

Reset Password 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



Reset Password for User Account



1 Introduction

This document describes how the administrator can reset password for a local Operation and Maintenance (O&M) user account.

Local user password must be reset when the user account has been locked, for example, because of password expiry. The password reset does not automatically unlock the user account; a separate unlock operation must be performed after the password reset.

In case the account has been locked because of too many failed login attempts, the password reset unlocks the account immediately and no additional unlock operation is required.

The system forces the user to update their password when it has been reset by administrator.

For Machine to Machine -type of accounts, it is possible to disable the forced password change at first login. This alternative is recommended only for M2M interactions.

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 Local Authentication Administrator role.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.
- The username for the local user account is known. In this document, username is `j_oedoe`.
- The administrator has constructed a new password for user `j_oedoe` according to settings in the *PasswordQuality* Managed Object (MO) and *PasswordPolicy*MO.





2 Procedure

To reset a password for a local O&M user account:

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

```
>dn ManagedElement=NODE06ST, SystemFunctions=1, SecM=1
, UserManagement=1, LocalAuthenticationMethod=1, UserAc
countM=1
```

2. Select user account, for example:

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

3. Reset the password:

```
(UserAccount=joedoe) >resetPassword --password
```

Enter password: <password>

```
(UserAccount=joedoe) >resetPassword --password *****
```

Note: For Machine to Machine -type of accounts, to disable the forced password change at first login, provide the `noChange` parameter before the `password` parameter:

```
(UserAccount=joedoe) >resetPassword --noChange
--password
```

Enter password: <password>

```
(UserAccount=joedoe) >resetPassword --password
*****
```

The password will still expire according to the password policy set, only the initial password change is omitted.

4. Verify that the password change time has been updated with current time, for example:

```
(UserAccount=joedoe) >show passwordChangedTime
```

```
passwordChangedTime="2015-01-19T12:31:59Z"
```

5. Verify that the user is forced to change the password at next logon, for example:

```
(UserAccount=joedoe) >show passwordState
```

The following is an example output:



```
passwordState=EXPIRED_MUSTCHANGE
```

Note: If the forced password change was disabled with `noChange` parameter, the following is an example output:

```
passwordState=VALID
```