

# CSCF Network Tracing

## Call Session Control Function

---

### USER GUIDE

**Copyright**

© Ericsson AB 2016–2018. 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>  |
| 1.1      | Prerequisites             | 1         |
| <b>2</b> | <b>Tools</b>              | <b>3</b>  |
| 2.1      | NetTrace                  | 3         |
| 2.2      | AppTrace and AppLog       | 8         |
| 2.3      | NetTraceCollector         | 8         |
| <b>3</b> | <b>NetTrace Function</b>  | <b>9</b>  |
| 3.1      | NetTrace Procedure        | 10        |
| 3.2      | Analysis of Trace Outputs | 12        |
| <b>4</b> | <b>File Management</b>    | <b>15</b> |





# 1 Introduction

This document describes the procedure that is to be used to obtain network traces from the Call Session Control Function (CSCF).

This document covers the following topics:

- Configuration and use of the network tracing function to obtain SIP or Cx/Dx, or both, traces in machine-readable format (XML<sup>®</sup> files)
- Configuration and use of the network tracing function to obtain SIP or Cx/Dx, or both, traces in human-readable format (read directly from AppLog)

**Note:** Post-processing of machine-readable trace outputs is not included in this document.

## 1.1 Prerequisites

This section describes the prerequisites for this document.

To use this document, the user must be authorized to access CSCF with sudo/root privileges for the required actions.

### 1.1.1 Documents

Before starting this procedure, ensure that the following documents have been read:

- *AppTrace User Guide*
- *CSCF Troubleshooting Guideline*
- *IMS Common Components Troubleshooting Guide*

### 1.1.2 Conditions

Certain troubleshooting activities can have an impact on node performance. For example, trace activation can be traffic disturbing and is not recommended without first consulting Ericsson. However, NetTrace can be activated for a few users and sessions without adversely affecting performance (up to 10 users is the recommended limit).





## 2 Tools

This section describes the tools that can be used for network tracing in the CSCF.

### 2.1 NetTrace

**Note:** The inherent problem with observing the behavior of a system by tracing is the consumed capacity of the tracing itself. If the cost is too high, it can interfere with the primary function of the system, at worst even causing system failure.

NetTrace is a tool that allows the user to trace transactions that traverse the CSCF depending on user-defined filter criteria. These transactions are formatted and output in standardized XML file format (in this document referred to as “machine readable”) according to the 3GPP® specification [\*Telecommunication management; Subscriber and equipment trace; Trace data definition and management\*](#).

Alternatively, traces can be read directly from the AppLog and AppTrace files (referred to as “human-readable”). Human-readable format of traces is proprietary and not specified by the TS 32.423.

It is possible to trace at two levels; Min (minimum) and Max (maximum) for both machine-readable and human-readable output formats.

When active, tracing is performed on all CSCF-implemented SIP interfaces and Standard Cx/Dx interfaces (except Push-Profile-Request (PPR)/Push-Profile-Answer (PPA), and Registration Termination Request (RTR)/Registration Termination Answer (RTA) when the Public User Identity is not included in the request message).

If CSCF nodes are collocated such as for ISP (I-CSCF S-CSCF P-CSCF) and IS (I-CSCF S-CSCF), signaling within a physical node is not traced unless there is a transition between the originating CSCF and the terminating CSCF or the opposite.

Descriptions for `ieGroup name` and `ie name` can be found in the TS 32.423.

The presence of an information element in the following tables is defined by the P (presence) column as follows:

- M = Mandatory. The element is always present.
- O = Optional. The element can be present.

The terms `tracedPublicId1` and `tracedPublicId2` used in the following tables refer to the Public User IDs that triggered the trace. The element

`tracedPublicId1` is always present as one Public User ID must have triggered the trace.

If the trace is triggered by more than one Public User ID, its output is as `tracedPublicId2`. For example, if a Public User ID is specified as an `OrigPublicId`, a different Public User ID is specified as a `TermPublicId`, and a session is set up between the users, both Public User IDs trigger in the same trace.

### 2.1.1 Machine-Readable SIP Output at Min Level

At Min Trace Level, the SIP transactions are represented by several XML tags. Limited information is output when tracing at this level.

