

**NOKIA**

**Release 4  
Nokia Lawful Interception Gateway**

# **CLI User's Guide**

**User Guide**

The information in this document is subject to change without notice and describes only the product defined in the introduction of this documentation. This document is intended for the use of Nokia's customers only for the purposes of the agreement under which the document is submitted, and no part of it may be reproduced or transmitted in any form or means without the prior written permission of Nokia. The document has been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using it. Nokia welcomes customer comments as part of the process of continuous development and improvement of the documentation.

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between Nokia and the customer. However, Nokia has made all reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions. Nokia will, if necessary, explain issues which may not be covered by the document.

Nokia's liability for any errors in the document is limited to the documentary correction of errors. **NOKIA WILL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT OR FOR ANY DAMAGES, INCIDENTAL OR CONSEQUENTIAL (INCLUDING MONETARY LOSSES)**, that might arise from the use of this document or the information in it.

This document and the product it describes are considered protected by copyright according to the applicable laws.

NOKIA logo is a registered trademark of Nokia Corporation.

Other product names mentioned in this document may be trademarks of their respective companies, and they are mentioned for identification purposes only.

Copyright © Nokia Corporation 2005. All rights reserved.

**Contents**

	<b>Summary of changes .....</b>	<b>5</b>
<b>1</b>	<b>Introduction to CLI .....</b>	<b>7</b>
1.1	Purpose .....	7
1.2	Scope .....	7
1.3	Overview .....	7
1.4	Setting up CLI users.....	8
1.5	CLI log file .....	10
1.6	Configuration file .....	11
1.7	Backward compatibility.....	11
<b>2</b>	<b>CLI syntax .....</b>	<b>13</b>
2.1	Input characters .....	13
2.2	Input syntax.....	13
2.2.1	Command extension .....	14
2.2.2	Escaped characters.....	14
2.3	Output characters.....	15
2.4	Output syntax .....	15
2.5	Parameters.....	16
2.6	Return values .....	29
<b>3</b>	<b>CLI commands.....</b>	<b>33</b>
3.1	Overview of CLI commands .....	33
3.2	Command numbers.....	33
3.3	Default values .....	37
3.4	Parameter conditionality in commands .....	37
3.5	Missing parameters in commands.....	38
3.6	Modified and new commands in release 4 .....	39
3.7	Commands for the AA.....	42
3.8	Combined AA and LEA commands.....	50
3.9	Commands for the LEA.....	61
3.10	Commands for the Administrator.....	72
3.11	Commands for the Administrator using CLI Admin .....	77
3.12	Commands for all users .....	85
<b>4</b>	<b>Using CLI.....</b>	<b>93</b>
4.1	Telnet session initialisation and the still alive command .....	93
4.2	Creating AA user account and listing users .....	93
4.3	Changing the password.....	94
4.4	Changing the alarm configuration .....	94
4.5	Showing the root user's public key.....	94
4.6	Listing the LIBs.....	95
4.7	Creating an LEA user account and listing LEA users.....	95
4.8	Authorising an interception and listing authorisations .....	96
4.9	Changing the validity period of an authorisation .....	96

4.10	Listing interceptions.....	97
4.11	Creating File Transfer Configuration (FTC) .....	97
4.12	Changing interception settings .....	97
4.13	Activating an interception .....	98
4.14	Deactivating an interception .....	99
4.15	Revoking an authorisation .....	99
4.16	Managing interception areas .....	99
4.17	Removing an LEA user account .....	100
4.18	Making a backup of the LIC .....	100
4.19	Adding a network element .....	101
4.20	Exiting a CLI session .....	101
	<b>References .....</b>	<b>103</b>
	<b>Glossary .....</b>	<b>104</b>

## Summary of changes

### Changes between releases 4 and 3

#### *Changes in content*

New commands have been added for managing File Transfer Configuration (FTC) files: 108, 109, 110, and 111.

New commands have been added for performing Admin operations: 208, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, and 233

The command changes are summarised in Table 5, *Modified and new CLI commands*.

