

Certificate Management, a Valid Certificate is Not Available

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 |
| 2.1 | Analyzing Alarm | 3 |
| 2.2 | Actions for Installation | 4 |
| 2.3 | Actions for Renewal | 4 |
| 2.4 | Actions for Repairing Automatic Configuration | 4 |



Certificate Management, a Valid Certificate is Not Available



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The alarm is raised when a secure service failed because of an expired, revoked, or non-existing certificate.

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

Table 1 Alarm Causes

| Alarm Cause | Description | Fault Reason | Fault Location | Impact |
|--|---|-----------------------------|-----------------|---|
| No valid certificate available at secured service invocation | No valid certificate is available when a secured service is invoked | No certificate exists yet | Node credential | A secured service fails, for example, an IP Security (IPsec) connection authenticated by an expired certificate fails |
| | | The certificate has expired | | |
| | | The certificate is revoked | | |

Note: Given the fault impact on secured protocols, more protocol-specific alarms can be raised as a consequence.

The alarm attributes are listed and explained in Table 2.

Table 2 Alarm Attributes

| Attribute Name | Attribute Value |
|-------------------------|---|
| Major Type | 193 |
| Minor Type | 6946817 |
| Managed Object Class | <i>NodeCredential</i> |
| Managed Object Instance | ManagedElement=<node_name>, SystemFunctions=1, SecM=1, CertM=1, NodeCredential=<node_credential_id> |
| Specific Problem | Certificate Management, a Valid Certificate is Not Available |
| Event Type | operationalViolation (8) |
| Probable Cause | x736OutOfService (414) |



Table 2 Alarm Attributes

| Attribute Name | Attribute Value |
|--------------------|---|
| Additional Text | The certificate provided by the alarming object is expired, revoked, or unavailable, which can result in the failure of a secure service using this certificate |
| Perceived Severity | critical (3) |

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:

- *Configure Enrollment Authority*
- *Configure Enrollment Server Group Together with Enrollment Servers*
- *Data Collection Guideline*
- *Install Node Credential Online*
- *Install or Renew Node Credential by CSR*
- *Install or Renew Node Credential by PKCS 12*

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, a Valid Certificate is Not Available 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

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

2.1 Analyzing Alarm

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 `certificateState`:

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

The following is an example output:

```
certificateState=EXPIRED
```

3. Select the appropriate action based on the result:
 - Attribute 'certificateState' not set – The certificate does not exist. Proceed with Section 2.2 Actions for Installation on page 4.
 - EXPIRED – The certificate has expired based on the `validTo` date. Continue with the next step.
 - REVOKED – The certificate was revoked by a trusted Certification Authority (CA). Continue with the next step.
4. Check attribute `renewalMode`:



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

The following is an example output:

```
renewalMode=MANUAL
```

5. Select the appropriate action based on the result:
 - **MANUAL** – The alarm can be cleared by repeating the installation or renewal for the `NodeCredential` MO. Proceed with Section 2.3 Actions for Renewal on page 4.
 - **AUTOMATIC** – Proceed with Section 2.4 Actions for Repairing Automatic Configuration on page 4.

2.2 Actions for Installation

Do the following:

1. Based on the security policy, use the appropriate operation among the following to install the node credential:
 - *Install Node Credential Online*
 - *Install or Renew Node Credential by PKCS 12* (select installation in step 2)
 - *Install or Renew Node Credential by CSR* (select installation in step 2)
2. Job is completed.

2.3 Actions for Renewal

Do the following:

1. Based on the security policy, use the appropriate operation among the following to renew the node credential:
 - *Install 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)
2. Job is completed.

2.4 Actions for Repairing Automatic Configuration

Do the following:

1. Navigate to the *CertM* MO, for example:



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

2. View the enrollment authority, enrollment server group, and enrollment server configuration:

```
(CertM=1) >show -r
```

The following is an example output:

```
CertM=1
[...]
  EnrollmentAuthority=1
    enrollmentAuthorityName="/CN=atrcus3409NECertCA/OU==>
ericssonOAM/O=Ericsson"
    enrollmentCaCertificate="ManagedElement=NODE06ST,=>
SystemFunctions=1, SecM=1, CertM=1, TrustedCertificate=1"
    userLabel="atrcus3409NECertCA O&M Certificate Authority"
  EnrollmentAuthority=2
    enrollmentAuthorityName="/CN=atrcus3841NECertCA/OU==>
ericssonOAM/O=Ericsson"
    enrollmentCaCertificate="ManagedElement=NODE06ST,=>
SystemFunctions=1, SecM=1, CertM=1, TrustedCertificate=2"
    userLabel="atrcus3841NECertCA O&M Certificate Authority"
  EnrollmentServerGroup=1
    EnrollmentServer=1
      protocol=CMF
      uri="cmp://192.0.2.10"
  EnrollmentServerGroup=2
    EnrollmentServer=1
      protocol=CMF
      uri="cmp://192.0.2.10"
```

3. Does the output in Step 2 show that an enrollment authority with the correct CA authority name (`enrollmentAuthorityName`) and CA certificate (`enrollmentCaCertificate`) is configured on the Managed Element (ME)? That is, does the attributes values for an *EnrollmentAuthority* MO match the values obtained from the IT or security administrator?

Yes: Continue with the next step.

No: Proceed with Step 5.

4. Does the output in Step 2 show that an enrollment server group contains a correct enrollment server configuration (attributes `protocol` and `uri`)?

Yes: Proceed with Step 8.

No: Proceed with Step 7.

5. Configure an enrollment authority.



For information on how to configure an enrollment authority, refer to *Configure Enrollment Authority*.

6. Proceed with Step 8.

7. Configure an enrollment server group with enrollment servers.

For information on how to configure an enrollment server group with enrollment servers, refer to *Configure Enrollment Server Group Together with Enrollment Servers*.

8. Navigate to the *NodeCredential* MO, for example:

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

9. Enter Config mode:

```
(NodeCredential=1) >configure
```

10. Change to manual renewal mode:

```
(config-NodeCredential=1) >renewalMode=MANUAL
```

11. Commit the change:

```
(config-NodeCredential=1) >commit
```

12. Install a node credential online using the enrollment authority and enrollment server group configuration checked or added previously.

For information how to install a node credential online, refer to *Install Node Credential Online* (step 3 results in navigating to the existing MO and not in creating an MO).

13. Is the alarm cleared?

Yes: Continue with the next step.

No: Proceed with Step 18.

14. Enter Config mode:

```
(NodeCredential=1) >configure
```

15. Change to automatic renewal mode:

```
(config-NodeCredential=1) >renewalMode=AUTOMATIC
```

16. Commit the change:

```
(config-NodeCredential=1) >commit
```

17. Proceed with Step 20.



18. Perform data collection, refer to *Data Collection Guideline*.
19. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
20. Job is completed.