

License Management, Key File Fault

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 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	Introduction	1
1.1	Alarm Description	1
1.2	Prerequisites	3
2	Procedure	5
2.1	Analyzing the Alarm	5
2.2	Actions for Sentinel RMS Configuration Issues	5
2.3	Actions for License Key File Issues	6
2.4	Actions for NeLS Connection Issues	8
	Reference List	17





1 Introduction

This document describes the License Management, Key File Fault alarm and provides instructions for fault management.

1.1 Alarm Description

License Management, Key File Fault is raised when License Manager (LM) transitions to Locked mode. This is a critical situation that may prevent the Managed Element from using licensed features and functionality.

Locked mode is initiated at the end of the 24-hour Autonomous mode period in response to one of the following scenarios:

- The Sentinel Rights Management Services (RMS) license server is unreachable.
- Any Ericsson License Manager (ELIM) formatted license key file is missing or corrupted.
- The Network License Server (NeLS) is unreachable.

Note: In an ELIM deployment with multiple license key files, this alarm is raised in response to one or more missing or corrupted license key files.

This primary alarm is issued by the ManagedElement=1, SystemFunctions=1, Lm=1 Managed Object (MO).

Possible causes and fault locations are explained in Table 1.



Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
159	License Management, Key File Fault	One of the following scenarios remains in effect for more than 24 hours: <ul style="list-style-type: none">• The Sentinel RMS license server is unreachable.• Any ELIM formatted license key file is missing or corrupted.• NeLS is unreachable.	LM Server	No license handling.

The following consequences are expected if the alarm condition is not resolved:

- LM operates in Locked mode. During Locked mode, requests for licensed features and capacities are blocked by LM.

Note: The License Management, Key File Fault alarm can appear as a result of maintenance activity.

The alarm attributes are listed and explained in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
activeSeverity	CRITICAL
additionalInfo	Not Applicable
additionalText	"Key file fault in Managed Element"
eventType	QUALITYOFSERVICEALARM



Table 2 Alarm Attributes

Attribute Name	Attribute Value
lastEventTime	A time stamp of the last alarm update, such as an alarm status change or severity change.
majorType	193
minorType	393221
originalAdditionalText	Content of the additionalText field when the alarm was raised.
originalEventTime	Time stamp when the alarm was raised.
originalSeverity	Value of the activeSeverity level when the alarm was raised.
probableCause	159 (Configuration or Customization Error)
sequenceNumber	The notification identity for this object instance. It is not the same as the fmAlarmId since multiple notifications may be sent for one alarm instance. This value changes for every notification (such as a severity change or alarm clear).
source	ManagedElement=1, SystemFunctions=1, Lm=1
specificProblem	License Management, Key File Fault

1.2 Prerequisites

This section lists the prerequisite documents, tools, and conditions for the alarm handling procedure.



1.2.1 Documents

Review the following documents before starting the procedure:

- Personal Health and Safety Information (Reference [1])
- System Safety Information (Reference [2])
- "Configuration Management Using CLI" in the COM Management Guide for your version of the product software.

1.2.2 Tools

Ensure that the following tools are available before starting the procedure:

- Element Management System (for example: OSS)
- Ericsson Command-Line Interface (ECLI)

For more information on these tools, refer to the documentation for your version of the product software.

1.2.3 Conditions

Ensure that the following conditions are met before starting the procedure:

- Verify that no ongoing maintenance activities are affecting the network or Network Elements.
- If applicable, know the IP addresses and port numbers of the Sentinel RMS license server.
- If applicable, know the host address and port number of NeLS.
- If applicable, have access to the Secure Sockets Layer (SSL) certificates for the NeLS customer security layer.
- Know the IP address of the blade where ECLI is running.
- Have the proper authority to handle configuration management of the Network Elements.
- Be familiar with basic Unix commands.



2 Procedure

This section describes the alarm handling procedure.

2.1 Analyzing the Alarm

License Management, Key File Fault is a persistent alarm that remains on the alarm list while LM is operating in Locked mode. The alarm clears automatically when locked mode ends.

