

# Audit Information

## USER GUIDE

**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

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Audit Log</b>	<b>3</b>
2.1	Syslog	3
2.2	Description of Syslog Entries	3
<b>3</b>	<b>Audit Trail</b>	<b>5</b>
3.1	Audit Trail in Syslog Example	5





# 1 Introduction

Audit information can be used to track access to files, directories, and resources of the system. It enables monitoring of the system for application misbehavior or code malfunctions.





## 2 Audit Log

The audit log record is forwarded to the syslog interface of the operating system. This provides a common audit trail that can be used for traceability of actions in the system.

### 2.1 Syslog

The syslog can be read from `/var/log/messages`, which in turn is a symbolic link to, for example, `/var/log/SC-2-1/messages`.

### 2.2 Description of Syslog Entries

The format of the syslog entries is as follows: `<date> <time> <hostname> <program_name>: <message>`

#### 2.2.1 Ericsson Command-Line Interface Examples

The following Ericsson Command-Line Interface (ECLI) example commands result in the following entries in the syslog:

```
>ManagedElement=NODE06ST
(ManagedElement=NODE06ST)>configure
(config-ManagedElement=NODE06ST)>siteLocation=SEKI2707353A
(config-ManagedElement=NODE06ST)>commit
>exit
```

```
2017-03-31 14:14:14.141 [INFO] [SEKI2707353A] [ManagedElement=NODE06ST] [configure]
2017-03-31 14:14:14.141 [INFO] [SEKI2707353A] [ManagedElement=NODE06ST] [commit]
2017-03-31 14:14:14.141 [INFO] [SEKI2707353A] [ManagedElement=NODE06ST] [exit]
2017-03-31 14:14:14.141 [INFO] [SEKI2707353A] [ManagedElement=NODE06ST] [configure]
2017-03-31 14:14:14.141 [INFO] [SEKI2707353A] [ManagedElement=NODE06ST] [commit]
2017-03-31 14:14:14.141 [INFO] [SEKI2707353A] [ManagedElement=NODE06ST] [exit]
```

#### 2.2.2 NETCONF Interface Example

The following Ericsson NETCONF Interface example commands result in the following entries in the syslog:







## 3 Audit Trail

The audit trail can, for example, be filtered out from the total syslog file by using keywords on the syslog entry, <message>.

### 3.1 Audit Trail in Syslog Example

...  
...  
...