The following new parameters have been included in LIG Release 4:

AlarmMode, AlarmSuppInfo, AlarmTransfer, DeleteLogs, Description, Filename, FileTransferStatus, FTCId, FTCIdCC, FTCIdIRI, IPPool, LicenseType, LIGRelease, LicensedInterceptions, LicensedLIEs, MCCMNC, Protocol, SIPURI, TELURI, TransmissionProtocol, ULICPort, WarningTime

#### *Changes in documentation*

Figure 1, *CLI between LIC and remote host LIMS*, has been updated.

Information about setting up the cliadmin user has been added to Chapter 1.4, *Setting up CLI users*.

Chapter 1.6, *Configuration file*, has been updated to contain information about the new location of the CLI compatibility parameter.

Chapter 1.7, *Backward compatibility*, has been updated with information about backwards compatibility with version 3.

New parameters have been added to Chapter 2.5, *Parameters*.

New return values have been added to Chapter 2.6, *Return values*.

The command descriptions have been updated, and new commands have been added in Chapter 3, *CLI commands*.

A new chapter has been added: 3.11, *Commands for the Administrator using CLI Admin*.



# 1 Introduction to CLI

## 1.1 Purpose

This document describes the Command Line Interface (CLI), which can be used instead of the Lawful Interception Controller (LIC) web interface. The CLI functions as a means of communication between the Lawful Interception Management System (LIMS) and the Lawful Interception Gateway (LIG). The CLI implements a subset of the LIC web interface actions performed by the Administrator, Authorising Authority (AA), and/or the Law Enforcement Agency (LEA).

The CLI is also used, for instance, if interceptions are activated in different systems such as the Global System for Mobile Communications (GSM) and the General Packet Radio Service (GPRS). The CLI makes it possible to unify the different activation procedures through a common interface.

## 1.2 Scope

The CLI was first supported by Nokia LIG Release 1.1. This document describes the CLI in Nokia LIG Release 4, introducing modified and new commands in the CLI version.

## 1.3 Overview

The CLI provides a restricted machine interface with the LIC. This interface is needed, for instance, when unifying interception activation procedures for different systems.

The CLI supports most actions of the LEA and AA users, and provides a set of commands for the Administrator. A CLI user's remote host uses the CLI

through a virtual terminal protocol, for example Telnet. Secured protocols such as SSH can also be used. The remote host has to provide a virtual terminal client and IPSO has to provide a virtual terminal server. In this document, Telnet is used as an example of a virtual terminal protocol. (Figure 1).

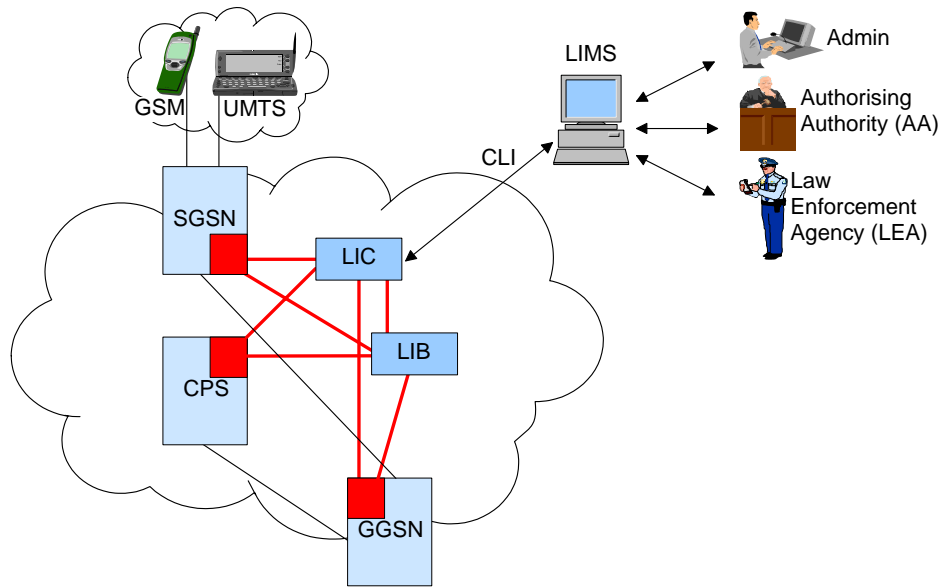


Figure 1. CLI between LIC and remote host LIMS

## 1.4 Setting up CLI users

Initially, no CLI users are defined. The Administrator has to add new CLI users to the LIC.