To determine the fault location and cause:

1. Check if there are any other active network or Network Element-related alarms.
2. Perform one of the following steps depending on your LM deployment:
 - For LM deployments using Sentinel RMS, check the IP addresses and port numbers of the Sentinel RMS license server in the `Lm.referenceToLicenseServer` attribute.
 - For LM deployments using ELIM, check the `KeyFileInformation.location` attribute for each license key file.
 - For LM deployments using NeLS, check that the following NeLS connection requirements have been met:
 - A valid NeLS server address is set using the `NeLSConfiguration.host` and `NeLSConfiguration.port` attributes.
 - If applicable, the network operator SSL certificate files are stored in `/storage/system/config/lm-apr9010503/certs`.
 - If applicable, the network operator SSL certificate files are properly referenced in `certificate_config.xml`.

2.2 Actions for Sentinel RMS Configuration Issues

IP addresses and port numbers of the Sentinel RMS license server are part of the LM configuration. A faulty configuration can lead to connectivity issues.

To correct issues with the Sentinel RMS license server configuration:

1. In ECLI, navigate to the `Lm` MO, for example:
>ManagedElement=NODE06ST, SystemFunctions=1, Lm=1



2. Verify that the `Lm.referenceToLicenseServer` parameter points to the correct License Server host addresses and port numbers:

```
(Lm=1)>show referenceToLicenseServer
```

3. If necessary, update the IP addresses and port numbers of the Sentinel RMS license server:

- a. `(Lm=1)>configure`

- b. `(config-Lm=1)>referenceToLicenseServer=[<address_values>]`

Where `<address_values>` is a comma-separated list of "`<FQDN_or_IP_Address>:<Port_Number>`" pairs, one pair per server.

For example:

```
referenceToLicenseServer=["SC-1:5093","SC-2:5093"]
```

- c. `(config-Lm=1)>commit`

The connection to Sentinel RMS has been configured.

4. After verifying the configuration, check connectivity by triggering a refresh of the license inventory:

```
(Lm=1)>refreshLicenseInventory
```

The system returns `true` if the action was executed successfully.

5. Verify that the license inventory has been synchronized with a Sentinel RMS license server by checking the `lastLicenseInventoryRefresh` time stamp:

```
(Lm=1)>show lastLicenseInventoryRefresh
```

A recent time stamp indicates a successful update.

6. Check the alarm status.

If the alarm is still active, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

Note: If resolving the issue is expected to take more than 24 hours, Emergency Unlock can be used to prevent the system from entering Locked Mode. For more information on Emergency Unlock, refer to the *LM User Guide for Sentinel RMS* (Reference [3]).

2.3 Actions for License Key File Issues

Note: This procedure only applies to ELIM deployments.



ELIM license key files are stored on the cluster persistent storage path. Issues accessing persistent storage or a problem locating a license key file can force the License Manager into Locked mode.

To correct issues with ELIM license key files:

1. Log on the ME to access a Linux® shell, for example:

```
ssh <user>@<hostname> -p 7022
```

2. At the command prompt, check connectivity with the persistent storage path:

```
ls -l /storage/system/software/lm-apr9010503
```

If persistent storage is inaccessible, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

3. Exit the shell:

```
exit
```

4. In ECLI, navigate to the `KeyFileManagement` MO, for example:

```
>ManagedElement=NODE06ST, SystemFunctions=1, Lm=1,  
KeyFileManagement=1
```

5. Verify the `locatable` attribute for each `KeyFileInformation` class:

```
(KeyFileManagement=1)>show all
```

The contents of `KeyFileManagement=1` are printed.

If one or more license key files are missing or corrupted, LM reports `locatable=false`.

For example:

```
KeyFileManagement=1  
reportProgress  
  actionId=0  
  actionName="loadLicKeyFile"  
  progressInfo=""  
  progressPercentage=100  
  result=SUCCESS  
  resultInfo="Successfully loaded the new LKF"  
  state=FINISHED  
  timeActionCompleted="2014-05-13T14:12:34"  
  timeActionStarted="2014-05-13T14:12:34"  
  timeOfLastStatusUpdate="2014-05-13T14:12:34"  
KeyFileInformation=1  
  installationTime="2014-05-13T14:12:34"  
  locatable=true  
  productType="SSR 8000"
```



```
KeyFileInformation=2
  installationTime="2014-05-13T14:11:35"
  locatable=false
  productType="SASN"
KeyFileInformation=3
  installationTime="2014-05-13T14:12:15"
  locatable=true
  productType="EDA 1500"
```

6. For each license key file with `locatable=false`, restore the files from a backup location to the correct storage path.

