

# Security, OAM User Gaining Privilege Failed Ericsson Centralized User Database

---

## OPERATING INSTRUCTION

**Copyright**

© Ericsson AB 2016-2018. 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

|          |                       |          |
|----------|-----------------------|----------|
| <b>1</b> | <b>Introduction</b>   | <b>1</b> |
| 1.1      | Alarm Description     | 1        |
| 1.2      | Prerequisites         | 2        |
| <b>2</b> | <b>Procedure</b>      | <b>5</b> |
|          | <b>Glossary</b>       | <b>7</b> |
|          | <b>Reference List</b> | <b>9</b> |





# 1 Introduction

This document provides the description and troubleshooting steps to take for the Security, OAM User Gaining Privilege Failed alarm.

## 1.1 Alarm Description

This alarm is raised when an Operation and Maintenance (OAM) user attempts to raise their access permissions with a `su` or `sudo` command, and the command fails due to a wrong password.

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  |
|---|----------------------|---|-------------------|---|
| An OAM user has unsuccessfully tried to increase their access permissions using <code>su</code> or <code>sudo</code> command. | Authorization Fault. | An OAM user has unsuccessfully tried to increase their access permissions using <code>su</code> or <code>sudo</code> command. | Operating System. | OAM user is not authorized to execute action issued with <code>su</code> or <code>sudo</code> . |

**Note:** An alarm can appear as a result of the maintenance activity.

The alarm attributes are listed and explained in Table 2.

*Table 2 Alarm Attributes*

| Attribute Name           | Attribute Value  |
|--------------------------|--|
| Auto Cease               | No   |
| Module                   | SECURITY(11)   |
| Error Code               | 7  |
| Timestamp First          | Date and time when the alarm was raised for the first time.                            |
| Repeated Counter         | Number which indicates how many times the alarm was raised.                            |
| Timestamp Last           | Date and time of the most recent alarm raised.   |
| Resource ID              | .1.3.6.1.4.1.193.169.11.7.<IP>.<usernameLength>.<usernameASCIIcode>                    |
| Alarm Model Description  | OAM User Privilege Raise Failed, Security.   |
| Alarm Active Description | Security: OAM User Privilege Raise Failed @<IP> by user <username> to <other username> |
| ITU Alarm Event Type     | securityServiceOrMechanismViolation (10)   |
| ITU Alarm Probable Cause | authenticationFailure (600)  |



| Attribute Name               | Attribute Value   |
|------------------------------|---|
| ITU Alarm Perceived Severity | (6) - Warning   |
| Originating Source IP        | Node IP where the alarm was raised.                           |
| Sequence Number              | Number which indicates the order in which alarms were raised. |

In Table 2, the indicated variables are as follows:

- `<usernameLength>`: The number of characters in the user name.
- `<usernameASCIICode>`: A series of dot-separated numbers where each number corresponds to the ASCII code of each character in the user name.  
For example:  
  
79.97.109.85.115.101.114 for OamUser.
- `<IP>`: The IP address of the blade or Virtual Machine (VM), where user privilege raise was attempted.
- `<username>`: The name of the user in text.
- `<other username>`: The privileged username in text.

For more information about attribute descriptions, refer to the *Alarm Format and Description* section of *CUDB Node Fault Management Configuration Guide*, Reference [1].

## 1.2 Prerequisites

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

### 1.2.1 Documents

Before starting this procedure, ensure that you have read the following documents:

- *System Safety Information*, Reference [5].
- *Personal Health and Safety Information*, Reference [6].
- *CUDB Node Fault Management Configuration Guide*, Reference [1].

### 1.2.2 Tools

Not applicable.

**1.2.3****Conditions**

Not applicable.





## 2 Procedure

If the alarm is raised, perform the following steps:

1. Make backup copies of the log files to preserve evidence of the (attempted) intrusion.
2. Examine the security log file to determine the source of the intrusion. For more information about logging information in CUDB, refer to *CUDB Node Logging Events*, Reference [2].
3. If the log file analysis indicates that an unauthorized operation was successful, seek further advice in order to secure the system again. For more information about security configuration in CUDB, refer to *CUDB Security and Privacy Management*, Reference [3].
4. Once system security has been reestablished, refer to *CUDB Node Fault Management Configuration Guide*, Reference [1] to manually clear the alarm.

Further actions are outside the scope of this Operating Instruction.





## Glossary

For the terms, definitions, acronyms and abbreviations used in this document, refer to *CUDB Glossary of Terms and Acronyms*, Reference [4].





## Reference List

### **CUDB Documents**

- [1] *CUDB Node Fault Management Configuration Guide*
- [2] *CUDB Node Logging Events*
- [3] *CUDB Security and Privacy Management*
- [4] *CUDB Glossary of Terms and Acronyms*

### **Other Ericsson Documents**

- [5] *System Safety Information*
- [6] *Personal Health and Safety Information*