

Certificate Management, the Certificate is to Expire

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2014, 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	3





1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm is raised when a certificate renewal is needed to prevent a secure service failure. The alarm is raised only if the node credential can cause interruption to the secure service.

The possible alarm causes and fault locations are explained in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
The certificate is about to expire and is to be renewed	The number of days until the certificate expires is equal to or less than defined by the attribute <code>expiryAlarmThreshold</code>	The threshold for certificate expiration time has been crossed	Node credential	Secured service can fail, for example, Internet Protocol Security connection authenticated by expired certificate can fail

The alarm attributes are listed and explained in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	6946818
Managed Object Class	<i>NodeCredential</i>
Managed Object Instance	<code>ManagedElement=<node_name>, SystemFunctions=1, SecM=1, CertM=1, NodeCredential=<node_credential_id></code>
Specific Problem	Certificate Management, the Certificate is to Expire
Event Type	<code>processingErrorAlarm (4)</code>
Probable Cause	<code>x733ThresholdCrossed (351)</code>



Table 2 Alarm Attributes

Attribute Name	Attribute Value
Additional Text	The threshold before certificate expiration has been crossed, and the certificate should be renewed to prevent a secure service failure
Perceived Severity	warning (6) ⁽¹⁾

(1) The `expiryAlarmThreshold` configuration determines how the alarming object is to define its severity level. The severity level is set to warning when the value of the `expiryAlarmThreshold` matches the number of days until the certificate expires.

The severity level is raised from warning to minor when 1/3 of the value of `expiryAlarmThreshold` matches the number of days until the certificate expires.

The severity level is raised from minor to major when 1/10 of the value of `expiryAlarmThreshold` matches the number of days until the certificate expires or there is only one week left until the certificate expires.

Note: When the certificate expires, this alarm is cleared and alarm *Certificate Management, a Valid Certificate is Not Available* is raised for the same `NodeCredential` MO.

1.2 Prerequisites

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

1.2.1 Documents

This instruction references the following documents:

- *Certificate Management, a Valid Certificate is Not Available*
- *Certificate Management, Automatic Enrollment Failed*
- *Data Collection Guideline*
- *Install or Renew Node Credential by CSR*
- *Install or Renew Node Credential by PKCS 12*
- *Renew Node Credential Online*

1.2.2 Tools

No tools are required.

1.2.3 Conditions

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



- A Certificate Management, the Certificate is to Expire alarm is raised.
- The user has the System Security Administrator role.
- The user is familiar with the security policy and environment of the organization. The user knows what mechanism is appropriate to use to install and renew node credentials (online, PKCS#12, or CSR).
- If online renewal of node credentials is used, the correct configuration information for enrollment server groups and enrollment authorities is obtained from the IT or security administrator.
- No ongoing maintenance activities are affecting the network or network elements.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.

2 Procedure

Do the following:

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

```
>ManagedElement=NODE06ST, SystemFunctions=1, SecM=1, CertM=1, NodeCredential=1
```

2. Check attribute `renewalMode`.

```
(NodeCredential=1)>show renewalMode
```

The following is an example output:

```
renewalMode=MANUAL
```

3. Select the appropriate action based on the result:
 - **MANUAL** – The alarm can be cleared by performing certificate renewal for the enrolled `NodeCredential` MO.
 - **AUTOMATIC** – Continue according to the instruction *Certificate Management, Automatic Enrollment Failed* instead. Further actions are outside the scope of this instruction.



4. Based on the security policy, use the appropriate operation among the following to renew the node credential:
 - *Renew Node Credential Online*
 - *Install or Renew Node Credential by PKCS 12* (select renewal in step 2)
 - *Install or Renew Node Credential by CSR* (select renewal in step 2)
5. Is the alarm cleared?

Yes: Proceed with Step 8.

No: Continue with the next step.
6. Perform data collection, refer to *Data Collection Guideline*.
7. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
8. Job is completed.