

Set User Roles for User Account

OPERATING INSTRUCTIONS

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
1.1	Prerequisites	1
2	Procedure	3





1 Introduction

This document describes how to configure roles for a local Operation and Maintenance (O&M) user account. Roles are used to control which parts of the node resources the local user is allowed to access.

The roles supported by the system are defined as Managed Objects (MOs) under the *LocalAuthorizationMethod* MO. The roles configured in the user account are used to fetch users access rights from the appropriate *Role* MOs or *CustomRole* MOs.

User authorization is activated by unlocking the *LocalAuthorizationMethod* MO.

Note: After authorization activation all users, not only users defined in the Local Authentication MO are subject for authorization. If proper user configuration is not made, then access to Ericsson Command-Line Interface (ECLI) is not possible.

1.1 Prerequisites

This section describes the prerequisites, which must be fulfilled before using the procedure.

1.1.1 Conditions

The following conditions must apply:

- The user has sufficient access rights to perform the task, for example, the user has System Security Administrator role.
- An ECLI session in Exec mode is in progress.
- The username for the local user account is known. In this document, username is `joedoe`.
- The role names to be assigned to the user are known. In this document, the role names `SystemAdministrator` and `EricssonSupport` are used as examples.





2 Procedure

To set user roles:

1. Navigate to the *LocalAuthorizationMethod* MO, for example:

```
>dn ManagedElement=NODE06ST,SystemFunctions=1,SecM=1,UserManagement=1,LocalAuthorizationMethod=1
```

2. List the roles defined in the system:

```
(LocalAuthorizationMethod=1) >show
```

The following is an example output:

```
LocalAuthorizationMethod=1
  administrativeState=UNLOCKED
  CustomRole=Custom_UserAdministrator
  Role=EricssonSupport
  Role=SystemAdministrator
  Role=SystemSecurityAdministrator
  Role=LocalAuthenticationAdministrator
```

3. Navigate to the *UserAccount* MO, for example:

```
>dn ManagedElement=NODE06ST,SystemFunctions=1,SecM=1,UserManagement=1,LocalAuthenticationMethod=1,UserAccountM=1,UserAccount=johndoe
```

4. Enter Config mode:

```
(UserAccount=johndoe) >configure
```

5. Set the appropriate role names for the user, for example:

```
(config-UserAccount=johndoe) > roles=["SystemAdministrator","EricssonSupport"]
```

6. Commit the settings:

```
(config-UserAccount=johndoe) >commit
```

7. Verify the settings, for example:

```
(UserAccount=johndoe) >show -v
```

The following is an example output:



```
UserAccount=joedoe
  accountPolicy="ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, =>
UserManagement=1, LocalAuthenticationMethod=1, AccountPolicy=1"
  accountState=LOCKED <read-only>
  accountUsageState=UNUSED <read-only>
  administrativeState=LOCKED <default>
  lastLoginTime="" <read-only>
  lockedTime="2015-11-13T11:20:24Z" <read-only>
  passwordChangedTime="" <read-only>
  passwordFailureTimes=[] <empty> <read-only>
  passwordPolicy="ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, =>
UserManagement=1, LocalAuthenticationMethod=1, PasswordPolicy=1"
  passwordState=[] <empty> <read-only>
  roles
    "SystemAdministrator"
    "EricssonSupport"
  userAccountId="joedoe"
  userLabel=[] <empty>
  userName="John M. Doe"
```