

Create User Account

OPERATING INSTRUCTIONS

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	Description	1
2	Procedure	1
2.1	Create User Account	1
	Reference List	5



Create User Account



1 Description

This document describes how to create a local Operation and Maintenance (O&M) user account.

2 Procedure

2.1 Create User Account

Prerequisites

- No documents are required.
- No tools are required.
- The following conditions must apply:
 - The user has sufficient access rights to perform the task, for example, the user has System Security Administrator role.
 - The user is familiar with the security policy of the organization.
 - An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.
 - The password policy is known.
 - The account policy is known.
 - The username (logon ID) for the new local user account is known. In this instruction, the username is joedoe.

Steps

1. Navigate to the `UserAccountM` Managed Object (MO), for example:

```
>dn ManagedElement=NODE06ST,SystemFunctions=1,SecM=1,UserManagement=1,LocalAuthenticationMethod=1,UserAccountM=1
```
2. Verify that no user account for username joedoe exists, for example:

```
(UserAccountM=1)>show UserAccount=joedoe
```



```
ERROR: Specific element not found
```



ECLI command for MO creation is identical to the ECLI command for changing the ECLI position to an existing MO. Therefore it is important to verify the uniqueness of the username before creation.

3. Enter Config mode:

```
(UserAccountM=1)>configure
```

4. Create the `UserAccount` MO, for example:

```
(config-UserAccountM=1)>UserAccount=joedoe
```

Note: joedoe is the username used at logon.

Do not use any personal or sensitive data as username.

5. Set the account policy for the account by giving a reference to the appropriate `AccountPolicy` MO, for example:

```
(config-UserAccount=joedoe)>accountPolicy="ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, UserManagement=1, LocalAuthenticationMethod=1, AccountPolicy=1"
```

Note: Ensure that the corresponding account policy `ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, UserManagement=1, LocalAuthenticationMethod=1, AccountPolicy=1` already exists. Otherwise, refer to Create Account Policy to create it.

6. Set the password policy for the account by giving a reference to the appropriate `PasswordPolicy` MO, for example:

```
(config-UserAccount=joedoe)>passwordPolicy="ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, UserManagement=1, LocalAuthenticationMethod=1, PasswordPolicy=1"
```

Note: Ensure that the corresponding password policy `ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, UserManagement=1, LocalAuthenticationMethod=1, PasswordPolicy=1` already exists. Otherwise, refer to Create Password Policy to create it.

7. Set the full name of the user assigned to the account, for example:

```
(config-UserAccount=joedoe)>userName="John M. Doe"
```

Note: This attribute contains a descriptive name of the user, not the logon ID.

Do not use any personal or sensitive data, other than user real name in this attribute.

8. Commit the settings:

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



9. Is Role Based Access Control used to control user access privileges?

Yes: Unlock the local authorization methods, refer to [Unlock Local Authorization Method](#). Assign roles to the user, refer to [Set User Roles for User Account](#). Proceed with the next step.

No: Lock the local authorization methods, refer to [Lock Local Authorization Method](#). All users are authorized for any Managed Object Model (MOM) operation. Proceed with the next step.

10. Is SSH public key used for authentication?

Yes: Create SSH public key, refer to [Create SSH Public Key](#). Proceed with the next step.

No: Proceed with the next step.

Note: It is recommended to use SSH public key for authentication.

11. Is password-based authentication used?

Note: If SSH public key is used for authentication, it is not recommended to use password-based authentication.

Yes:

- a. Enter Config mode:

```
(UserAccountM=1)>configure
```

- b. Enter the user account:

```
(config-UserAccountM=1)>UserAccount=joedoe
```

- c. Set the password policy for the account by giving a reference to the appropriate [PasswordPolicy](#) MO, for example:

```
(config-UserAccount=joedoe)>passwordPolicy="ManagedElement=NODE06ST,SystemFunctions=1,SecM=1,UserManagement=1,LocalAuthenticationMethod=1,PasswordPolicy=1"
```

- d. Commit the settings:

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

- e. Assign a password for the user, refer to [Reset Password for User Account](#). Proceed with next step.

No: Proceed with next step.

12. Verify the settings, for example:

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



The following is an example output:

```
UserAccount=joedoe
  accountPolicy="ManagedElement=NODE06ST,⇒
SystemFunctions=1,SecM=1,UserManagement=1,⇒
LocalAuthenticationMethod=1,AccountPolicy=1"
  accountState=UNLOCKED <read-only>
  accountUsageState=UNUSED <read-only>
  administrativeState=UNLOCKED
  lastLoginTime="" <read-only>
  lockedTime="" <read-only>
  passwordChangedTime="20151110161432Z" <read-only>
  passwordFailureTimes=[] <empty> <read-only>
  passwordPolicy="ManagedElement=NODE06ST,⇒
SystemFunctions=1,SecM=1,UserManagement=1,⇒
LocalAuthenticationMethod=1>PasswordPolicy=1"
  passwordState=EXPIRED_MUSTCHANGE <read-only>
  roles
    "SystemAdministrator"
    "EricssonSupport"
  userAccountId="joedoe"
  userLabel=[] <empty>
  userName="John M. Doe"
```




Reference List

- [1] Create Account Policy
- [2] Create Password Policy