Note: Each license key file is stored in a hashed subdirectory. The path to the hashed directory contains the `productType` of the license key file.

For example:

```
/storage/system/software/lm-apr9010503/SSR\
8000/8887563311a276a54cba15d6359a7f8c
```

LM detects the restored file within 1 minute.

7. If backup files are not available, order replacement license key files from the Ericsson software supply organization and have them installed.

For more information on installing ELIM license key files, refer to "Installing License Key Files" in the *LM User Guide for ELIM* (Reference [4]).

Note: If resolving the issue is expected to take more than 24 hours, Emergency Unlock can be used to prevent the system from entering Locked mode. For more information on Emergency Unlock, refer to the *LM User Guide for ELIM* (Reference [4]).

8. Check the alarm status.

If the alarm is still active, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

2.4 Actions for NeLS Connection Issues

To work with NeLS, LM must be configured to direct license requests to the NeLS server and use the appropriate Secure Sockets Layer (SSL) configuration for that connection.

Note: When the NeLS connection goes down, LM waits 3–5 minutes before attempting to reconnect for the first time. After the initial attempt, LM tries to reconnect to NeLS at regular intervals as specified by the `NeLSConfiguration.retryInterval` attribute.



2.4.1 Correcting NeLS Configuration Issues

The NeLS server address and port number are configured using `NeLSConfiguration.host` and `NeLSConfiguration.port` attributes. A faulty configuration can lead to connectivity issues.

To correct issues with the NeLS configuration and clear the alarm:

1. Ensure that the network infrastructure (physical connections, firewalls, routers, and so on) allows communication between LM and NeLS.
2. In ECLI, navigate to the `NeLSConfiguration` MO, for example:

```
>ManagedElement=NODE06ST,SystemFunctions=1,Lm=1,
NeLSConfiguration=1
```

3. Check the NeLS connection status:

```
(NeLSConfiguration=1)>show connectionStatus
```

`connectionStatus=UNDEFINED` indicates that LM has not made an initial connection attempt to NeLS.

`connectionStatus=CONNECTED` indicates that a connection to NeLS is established.

`connectionStatus=NOT_CONNECTED` indicates that the NeLS connection is down.

4. If `connectionStatus=CONNECTED`, check the alarm status.

If the alarm is still active, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

Note: If resolving the issue is expected to take more than 24 hours, Emergency Unlock can be used to prevent the system from entering Locked Mode. For more information on Emergency Unlock, refer to the LM User Guide for NeLS (Reference [5]).

5. If `connectionStatus` is `UNDEFINED` or `NOT_CONNECTED`, verify that the `NeLSConfiguration` points to the correct host address and port number:

- a. `(NeLSConfiguration=1)>show host`

- b. `(NeLSConfiguration=1)>show port`

6. If necessary, update the NeLS configuration.

- a. `(NeLSConfiguration=1)>configure`

- b. `(config-NeLSConfiguration=1)>host=<IP_Address_or_FQDN>`

- c. `(config-NeLSConfiguration=1)>port=<Port_Number>`



d. (config-NeLSConfiguration=1)>**commit**

The connection to NeLS has been configured. After committing the configuration changes, LM attempts to reconnect using the updated configuration settings.

7. Check the NeLS connection status:

(NeLSConfiguration=1)>**show connectionStatus**

If connectionStatus=CONNECTED, the NeLS connection has been restored.

8. If connectionStatus=NOT_CONNECTED, use Telnet to attempt to reach NeLS from the SC blade where LM is running.

telnet <NeLS_IP_Address:Port>

The following output shows that NeLS is down:

```
Trying <NeLS_IP_Address>...  
telnet: connect to address <IP_Address>: No route to host
```

If NeLS is down, wait five minutes and retry the command. If the output is the same, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

9. If NeLS was reachable (different Telnet output), check the NeLS connection retry interval in ECLI:

(NeLSConfiguration=1)>**show retryInterval**

Take note of the current setting.

10. Wait for the retry interval to elapse. If necessary, update the attribute to a shorter interval:

a. (NeLSConfiguration=1)>**configure**

b. (config-NeLSConfiguration=1)>**retryInterval=<seconds>**

c. (config-NeLSConfiguration=1)>**commit**

The NeLS connection retry interval has been updated.

