

P-CSCF Rejected Messages On Unprotected Server Port

Call Session Control Function

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2016. 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





1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The threshold alarm `P-CSCF Rejected Messages On Unprotected Server Port` is issued if the number of messages which unexpectedly arrives under the granularity period to the unprotected port in the Proxy Call Session Control Function (P-CSCF) reaches or exceeds the threshold value.

The alarm is associated to the Performance Management counter `cscfRejectedUnprotectedMessages`. The alarm is enabled by default.

The alarm is raised when the number of `cscfRejectedUnprotectedMessages` has reached or exceeded its configured `thresholdHigh` within the time period configured by `thresholdRateOfVariation` and `granularityPeriod`.

The alarm is automatically ceased when it reaches or goes below the configured `thresholdLow` value.

The default values related to this alarm are: `thresholdRateOfVariation=PER_GP`, `granularityPeriod=FIVE_MIN`, `thresholdHigh=6`, and `thresholdLow=0`. This means that when the counter value is 6 or higher, the alarm is raised when the granularity period is ended. The alarm is ceased when the counter `cscfRejectedUnprotectedMessages` has reached a value of 0 at the end of a granularity period.

Note: The thresholds for raising and ceasing this alarm are configurable. The default distinguished name for the threshold is `ManagedElement=<node_name>`, `SystemFunctions=1`, `Pm=1`, `PmJob=CscfUsimAkaSpecificThreshold`, `MeasurementReader=cscfRejectedUnprotectedMessagesMeasReader`, `PmThresholdMonitoring=cscfRejectedUnprotectedMessages`.

It is not possible to change threshold values once they have been set. To change a threshold, first the `PmThresholdMonitoring` instance must be deleted and recreated with required `thresholdHigh` and `thresholdLow`.

For more information, refer to *Performance Management*.

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
The PM counter <code>cscfRejectedUnprotectedMessages</code> has reached or exceeded its configured upper threshold value.	The number of RE-REGISTER or DE-REGISTER messages received from Authentication and Key Agreement (AKA) authenticated User Equipment (UE) on the P-CSCF unprotected server port has reached or exceeded the configured threshold value.	Too many RE-REGISTER or DE-REGISTER messages received on the P-CSCF unprotected server port.	Mis-configuration on the User Equipment (UE).	The P-CSCF Rejects Messages On Unprotected Server Port for misbehaving UEs.

Note: An 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
Major Type	193
Minor Type	6684692
Managed Object Class	MeasurementReader
Managed Object Instance	ManagedElement=<node_name>, SystemFunctions=1, Pm=1, PmJob=CscfUsimAkaSpecificThreshold, MeasurementReader=cscfRejectedUnprotectedMessagesMeasReader
Specific Problem	P-CSCF Rejected Messages On Unprotected Server Port
Event Type	communication (2)
Probable Cause	x733ThresholdCrossed (351)



Attribute Name	Attribute Value
Additional Text	cscfRejectedUnprotectedMessages, too many RE-REGISTER, or DE-REGISTER messages received from AKA authenticated UE on P-CSCF unprotected server port.
Perceived Severity	warning (6)

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 document:

- *Performance Management*
- *Managed Object Model (MOM)*

1.2.2 Tools

No tools are required.

1.2.3 Conditions

No conditions.





2 Procedure

Note: If the reason for the alarm has disappeared after the granularity period, the alarm automatically ceases.

Do the following:

1. Identify the misbehaving UEs (public ID and IP address) from the content of the generated `SIP 403 Unprotected Traffic Forbidden` response.
2. Correct the configuration of the UEs.
3. The alarm ceases after the configuration of the UEs is corrected.
4. Confirm that the alarm has ceased. If the alarm remains, consult the next level of maintenance support. Further actions are outside the scope of this instruction.
5. Job is completed.