

Local Authentication Management

DESCRIPTION

Copyright

© Ericsson AB 2015, 2016. 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	Functions and Concepts	3
2.1	Types of Operations	9
3	Managed Object Model	13
4	Configuration Management	15
5	Fault Management	17





1 Introduction

This document provides an overview of the management model and concepts associated with the Local Authentication managed area.

A managed area is represented by a group of Managed Object Classes (MOCs) within the Managed Object Model (MOM).





2 Functions and Concepts

The Local Authentication provides a management interface to manage a standalone authentication service for Operation and Maintenance (O&M) access in the Managed Element (ME) that does not rely on a data store external to the ME.

Local Authentication Administrator role, System Security Administrator role, or a similar customer-specific role, is required for the operations described in this document.

Basic Concepts

- O&M User Account

The association of an O&M User with an identity. It includes the username and password for identification and authentication.

- O&M User

One who interacts with the ME. It is either a human or an automated process, for example, in the Management System. In Access Control terminology, this is called Subject.

- Role

A role is a set of authorization rules to define access permissions.

- LocalAuthenticationAdministrator Role

The role `LocalAuthenticationAdministrator` can be attached to an O&M user account. That account is then allowed to manage the user accounts configured under the Local Authentication MOM fragment. Such an account becomes an administrator account of the Local Authentication managed area, and is also referred as "administrator" in this document.

The rules connected to this role can be found from the `LocalAuthenticationAdministrator` instance of *Role* under the *LocalAuthorizationMethod* MO.

This role gives the O&M user account full access to the *LocalAuthenticationMethod* MO and all its child MOs.

- Self Role

The role `Self` is automatically applied to an O&M user account then that account is allowed partially to manage the own *UserAccount* instance under the *UserAccountM* MO. The role `Self` is not visible in the attribute `roles` in the *UserAccount* MO.



The rules connected to this role can be found from the `Self` instance of *Role* under the *LocalAuthorizationMethod* MO.

This role gives rights for O&M user account to create, change, and delete only the *SshPublicKey* MO under the user's own *UserAccount*.

- Key-based SSH Login

This is a Secure Shell (SSH) user login without password using an SSH private and public key pair. The public key of the user is stored to the ME and a corresponding private key is used by the user instead of password when logging in.

O&M Accounts

The Local Authentication model classifies O&M user accounts in the following two categories:

- User account

This account type is used for the users that operate normal O&M activities and commands.

- Administrator account

This account type is used for creating Local Authentication users and for giving them sufficient roles to continue system recovery from a fault situation. The ME raises alarm *Local Authentication, Authentication Failure Limit Reached* when wrong password is repeatedly given, for example, during malicious attack.

The system creates one such an account by default and this is represented by the *AdministratorAccount* MO.

Account Policy

Account policy holds non-password related properties of the O&M user accounts.

If an account has not been used for a long time, the system determines the account to be dormant and locks the account, based on the settings in the account policy. To enable such an account, action `unlockOperationalLock` is required.

The O&M user account state diagram for password policy is shown in Figure 1. The states are described in Table 1 and the transitions in Table 2.