For the standard XML elements included in output, refer to the 3GPP Specification [Telecommunication management; Subscriber and equipment trace; Trace data definition and management](#).

The CSCF implemented data output is listed in Table 1 and Table 2.

*Table 1 Machine-Readable SIP Output Request Data at Min Level*

| Request                                     |                              |          |  |
|---|------------------------------|----------|--|
| ieGroup Name                                | ie Name                      | Presence | Comment  |
| <code>tracedPublicIds</code> <sup>(1)</sup> | <code>tracedPublicId1</code> | M        | A Public User ID that triggered tracing of this Request. |
| <code>tracedPublicIds</code> <sup>(1)</sup> | <code>tracedPublicId2</code> | O        | A Public User ID that triggered tracing of this Request. |
| -   | Request-Line                 | M        | SIP Request line   |
| Message Headers                             | To                           | M        | SIP To header  |
| Message Headers                             | From                         | M        | SIP From header  |
| Message Headers                             | Call-ID                      | M        | SIP Call-ID header                                       |
| Message Headers                             | CSeq                         | M        | SIP CSeq header  |

(1) *ieGroup name* `tracedPublicIds` is only output once, when the trace session is started.

*Table 2 Machine-Readable SIP Output Response Data at Min Level*

| Response     |             |          |                 |
|--------------|-------------|----------|-----------------|
| ieGroup Name | ie Name     | Presence | Comment         |
| -            | Status-Line | M        | SIP Status line |





| Response        |         |          |                    |
|-----------------|---------|----------|--------------------|
| ieGroup Name    | ie Name | Presence | Comment            |
| Message Headers | To      | M        | SIP To header      |
| Message Headers | From    | M        | SIP From header    |
| Message Headers | Call-ID | M        | SIP Call-ID header |
| Message Headers | CSeq    | M        | SIP CSeq header    |

## 2.1.2

### Machine-Readable Cx Output at Min Level

At Min Trace Level, the Cx transactions are represented by several XML tags. Limited information is output when tracing at this level.

For the standard XML elements included in output, refer to the 3GPP specification [Telecommunication management; Subscriber and equipment trace; Trace data definition and management](#).

The CSCF implemented data output is listed in Table 3 and Table 4.

*Table 3 Machine-Readable Cx Output Command Data at Min Level*

| Command                        |                 |          |  |
|--------------------------------|-----------------|----------|--|
| ieGroup Name                   | ie Name         | Presence | Comment  |
| tracedPublicIds <sup>(1)</sup> | tracedPublicId1 | M        | A Public User ID that triggered tracing of this Command. |

*(1) ieGroup name tracedPublicIds is only output once, when the Trace Session is started.*

*Table 4 Machine-Readable Cx Output Response Data at Min Level*

| Response     |                          |          |                                   |
|--------------|--------------------------|----------|-----------------------------------|
| ieGroup Name | ie Name                  | Presence | Comment                           |
| -            | Result-Code              | O        | Diameter Result-Code              |
| -            | Experimental-Result-Code | O        | Diameter Experimental-Result-Code |

Either Result-Code or Experimental-Result-Code is present.

Post-processing is required on the generated XML files to obtain meaningful trace data.

### 2.1.3 Human-Readable SIP Output at Min Level

At Min Trace Level, the SIP transactions are represented in plain-text form within the AppTrace. The Message Header and applicable parameters are included in output on individual lines. Limited information is included in output when tracing at this level.

The CSCF implemented data output is listed in Table 5 and Table 6.