There are two kinds of users, normal CLI users and a CLI Admin user. A normal CLI user can run non-administrator commands. The CLI Admin user is a new CLI user type in LIG4 and has the privileges to run new admin commands. There can be only one CLI Admin user in the system and the username is always `cliadmin`.

A new normal CLI user can be created by entering, at the LIC command line, the following command:

```
cli <new CLI username> <password>
```

**Example 1. Adding a CLI user**

```
lic> cli imssi password
CLI user imssi created with password password.
lic>
```

A new CLI Admin user can be created by entering, at the LIC command line, the following command:

```
cliadmin <password>
```

**Example 2. Adding a CLI admin user**

```
lic> cliadmin password
CLI user cliadmin created with password password.
lic>
```

The normal CLI user uses the `cli` program and the CLI Admin user uses the `cliadmin` program. The prompts in these programs differ:

The prompt for a regular CLI user:

```
LIC Command Line Interface version 4.0
CLI#
```

The prompt for CLI Admin user:

```
LIC Admin Command Line Interface version 4.0
cliadmin#
```

The Administrator can change the CLI user password using the LIC web interface in the following way (this can also be done with the CLI command 1000):

**Changing the CLI user password**

1. Establish a web connection to the Nokia (Ipsilon) Router Operating System (IPSO) configuration page on the LIC. Use the user account `admin`.
2. Click the **Config** button.
3. Under *Security and Access Configuration*, click the *Users* link
4. Find the CLI username (for example, 'imssi') in the list of users.
5. Type the old password in the **Old password** text box.
6. Type the new password in the **New password** text box.
7. Type the new password again in the **New password (verify)** text box.
8. Click the **Apply** button at the bottom of the page.
9. Click the **Save** button at the top of the page. The user's password has now been changed.

The Administrator can remove the CLI user using the LIC web interface in the following way:



### Removing a CLI user

1. Establish a web connection to the IPSO configuration page on the LIC. Use the user account `admin`.
2. Click the **Config** button.
3. Under *Security and Access Configuration*, click the *Users* link.
4. Find the desired CLI user in the list of users.
5. Select the **Off** radio button.
6. Click the **Apply** button at the bottom of the page.

## 1.5 CLI log file

The CLI provides a log file for administrative purposes. Every CLI user action is recorded in the log file. The log format is as follows:

```
<sequence number><date and time><severity of the log file>  
<process id used by the CLI program><user id><program name>  
<contents of the log file message in the plain text format>
```

### Example 3. Log file message

```
869687 2001-02-13 11:30:25,severity 4,pid 08934,uid  
0000,cli,User clmin executed command 0 with successful  
status.
```

The following actions are recorded:

- who logged in
- who logged out
- all command executions and their status (including erroneous commands)
- some internal error situations, such as a missing or corrupted CLI configuration file

The CLI log file can only be read by the Auditor. For more information, see *Nokia LIG Release 4 Product Documentation: Auditor's Guide*.

## 1.6 Configuration file

The CLI uses encrypted configuration files, which specify the commands that can be used, as well as the maximum number of LEA user accounts allowed. All commands available for the CLI are described in Chapter 3, *CLI commands*. However, the configuration files located in `/var/ligdb/cli.conf` for the CLI and in `/var/ligdb/cliadmin.conf` for CLI Admin in the LIC define the global set of commands which can be used. All commands outside this set are disabled.

Nokia provides the configuration files according to customer request.

The CLI compatibility parameter is on the *LIC General Configuration* web page. CLI compatibility defines the compatibility level of the commands.

## 1.7 Backward compatibility

CLI Release 4 provides a strict backward compatibility mode. It should be used if the Lawful Interception Management System (LIMS) has not been upgraded for the new commands and parameters of CLI Release 3 or 4. If the strict backward compatibility mode is used, the commands that were modified into CLI Release 4 work as they did in CLI Release 2 or 3. That is, the input and output parameters are the same as in the appropriate release.

The Administrator can enable the strict backward compatibility mode on the *LIC General Configuration* web page. The compatibility mode used is set by choosing a value for the parameter CLI compatibility. If the selected value is '2' or '3', the strict backward compatibility is in use. Otherwise, (as the default) all the parameters of release 4 are in use.