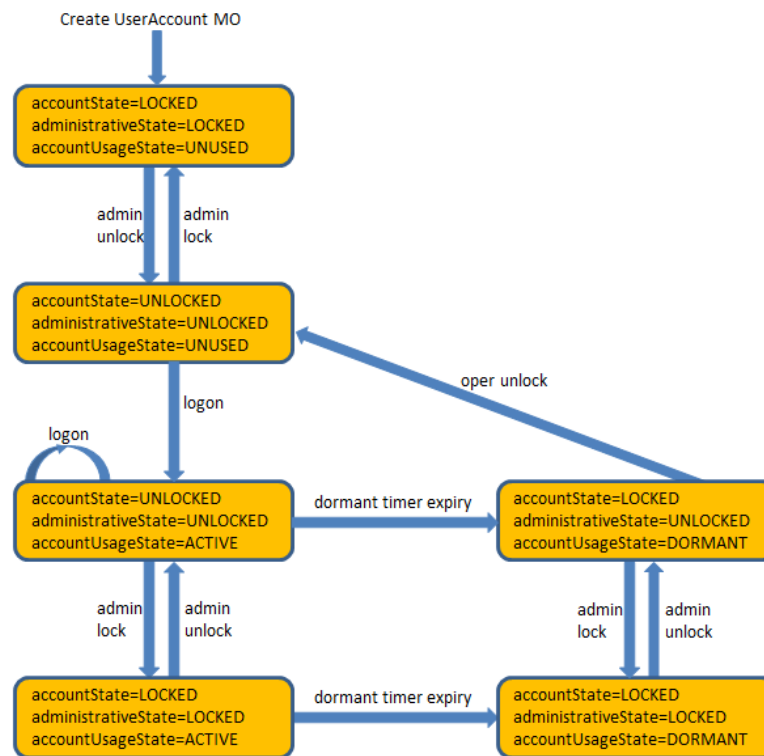


Figure 1 Account Policy State Transitions

Table 1 States for Account Policy Transitions

State	Description
accountState = LOCKED	The account is locked. The user cannot authenticate to this account.
accountState = UNLOCKED	The account is unlocked. The user can authenticate to this account.
administrativeState = LOCKED	Locked administrative state.
administrativeState = UNLOCKED	Unlocked administrative state.
accountUsageState = UNUSED	The account is unused. No successful authentication has been performed to the account.
accountUsageState = ACTIVE	The account is active based on the configured account policy threshold. At least one successful authentication has been made to the account.
accountUsageState = DORMANT	The account is dormant based on the configured account policy threshold. The system time passes the value of attribute <code>lastLoginTime</code> plus the value of attribute <code>dormantTimer</code> , thus indicating lock because of account inactivity. The account gets locked by changing attribute <code>accountState</code> to LOCKED.



Table 2 Account Policy Transitions

Transition	Description
admin lock	According to the procedure in <i>Lock User Account Administratively</i> .
admin unlock	According to the procedure in <i>Unlock Administrative Lock for User Account</i> .
dormant timer expiry	The account has not been used for a long time, the account becomes dormant, and the account becomes locked.
logon	The user logs on to the account.
oper unlock	According to the procedure in <i>Unlock Operational Lock for User Account</i> .

Password Policy

Password management policies help to achieve secure and strong passwords. Several password policy instances are supported, thus giving possibility to create different O&M user account types, based on operator policies. Password policy helps to lock an account if the configured limits indicate a possible threat of password cracking. Selection of strong passwords is also important to improve the resistance of passwords against guessing and brute-force attacks. The same password quality setting is applied to all accounts.

For protection against old passwords, the policies lock an account that has expired credentials. Password expiry is followed by a grace period when the user is enforced to change password. If the grace period is over and the password is not changed, an automatic operational lock is placed on the account.

The O&M user account state diagram for password policy is shown in Figure 2. The states are described in Table 3 and the transitions in Table 4.

Note: Figure 2 does not show the state transitions caused by the `removePassword` action (`removePw`), see Table 4.

Figure 2 The Most Common Password Policy State Transitions

Table 3 States for Password Policy Transitions

State	Description
accountState = LOCKED	<p>The account is locked. The user cannot authenticate to this account.</p> <p>In case the account has been locked because of too many failed login attempts, the <code>resetPassword</code> action unlocks the account immediately and no additional unlock operation is required.</p>
accountState = UNLOCKED	The account is unlocked. The user can authenticate to this account.
administrativeState = LOCKED	Locked administrative state.
administrativeState = UNLOCKED	Unlocked administrative state.
passwordState = uninitiated	<p>The password is not initiated by action <code>resetPassword</code> after creating the account. Thus, no password is set.</p> <p>If the action <code>removePassword</code> is executed, it also resets the <code>passwordState</code> to uninitiated state.</p>
passwordState = VALID	The password is valid based on system time, password changed time, and aging policy.



Table 3 States for Password Policy Transitions

State	Description
passwordState = EXPIRED_MUSTCHANGE	The password has expired based on system time, password changed time, and aging policy. The user is forced to change password at next logon. After a grace period, the state turns to EXPIRED and accountState becomes LOCKED.
passwordState = EXPIRED	The password has expired based on system time, password changed time, and aging policy. The password must be reset by action resetPassword.

Table 4 Password Policy Transitions

Transition	Description
admin lock	According to the procedure in <i>Lock User Account Administratively</i> .
admin unlock	According to the procedure in <i>Unlock Administrative Lock for User Account</i> .
failure threshold	The account becomes locked because of too many failed logon attempts.
oper unlock, unlock timer	According to the procedure in <i>Unlock Operational Lock for User Account</i> .
pw expiry, resetPw	The password has expired. The user is forced to change password at the next logon.
pw grace period expiry	The account becomes locked because the user did not change the password before the grace period expired.
resetPw	<p>According to the procedure in <i>Reset Password for User Account</i>.</p> <p>If the noChange parameter was provided, the passwordState is always set to VALID and no forced password change is required. This is recommended for machine to machine -type of accounts only. The password is still expiring according to the password policy set, only the initial password change is omitted.</p>



Table 4 Password Policy Transitions

Transition	Description
removePw	<p>According to the procedure in <i>Remove Password from User Account</i>.</p> <p>This transition removes the password from the account and clears the <code>passwordState</code> value to <code>uninitiated</code>.</p> <p>The password is recommended to be removed when <i>SshPublicKey</i> MO is defined and SSH Key based authentication is the only authentication method expected to be used for the account (to avoid password expiration and account becoming locked).</p>
user pw change	The user changes password.