*Table 5 Human-Readable SIP Output Request Data at Min Level*

| Request                        |          |  |
|--------------------------------|----------|--|
| Message                        | Presence | Comment  |
| traceSessionRef <sup>(1)</sup> | M        | Indicates the forloop specified used by the operator             |
| origPublicId <sup>(1)</sup>    | M        | The Originating Public User ID derived from this Request         |
| termPublicId <sup>(1)</sup>    | M        | The Terminating Public User ID derived from this Request         |
| tracedPublicId1 <sup>(1)</sup> | M        | A Public User ID that triggered tracing of this Request          |
| tracedPublicId2 <sup>(1)</sup> | O        | A Public User ID that triggered tracing of this Request          |
| Initiator                      | M        | IP/Port/Transport that initiated this Request                    |
| Target                         | M        | IP/Port/Transport that is the intended recipient of this Request |
| Request-Line                   | M        | SIP Request line   |
| To                             | M        | SIP To header  |
| From                           | M        | SIP From header  |
| Call-ID                        | M        | SIP Call-ID header   |
| CSeq                           | M        | SIP CSeq header  |

*(1) These fields are only output once, when the trace session is started.*



*Table 6 Human-Readable SIP Output Response Data at Min Level*

| Response    |          |  |
|-------------|----------|--|
| Message     | Presence | Comment  |
| Initiator   | M        | IP/Port/Transport that initiated this Request                    |
| Target      | M        | IP/Port/Transport that is the intended recipient of this Request |
| Status-Line | M        | SIP Status line  |
| To          | M        | SIP To header  |
| From        | M        | SIP From header  |
| Call-ID     | M        | P Call-ID header   |
| CSeq        | M        | SIP CSeq header  |

#### 2.1.4

#### Human-Readable Cx Output at Min Level

At Min Trace Level, the Cx transactions are represented in plain-text form within the AppLog. The Command and Response and the Result-Code or Experimental-Result-Code AVP is included in output on individual lines. Limited information is included in output when tracing at this level.

The CSCF implemented data output is listed in Table 7 and Table 8.

*Table 7 Human-Readable Cx Output Command Data at Min Level*

| Command      |          |                       |
|--------------|----------|-----------------------|
| Message      | Presence | Comment               |
| Command-Name | M        | Diameter Command Name |

*Table 8 Human-Readable Cx Output Response Data at Min Level*

| Response                 |          |                                   |
|--------------------------|----------|-----------------------------------|
| Msg                      | Presence | Comment                           |
| Response-Name            | M        | Diameter Response Name            |
| Result-Code              | O        | Diameter Result-Code              |
| Experimental-Result-Code | O        | Diameter Experimental-Result-Code |

Either Result-Code or Experimental-Result-Code is present.

### 2.1.5 Machine-Readable SIP and Cx Output at Max Level

At Max Trace Level, the SIP and Cx transactions are encoded into hexadecimal and output as raw data in XML file format. In contrast to Min level, the complete contents of each request or command and response are output.

The mandatory data specified in Section 2.1.1 Machine-Readable SIP Output at Min Level on page 4 and Section 2.1.2 Machine-Readable Cx Output at Min Level on page 5 for Min level are also mandatory at Max level.

For the standard XML elements included in output, refer to the 3GPP Specification [Telecommunication management; Subscriber and equipment trace; Trace data definition and management](#).

Post-processing is required on the generated XML files to obtain meaningful trace data.

### 2.1.6 Human-Readable SIP and Cx Output at Max Level

At Max Trace Level, the SIP and Cx transactions are represented in plain-text form within the AppLog. In contrast to Min level, the complete contents of each request or command and response are output.

The mandatory data specified in Section 2.1.3 Human-Readable SIP Output at Min Level on page 6 and Section 2.1.4 Human-Readable Cx Output at Min Level on page 7 for Min level are also mandatory at Max level.

## 2.2 AppTrace and AppLog

vDicos AppTrace is used to realize the NetTrace.

For a detailed description of AppTrace functionality, refer to *AppTrace User Guide*.

For machine-readable format, the AppTrace output must be directed to AppLog.

For human-readable format, the AppTrace output is to be directed to AppLog.

## 2.3 NetTraceCollector

The `NetTraceCollector` is a Perl-based script that collects trace data from the AppLog and outputs the data as in XML format.

### 3 NetTrace Function

The principle of NetTrace is to allow a user the possibility to log SIP and Cx transactions traversing the CSCF for fault finding and localization purposes.

Using the AppTrace, a trace session can be configured to trace SIP and Cx transactions based on the filtering of the Originating Public User IDs and Terminating Public User IDs for both Min and Max levels. The flow of actions required to obtain trace outputs for SIP and Cx is shown in Figure 1.