11. After the retry interval and a short grace period have elapsed, check the connection status:

(NeLSConfiguration=1)>**show connectionStatus**



Note: If `retryInterval` was modified, the change may need to be reverted.

To reset the `retryInterval`:

- a `(NeLSConfiguration=1)>configure`
- b `(config-NeLSConfiguration=1)>retryInterval=<seconds>`
- c `(config-NeLSConfiguration=1)>commit`

12. If `connectionStatus=CONNECTED`, check the alarm status.

If the alarm is still active, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

Note: If resolving the issue is expected to take more than 24 hours, Emergency Unlock can be used to prevent the system from entering Locked Mode. For more information on Emergency Unlock, refer to the LM User Guide for NeLS (Reference [5]).

13. If `connectionStatus=NOT_CONNECTED`, investigate possible certificate issues by following the steps in section Section 2.4.2 on page 11.

2.4.2 SSL Certificate Issues

Communication between LM and NeLS requires SSL. This network connection can be secured by two layers of encryption, as follows:

- Ericsson security layer
- Customer security layer

The NeLS connection must always be encrypted using SSL certificates provided by Ericsson. The customer security layer, using the network operator SSL certificates, must be enabled only if NeLS is configured with network operator node credentials. A faulty SSL setup can lead to connectivity issues.

2.4.2.1 Correcting Issues When the Customer Security Layer is Disabled

When the customer security layer is disabled, all configuration values must be removed from `/storage/system/config/lm-apr9010503/certs/certificate_config.xml`.

To correct issues with `certificate_config.xml` and clear the alarm:

1. Log on the SC blade where LM is active to access a Linux shell, for example:

```
ssh <user>@<hostname> -p 7022
```



Note: To identify the SC where LM is active, execute the following command from any SC:

```
cmw-status -v siass | grep -A 1 LmSa
```

If LM is active on SC-1, the printout reads:

```
safSISU=safSu=LmSa-Su-0\,...  
HASState=ACTIVE(1)
```

If LM is active on SC-2, the printout reads:

```
safSISU=safSu=LmSa-Su-1\,...  
HASState=ACTIVE(1)
```

2. Verify that `/storage/system/config/lm-apr9010503/certs/certificate_config.xml` has empty values for all SSL filenames.

The following example shows the structure of `certificate_config.xml` when the customer security layer is properly disabled:

```
<?xml version="1.0" encoding="utf-8"?>  
  <nels-ssl-config>  
    <certificate-authority>  
      <path></path>  
    </certificate-authority>  
    <client-certificate>  
      <path></path>  
    </client-certificate>  
    <client-private-key>  
      <path></path>  
    </client-private-key>  
  </nels-ssl-config>
```

3. If necessary, update `certificate_config.xml` to remove the filenames.

30 seconds after updating `certificate_config.xml`, LM automatically reloads the SSL configuration settings and attempts to reestablish communication with NeLS.

4. If `certificate_config.xml` is missing, recreate it from the original template:

```
cp /opt/lm/etc/certificate_config_template.xml =>  
/storage/system/config/lm-apr9010503/certs/certificate_config.  
xml
```

After recreating the file, update it as required.

30 seconds after recreating `certificate_config.xml`, LM automatically reloads the SSL configuration settings and attempts to reestablish communication with NeLS.



5. In ECLI, navigate to the NeLSConfiguration MO, for example:

```
>ManagedElement=NODE06ST, SystemFunctions=1, Lm=1,
NeLSConfiguration=1
```

6. Check the NeLS connection status:

```
(NeLSConfiguration=1)>show connectionStatus
```

connectionStatus=UNDEFINED indicates that LM has not made an initial connection attempt to NeLS.

connectionStatus=CONNECTED indicates that a connection to NeLS is established.

connectionStatus=NOT_CONNECTED indicates that the NeLS connection is down.

7. If the NeLS and SSL configurations are valid and connectionStatus=NOT_CONNECTED, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

Note: If resolving the issue is expected to take more than 24 hours, Emergency Unlock can be used to prevent the system from entering Locked Mode. For more information on Emergency Unlock, refer to the LM User Guide for NeLS (Reference [5]).

After successfully configuring the SSL connection, it is highly recommended to perform a system backup with the Backup and Restore Framework (BRF).