SSH Public Key

SSH Public Key represents the stored SSH public key for O&M User Account or Administrator Account for key-based SSH login.

The user is allowed to create, change, and delete the user's own *SshPublicKey* MO based on the role `Self`, see Basic Concepts. If the user password is removed with action `removePassword` and the *SshPublicKey* MO is deleted, the user cannot relogin before the administrator has reset the password.

Successful public key authentication requires the account to be in `UNLOCKED` state. If an SSH public key is set and password authentication is not expected to be used, it is recommended to remove the password. Otherwise, the expiry of the password blocks the account from any type of authentication attempts.

2.1 Types of Operations

The Local Authentication supports the following operations:

Manage O&M User Accounts

- Create, change, and delete user account

An O&M user account can be created and changed. It includes username and password 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.

- Create, change, and delete account policy

An account policy for a user account can be created and changed. 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 selected to prevent from brutal password attacks. The procedure in *Change Password Quality Configuration* provides further details on how to perform this operation.

- Create, change, and delete SSH public key

An SSH public key for O&M user or administrator can be created and changed. It includes an SSH public key value used for key-based SSH login. The procedures in *Create SSH Public Key*, *Change SSH Public Key*, and *Delete SSH Public Key* 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

If the user account has the SSH public key set and used only with the key-based SSH Login, a remove password operation is recommended to be performed by the administrator, see Basic Concepts. The procedure in *Remove Password from User Account* provides further details on how to perform this operation.

- Set user account roles

A user account is assigned with roles to provide the access to control the node resources. The procedure in *Set User Roles for User Account* provides further details on how to perform this operation.

- Lock and unlock user account

The administrator can lock and unlock the user account. The procedures in *Lock User Account Administratively* and *Unlock Administrative Lock for User Account* provide further details on how to perform these operations. A user account can also be locked by system, which can be unlocked by administrator. The procedure in *Unlock Operational Lock for User Account* provides further details on how to perform this operation.



Manage O&M Administrator Account

- Change administrator account

Administrator account attributes can be updated when authentication to regular O&M accounts is not accessible. The procedure in *Change Administrator Account* provides further details on how to perform this operation.



3 Managed Object Model

The Local Authentication managed area is represented in the *Managed Object Model (MOM)* as follows:

```
ManagedElement
+-SystemFunctions
+-SecM
+-UserManagement
+-LocalAuthenticationMethod
+-AccountPolicy
+-AdministratorAccount
+-SshPublicKey
+-PasswordPolicy
+-PasswordQuality
+-UserAccountM
+-UserAccount
+-SshPublicKey
```

For general information about the MOM, MOCs, Managed Objects (MOs), cardinality, and related concepts, refer to *Managed Object Model User Guide*.

The Local Authentication MOCs are described in Table 5.

Table 5 The Local Authentication Managed Object Class Descriptions

Managed Object Class	Description
<i>LocalAuthenticationMethod</i>	The root MOC of the Local Authentication.
<i>AccountPolicy</i>	Handles properties of account policy.
<i>AdministratorAccount</i>	Used for initial and recovery scenarios when authentication to regular O&M accounts is inaccessible.
<i>PasswordPolicy</i>	Handles properties of password policy.
<i>PasswordQuality</i>	Handles the criteria of password quality checking.
<i>UserAccountM</i>	Defines and handles the management of O&M user accounts.
<i>UserAccount</i>	Represents a user account. The O&M users must authenticate to a <i>UserAccount</i> MO to access the ME.
<i>SshPublicKey</i>	Represents an SSH public key for a user or administrator account.





4 Configuration Management

The Local Authentication is accessed using NETCONF or the Ericsson Command-Line Interface (ECLI) to manipulate the Management Information Base (MIB).

The following operations can be performed for the O&M User Account and Administrator Account using the ECLI and are described in the Operating Instructions:

Manage O&M User Accounts

- *Create User Account*
- *Change User Account*
- *Delete User Account*
- *Create Account Policy*
- *Change Account Policy*
- *Delete Account Policy*
- *Create Password Policy*
- *Change Password Policy*
- *Delete Password Policy*
- *Create SSH Public Key*
- *Change SSH Public Key*
- *Delete SSH Public Key*
- *Change Password Quality Configuration*
- *Reset Password for User Account*
- *Remove Password from User Account*
- *Set User Roles for User Account*
- *Lock User Account Administratively*
- *Unlock Administrative Lock for User Account*
- *Unlock Operational Lock for User Account*



Manage O&M Administrator Account

- *Change Administrator Account*



5 Fault Management

The Local Authentication alarm is described in Table 6.

Table 6 The Local Authentication Alarm

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