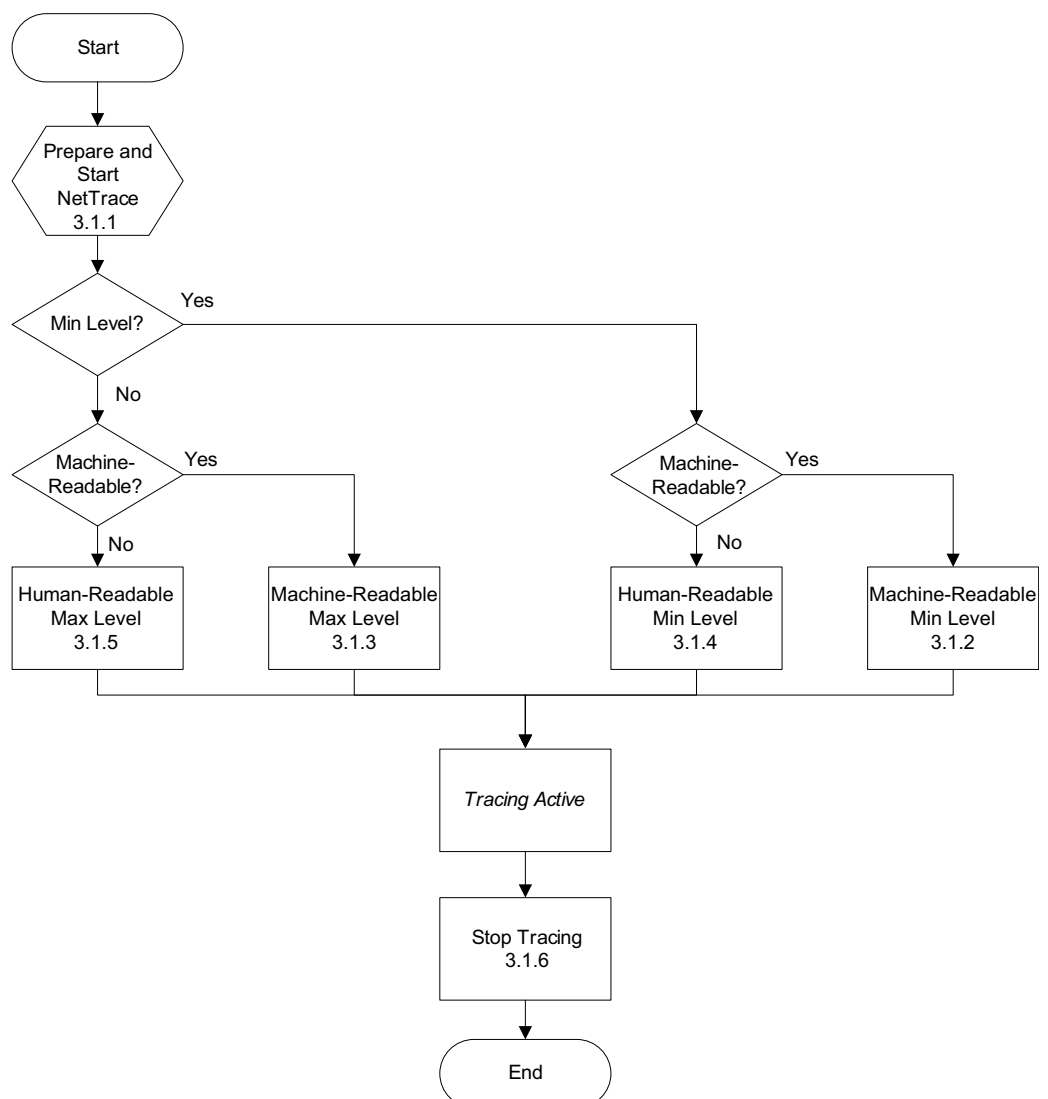


Figure 1 Simplified Flow Configuration and Use of NetTrace



## 3.1 NetTrace Procedure

### 3.1.1 Prepare and Start NetTrace

The following sequence is applicable when preparing and starting NetTrace for any type of trace output.

This procedure is valid when the user has direct access to the node.