# 2 CLI syntax

## 2.1 Input characters

Only visible characters are allowed in the CLI. In addition, to maintain compatibility with the LIC web interface, the following characters should not be used in parameter values: quotation marks ("), ampersand (&), backslash (\), percent mark (%), question mark (?), and equal sign (=).

## 2.2 Input syntax

The CLI input command line uses the following syntax:

```
<command>?<par_1>=<val_1>&...&<par_n>=<val_n><newline>
```

where

- <command> is the command number
- <par\_1> and <par\_n> are the names of parameters for the command
- <val\_1> and <val\_n> are the parameter values, respectively
- <newline> is the line terminator.

The separator character between the command and the parameter value pairs is a question mark (?). If the command has no input parameters, the question mark is not given. The parameter name and value are separated by an equal sign (=), and the parameter-value pairs are separated by an ampersand (&). A line terminator ends an input command line.

---

### Note

All parameter names and values are case sensitive. No spaces are allowed, with the exception of the Secure Shell (SSH) host key value.

---

Example 4. A legal CLI input for authorising an interception

```
1?AAUsername=aauser&IMSI=123456789012345&LEAUsername=lea10000&LIBaddr=1.2.3.4&AuthorizedInterceptType=4&AuthorizedOptions=3&ValidFrom=10.11.2005&StartTime=15:42&ValidTo=10.12.2005&EndTime=15:42&WarrantID=wa538H
```

## 2.2.1 Command extension

The IPSO shell allows a maximum command length of up to 1024 characters. In the CLI this limitation can be bypassed with the command extension feature. When the CLI encounters two consecutive ampersands (&&) at the end of the command (before the line terminator), it returns with a special return value and expects the next command to contain the rest of the command. The following is a simple example of the command extension:

The first command:

```
<command>?<var_1>=<val_1>& ... &<var_k>=<val_k>&&<newline>
```

The second command:

```
&<var_k+1>=<val_k+1>&...&<var_n>=<val_n><newline>
```

The following is the resulting command that is executed:

```
<command>?<var_1>=<val_1>&...&<var_k>=<val_k>&<var_k+1>=<val_k+1>&...&<var_n>=<val_n><newline>
```

The command can be split starting from any character of the command, even inside a variable, but this can only be done once in one command.

## 2.2.2 Escaped characters

There are two cases where the characters in the input have to be specially considered: when there are characters, which are not a part of the 7-bit ASCII character set in SIP URIs, or when the CLI delimiter characters are used in the SIP URIs.

The SIP URI may contain characters that do not belong to the 7-bit ASCII character set. The CPS LIE expects the URI to be a visible ASCII string with all the characters, which are not part of the 7-bit ASCII character set, to be UTF-8 encoded. The LIMS or a CLI user is required to give all non-ASCII characters in the so-called URL-encoded format. In the URL-encoded format, each UTF-8 octet is preceded by a percent sign (%). For example, the character 'ä' (small letter 'a' with dieresis) becomes '%C3%A4'.

The characters '?' and '&' are used as delimiters in CLI input parsing. They both may appear in the SIP URI. The LIMS or a CLI user is required to give all '?' and '&' characters in the same URL-encoded format as described above. Below is an example of an escaped SIP URI.

The escaped version of the SIP URI `name1&name2@company.com` is `name1%26name2@company.com`.

## 2.3 Output characters

The CLI output contains visible characters only. The length of the output line depends on the command and the LIC database values (for example, how many authorisations are defined for a user).

## 2.4 Output syntax

The CLI output uses the following syntax:

```
<command>?<par_1>=<val_1>&...&<par_n>=<val_n>&status=<status and explanation><newline>
```

where

- `<command>` is the input command number
- `<par_1>` and `<par_n>` are the predefined names of parameters needed for the command
- `<val_1>` and `<val_n>` are the parameter values, respectively
- `<status and explanation>` contains the output status of the command (see Chapter 2.6, *Return values*) with an explanatory text
- `<newline>` is the line terminator.

The separator character between the command and the parameter value pairs is a question mark (?). The parameter name and value are separated by an equal sign (=), and the parameter value pairs are separated by an ampersand (&). If the command has no output parameters, no ampersand is displayed (for example, `4? Status=2000k`). In the output there may be a line terminator before the ampersand. Parameters may be returned without a value, which means there is no value in the database for the requested parameter.

