

Local Authentication, Authentication Failure Limit Reached

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2015. 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	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	2



Local Authentication, Authentication Failure Limit Reached



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

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

The possible alarm causes and the corresponding fault reasons, fault locations, and impacts are described in Table 1.

Table 1 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 <code>passwordMaxFailure</code> within the time interval <code>passwordFailureCountInterval</code> .	Someone is trying to log on to Administrator account with wrong user credentials.	Administrator account	Unallowed access to the Administrator account.

The alarm attributes are listed and explained in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	6946820
Managed Object Class	<i>AdministratorAccount</i>
Managed Object Instance	<code>ManagedElement=<node_name>, SystemFunctions=1, SecM=1, UserManagement=1, LocalAuthenticationMethod=1, AdministratorAccount=<user ID></code>
Specific Problem	Local Authentication, Authentication Failure Limit Reached
Event Type	<code>securityServiceOrMechanismViolation (10)</code>
Probable Cause	<code>x736AuthenticationFailure (401)</code>



Table 2 Alarm Attributes

Attribute Name	Attribute Value
Additional Text	The authentication failure limit is reached based on the configured threshold. A password attack is suspected that should be isolated from the ME.
Perceived Severity	Warning (6)

1.2 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedure.

1.2.1 Documents

Not applicable.

1.2.2 Tools

No tools are required.

1.2.3 Conditions

Before starting this procedure, ensure that the following conditions are met:

- A Local Authentication, Authentication Failure Limit Reached 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.

2 Procedure

This section describes the procedure to follow when this alarm is received.



Do the following:

1. Navigate to the *AdministratorAccount* Managed Object (MO) given in the alarm, for example:

```
>dn ManagedElement=NODE06ST, SystemFunctions=1, Sec
M=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 passwordFail
ureTimes
```

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) >clearFailedAuthenticat
ionAlarm
```

5. Job is completed.