

Local Authentication, Authentication Failure Limit Reached

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2015, 2017. 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	Alarm Description	1
2	Procedure	1
2.1	Handle Alarm Local Authentication, Authentication Failure Limit Reached	1



Local Authentication, Authentication Failure Limit Reached



1 Alarm Description

The alarm is issued when the authentication failure limit is reached for the Administrator account. A password cracking attack is suspected.

Table 1 Local Authentication, Authentication Failure Limit Reached Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
Several consecutive failed logon attempts for the Administrator account.	The number of failed logon attempts on Administrator account exceed the threshold passwordMaxFailure within the time interval passwordFailureCountInterval.	Someone is trying to log on to Administrator account with wrong user credentials.	Administrator account	Unallowed access to the Administrator account.

2 Procedure

2.1 Handle Alarm Local Authentication, Authentication Failure Limit Reached

Prerequisites

- No documents are required.
- No tools are required.
- The following conditions must apply:
 - The alarm is raised.
 - The user has sufficient access rights to perform the task, for example, the user has system security administrator role, and root privileges to access operating system logs.
 - An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.

Steps

1. Navigate to the `AdministratorAccount` managed object given in the alarm, for example:



```
>dn ManagedElement=NODE06ST,SystemFunctions=1,SecM=1,UserManagement=1,LocalAuthenticationMethod=1,AdministratorAccount=la-admin
```

2. Check how many failed attempts have been made to the Administrator account during the passwordFailureCountInterval:

```
(AdministratorAccount=la-admin)>show -r passwordFailureTimes
```

The following is an example output:

```
AdministratorAccount=la-admin
passwordFailureTimes
  "2015-02-02T17:15:02Z"
  "2015-02-03T13:47:53Z"
  "2015-02-03T13:53:28Z"
  "2015-02-03T13:55:16Z"
  "2015-02-03T13:59:03Z"
  "2015-02-03T14:03:17Z"
  "2015-02-03T14:04:18Z"
  "2015-02-03T14:06:27Z"
```

Note: Successful authentication to the AdministratorAccount clears the passwordFailureTimes list.

3. Provide the information to the security organization.
4. Clear the alarm:

```
(AdministratorAccount=la-admin)>clearFailedAuthenticationAlarm
```

5. Job is completed.