		Security Management	RWX	SecM,UserManagement,LocalAuthorizationMethod,Role=CSCF_Application_Security_Administrator,* The MO, its attributes, actions, and child MOs
		Software Inventory Management	R	The MO, its attributes, actions, and child MOs



Table 12 CSCFApplicationOperator Permissions

MOM Fragment		Permission	Scope
Managed Element		R	Only the MO but not the attributes (enables navigation in the ECLI)
	CSCF Function	R	The MO, its attributes, actions, and child MOs
	System Functions	R	Only the MO but not the attributes (enables navigation in the ECLI)
	Fault Management	R	The MO, its attributes, actions, and child MOs
	File Management	R	Only the MO but not the attributes (enables navigation in the ECLI)
	Logical FS	R	
	FileGroup Policy	R	The MO, its attributes, actions, and child MOs
	Software Inventory Management	R	
	Software Management	R	

For the CSCF, the default application roles from Table 10 to Table 12 are applied for File Management when an OAM user accesses these directories exposed by the SFTP protocol.

The directories with access permissions assigned to the default roles LocalAuthenticationAdministrator, SystemAdministrator, and SystemSecurityAdministrator are listed in Table 13 to Table 15 respectively.

The directories with access permissions assigned to the roles CSCFApplicationAdministrator and System Troubleshooter are listed in Table 16.

The directories with access permissions assigned to the CSCF roles CSCFApplicationSecurityAdministrator and CSCFApplicationOperator are listed in Table 17 to Table 18 respectively.

Table 13 LocalAuthenticationAdministrator Permissions in File Management Directories

Directories in File Management	Permission ⁽¹⁾
AlarmLogs	Deny
AlertLogs	Deny
BackupAndRestoreManagementFiles	Deny
Cscf	Deny



Directories in File Management	Permission ⁽¹⁾
InServicePerformance	Deny
PerformanceManagementReportFiles	Deny
SoftwareManagement	Deny

(1) Permission is applied on the directory and its all subdirectories.

Table 14 SystemAdministrator Permissions in File Management Directories

Directories in File Management	Permission ⁽¹⁾
AlarmLogs	RWX
AlertLogs	RWX
BackupAndRestoreManagementFiles	Deny
Cscf	Deny
InServicePerformance	R
PerformanceManagementReportFiles	RWX
SoftwareManagement	RWX

(1) Permission is applied on the directory and its all subdirectories.

Table 15 SystemSecurityAdministrator Permissions in File Management Directories

Directories in File Management	Permission ⁽¹⁾
AlarmLogs	R
AlertLogs	R
BackupAndRestoreManagementFiles	Deny
Cscf	Deny
InServicePerformance	Deny
PerformanceManagementReportFiles	Deny
SoftwareManagement	Deny

(1) Permission is applied on the directory and its all subdirectories.

Table 16 CSCFApplicationAdministrator and System Troubleshooter Permissions in File Management Directories

Directories in File Management	Permission ⁽¹⁾
AlarmLogs	RWX
AlertLogs	RWX
BackupAndRestoreManagementFiles	RWX
Cscf	RWX



Directories in File Management	Permission ⁽¹⁾
InServicePerformance	Deny
PerformanceManagementReportFiles	RWX
SoftwareManagement	RWX

(1) Permission is applied on the directory and its all subdirectories.

Table 17 CSCFApplicationSecurityAdministrator Permissions in File Management Directories

Directories in File Management	Permission ⁽¹⁾
AlarmLogs	R
AlertLogs	R
BackupAndRestoreManagementFiles	Deny
Cscf	Deny
InServicePerformance	Deny
PerformanceManagementReportFiles	Deny
SoftwareManagement	R

(1) Permission is applied on the directory and its all subdirectories.

Table 18 CSCFApplicationOperator Permissions in File Management Directories

Directories in File Management	Permission ⁽¹⁾
AlarmLogs	R
AlertLogs	R
BackupAndRestoreManagementFiles	R
Cscf	R
InServicePerformance	Deny
PerformanceManagementReportFiles	R
SoftwareManagement	R

(1) Permission is applied on the directory and its all subdirectories.

For more detailed information, for example how to view RuleId for a specific Rule, see [View Roles and Rules](#).