2.4.2.2

Correcting Issues with the Customer Security Layer

The customer encryption layer between LM and NeLS requires the network operator SSL certificates and updates to the /storage/system/config/lm-apr9010503/certs/certificate_config.xml file.

To correct issues with the customer security layer:

1. Log on the SC blade where LM is active to access a Linux shell, for example:

```
ssh <user>@<hostname> -p 7022
```



Note: To identify the SC where LM is active, execute the following command from any SC:

```
cmw-status -v siass | grep -A 1 LmSa
```

If LM is active on SC-1, the printout reads:

```
safSISU=safSu=LmSa-Su-0\,....  
HASState=ACTIVE(1)
```

If LM is active on SC-2, the printout reads:

```
safSISU=safSu=LmSa-Su-1\,....  
HASState=ACTIVE(1)
```

2. Ensure that the following SSL files are located in `/storage/system/config/lm-apr9010503/certs/`:

- Certificate Authority (CA) file
- Client Certificate file
- Client Private Key file

If any of these files are missing, or if new files are required, follow your internal processes to obtain replacements and store them in `/storage/system/config/lm-apr9010503/certs/`.

Note: If multiple Certificate Authorities are required, all CAs must be defined in a single CA file. At least one CA must be valid for a successful NeLS connection.

30 seconds after changing any files in `/storage/system/config/lm-apr9010503/certs` from the SC where LM is active, LM attempts to connect to NeLS using the SSL configuration settings stored in `/storage/system/config/lm-apr9010503/certs/certificate_config.xml`.

3. Verify that `certificate_config.xml` references the correct SSL filenames.

The following example shows the structure of `certificate_config.xml`:

```
<?xml version="1.0" encoding="utf-8"?>  
<nels-ssl-config>  
  <certificate-authority>  
    <path>certificate-authority-file-name</path>  
  </certificate-authority>  
  <client-certificate>  
    <path>client-certificate-file-name</path>  
  </client-certificate>  
  <client-private-key>  
    <path>client-private-key-file-name</path>
```



```
</client-private-key>
</nels-ssl-config>
```

Where:

`certificate-authority-file-name` is the certificate authority filename.
The file must contain all certificates in the certificate chain.

`client-certificate-file-name` is the client certificate filename.

`client-private-key-file-name` is the client private key filename.

4. If necessary, update `certificate_config.xml` with the correct filenames.

30 seconds after updating `certificate_config.xml`, LM automatically reloads the SSL configuration settings and attempts to reestablish communication with NeLS.

5. If `certificate_config.xml` is missing, recreate it from the original template:

```
cp /opt/lm/etc/certificate_config_template.xml =>
/storage/system/config/lm-apr9010503/certs/certificate_config.
xml
```

After recreating the file, update it as required.

30 seconds after recreating `certificate_config.xml`, LM automatically reloads the SSL configuration settings and attempts to reestablish communication with NeLS.

6. In ECLI, navigate to the `NeLSConfiguration` MO, for example:

```
>ManagedElement=NODE06ST, SystemFunctions=1, Lm=1,
NeLSConfiguration=1
```

7. Check the NeLS connection status:

```
(NeLSConfiguration=1)>show connectionStatus
```

`connectionStatus=UNDEFINED` indicates that LM has not made an initial connection attempt to NeLS.

`connectionStatus=CONNECTED` indicates that a connection to NeLS is established.

`connectionStatus=NOT_CONNECTED` indicates that the NeLS connection is down.

8. If the NeLS and SSL configurations are valid and `connectionStatus=NOT_CONNECTED`, consult the next level of maintenance support. Further actions are outside the scope of this instruction.



Note: If resolving the issue is expected to take more than 24 hours, Emergency Unlock can be used to prevent the system from entering Locked Mode. For more information on Emergency Unlock, refer to the [LM User Guide for NeLS \(Reference \[5\]\)](#).

After successfully configuring the SSL connection, it is highly recommended to perform a system backup with BRF to preserve the certificate files.



Reference List

- [1] Personal Health and Safety Information, 12446-2885 Uen
- [2] System Safety Information, 12446-2886 Uen
- [3] LM User Guide for Sentinel RMS, 1/1553-APR 901 0503/6 Uen
- [4] LM User Guide for ELIM, 2/1553-APR 901 0503/6 Uen
- [5] LM User Guide for NeLS, 3/1553-APR 901 0503/6 Uen