For more information on how to ensure the XML files (if applicable) are output correctly, refer to *IMS Common Components Troubleshooting Guide*.

To prepare NetTrace for any type of trace output:

1. Log on to the SC processor of the CSCF node:

```
> ssh -A user1@<IP-address>
```

2. Start the NetTraceCollector script (applicable for machine-readable only):

- a. Check if the NetTraceCollector script is already running by using, for example:

```
> ps -ef | grep nettracecollector
```

- b. If the NetTraceCollector script is not running, start the script:

```
> nettracecollector &
```

3. Choose one of the following NetTrace output types:

- Machine-Readable at Min Level, see Section 3.1.2 Start NetTrace for Machine-Readable Output at Min Level on page 10.
- Machine-Readable at Max Level, see Section 3.1.3 Start NetTrace for Machine-Readable Output at Max Level on page 11.
- Human-Readable at Min Level, see Section 3.1.4 Start NetTrace for Human-Readable Output at Min Level on page 11.
- Human-Readable at Max Level, see Section 3.1.5 Start NetTrace for Human-Readable Output at Max Level on page 12.

### 3.1.2 Start NetTrace for Machine-Readable Output at Min Level

To specify the public users to trace and to make the trace output machine-readable (XML) at Min level:



```
1. > CscfTrace -ro applog -user sip:user@domain --forlop
    sip:user@domain=<forlop> --net_min_sip_method <sip method
    (s)> CSCFv_NetTraceMinMachineReadable_Trace_Profile
```

The following apply:

- Option `-ro` specifies where the output is routed. Always set this to **Applog**.
- Option `--forlop` is optional. By default, if this option is absent, `forlop` values are allocated.
- Option `--net_min_sip_method` is optional. By default, if this option is absent, all SIP methods are applied.
- Parameter `forlop` is a Trace Identity and is an integer value. The value is chosen by the operator. Normally, a unique `forlop` value is assigned to each Public User ID, but this is not mandatory. It is allowed to assign the same `forlop` value to all traced Public User IDs.

**Note:** It is possible to express multiple user IDs and multiple `forlop` values using command `CscfTrace`.

For more information, run `CscfTrace -h`. After starting trace, to see what process types and domains are enabled for the current session, run `CscfTrace display`.

### 3.1.3 Start NetTrace for Machine-Readable Output at Max Level

To specify the public users to trace and to make the trace output machine-readable (XML) at Max level:

```
1. > CscfTrace -ro applog -user sip:user@domain --forlop
    sip:user@domain=<forlop> CSCFv_NetTraceMaxMachineReadabl
    e_Trace_Profile
```

For more information on options, parameters, and `CscfTrace`, see Section 3.1.2 Start NetTrace for Machine-Readable Output at Min Level on page 10.

### 3.1.4 Start NetTrace for Human-Readable Output at Min Level

To specify the public users to trace and to make the trace output human-readable (read directly from AppLog) at Min level:

```
1. > CscfTrace -ro applog -user sip:user@domain --forlop
    sip:user@domain=<forlop> --net_min_sip_method <sip
    method(s)> CSCFv_NetTraceMinHumanReadable_Trace_Profile
```

For more information on options, parameters, and `CscfTrace`, see Section 3.1.2 Start NetTrace for Machine-Readable Output at Min Level on page 10.



### 3.1.5 Start NetTrace for Human-Readable Output at Max Level

To specify the public users to trace and to make the trace output human-readable (read directly from AppLog) at Max level:

```
1. > CscfTrace -ro applog -user sip:user@domain --forlop
    sip:user@domain=<forlop> CSCFv_NetTraceMaxHumanReadabl
    e_Trace_Profile
```

For more information on options, parameters, and `CscfTrace`, see Section 3.1.2 Start NetTrace for Machine-Readable Output at Min Level on page 10.

### 3.1.6 Stop NetTrace

To stop NetTrace:

```
1. > CscfTrace stop
```

## 3.2 Analysis of Trace Outputs

### 3.2.1 Machine-Readable Traces

NetTrace XML files are located in the following directory in CSCF node:

```
/storage/no-backup/cmco_utils-cxp9020686/nettrace/cscf
```

The following naming convention applies to an XML file that is being created:

```
A<date>.<time>-CSCF.<nodeName>.<TraceReference>.<SessionRef>.
xml.COMPLETE
```

Where:

- `<date>` is in the form `yyyymmdd`.
- `<time>` is in the form `hhmm`.
- `<TraceReference>` is the user-defined forlop ID.
- `<SessionRef>` is the system-defined Trace Session Recording Session Reference.
- `<nodeName>` is specified by environment variable `Node_Distinguished_Name`. If the environment variable is absent, the default value is `ManagedElement1`.

For example:

```
A20110128.1609-CSCF.ManagedElement1.1111.56032.xml
```

Post-processing is required by a system compliant with the TS 32.423.





After an XML file is completed and ready for post-processing, the suffix .COMPLETE is appended to the filename.

For example:

```
A20110128.1609-CSCF.ManagedElement1.1111.56032.xml.COMPL
ETE
```

NetTrace XML files can be fetched using File Management. For more information, see Section 4 on page 15.

### 3.2.2 Human-Readable Traces at Min Level

Trace outputs are located in the AppLog, /storage/no-backup/coremw/var/log/saflog/AppTrace\_\*.log. The user locates the so called “start” message, which is a line with the ims.cscf.netio.info domain and Msg: “traceSessionRef: <TraceReference>” where the <TraceReference> is the forlop defined by the user, for example:

```
...pid:581 forlop:237897 id:"ims.cscf.netio.info"
MsgLength:"123" Msg:"traceSessionRef: 1234"
```

The TraceReference in this case is “1234”.

This line is followed by three more AppTrace lines containing the origPublicId, termPublicId, and tracedPublicIds, for example:

```
...pid:581 id:"ims.cscf.netio.info" forlop:237897 ...MsgLe
ngth:"102" Msg:"origPublicId: sip:user_a@cscf.com"
...pid:581 id:"ims.cscf.netio.info" forlop:237897
...MsgLength:"69" Msg:"termPublicId: sip:user_a@cscf.com"
...pid:581 id:"ims.cscf.netio.info" forlop:237897 ...MsgLe
ngth:"36" Msg:"tracedPublicId1: sip:user_a@cscf.com"
```

The forlop, “237897” represents a session that has been traced (associated with TraceReference 1234). Any line that contains “forlop: 237897” represents a header of a traced message or response from the same session, for example:

```
...pid:581 id:"ims.cscf.netio.sip.register" forlop:237897
...MsgLength:"130" Msg:"REGISTER sip:cscf.com"
...pid:581 id:"ims.cscf.netio.sip.register" forlop:237897
...MsgLength:"109" Msg:"To: <sip:user_a@cscf.com>"
...pid:581 id:"ims.cscf.netio.sip.register" forlop:237897
...MsgLength:"84" Msg:"From: <sip:user_a@cscf.com>"
...pid:581 id:"ims.cscf.netio.sip.register" forlop:237897
...MsgLength:"57" Msg:"Call-ID: 18be-147-67840"
...pid:581 id:"ims.cscf.netio.sip.register" forlop:237897
...MsgLength:"20" Msg:"CSeq: 12271 REGISTER"
...pid:186 id:"ims.cscf.netio.dia.cx" forlop:237897
...MsgLength:"85" Msg:" Name: User-Authorization-Answer"
```



```
...pid:186 id:"ms.cscf.netio.dia.cx" forlop:237897  
...MsgLength:"62" Msg:" AVP: Result-Code 2001"
```

### 3.2.3 Human-Readable Traces at Max Level

Trace outputs at this level follow the same principle as those at Min level. The user locates the “start” message as for Min level, notes the `forlop`, and finds the corresponding lines that represent the session.

The only difference when locating the lines for headers at Max level is that the trace domains are `ims.sip.netio.rx`, `ims.sip.netio.rx`, `ims.diaif.netio.rx`, and `ims.diaif.netio.rx`.



## 4 File Management

The CSCF Network Tracing XML files are exposed by File Management in the following file group structure:

- FileGroup=Cscf
  - FileGroup=CscfNetTraceLogs

For more information on file groups, refer to *Handling Files*.