The `<status and explanation>` contains a three-digit status code and an explanation text. A line terminator ends the output line.

**Example 5.** CLI output of a successful interception authorisation

```
1?ReqId=1-1203&Status=2000k
```

## 2.5 Parameters

The CLI uses the parameters listed in the following table. All parameter names are case sensitive.

Table 1. Parameters used in CLI input and output

Parameter name	Description and value
AAUsername	The AA user account; from 3 to 8 alphanumeric characters. The first character has to be a letter, for example, 'aa123' and 'Judge'.
AALogLife	The maximum log lifetime (in seconds) for the AA log files. Possible values: <ul style="list-style-type: none"> <li>• 86400</li> <li>• 172800</li> <li>• 345600</li> <li>• 604800</li> <li>• 1209600</li> <li>• 1814400</li> <li>• 2419200</li> <li>• 3024000</li> <li>• 3628800</li> <li>• 4233600</li> <li>• 4838400</li> </ul>
AALogSize	The maximum log size (in bytes) for the AA log files. Possible values: <ul style="list-style-type: none"> <li>• 51200</li> <li>• 76800</li> <li>• 102400</li> <li>• 153600</li> <li>• 204800</li> <li>• 256000</li> <li>• 307200</li> <li>• 409600</li> <li>• 512000</li> <li>• 614400</li> <li>• 716800</li> </ul>

AARealName	The real name of the AA user, from 1 to 30 characters.
AAUserStatus	The status of the AA user (ACTIVE or DEACTIVE).
AdLogLife	The maximum log lifetime (in seconds) for the Administrator log files. Possible values: <ul style="list-style-type: none"> <li>• 900</li> <li>• 1800</li> <li>• 3600</li> <li>• 7200</li> <li>• 21600</li> <li>• 43200</li> <li>• 86400</li> <li>• 172800</li> <li>• 345600</li> <li>• 604800</li> <li>• 1209600</li> </ul>
AdLogSize	The maximum log size (in bytes) for the Administrator log files. Possible values: <ul style="list-style-type: none"> <li>• 51200</li> <li>• 76800</li> <li>• 102400</li> <li>• 153600</li> <li>• 204800</li> <li>• 256000</li> <li>• 307200</li> <li>• 409600</li> <li>• 512000</li> <li>• 614400</li> <li>• 716800.</li> </ul>
AlarmAddr	The IPv4 or IPv6 address where alarms are delivered. In decimal notation, for example, '123.234.2.2' and '22.131.128.34' are legal, but not 'my.host.net.com'.
AlarmHandler	The status of the alarm handler process (ENABLED or DISABLED).
AlarmMode	Describes how Admin alarms are delivered, as normal LIG alarm files or with SNMP. Possible values: <p>1 = file</p> <p>2 = SNMP</p>

	3 = file and SNMP
AlarmPasswd1	The alarm password; from 6 to16 printable ASCII characters.
AlarmPasswd2	The alarm password for verification. This must have the same value as AlarmPasswd1.
AlarmPath	The path name; from 1 to 80 characters. The legality of the value depends on the operating system of the destination.
AlarmSuppInfo	Supplementary alarm information. A character string; from 1 to 80 characters.
AlarmUsername	The username; from 3 to 8 printable ASCII characters. The legality of the value depends on the operating system of the destination.
AuditLogLife	The maximum log lifetime (in seconds) for the Audit log files. Possible values: <ul style="list-style-type: none"> <li>• 900</li> <li>• 1800</li> <li>• 3600</li> <li>• 7200</li> <li>• 21600</li> <li>• 43200</li> <li>• 86400</li> <li>• 172800</li> <li>• 345600</li> <li>• 604800</li> <li>• 1209600</li> </ul>
AuditLogSize	The maximum log size (in bytes) for the Audit log files. Possible values: <ul style="list-style-type: none"> <li>• 51200</li> <li>• 76800</li> <li>• 102400</li> <li>• 153600</li> <li>• 204800</li> <li>• 256000</li> <li>• 307200</li> <li>• 409600</li> <li>• 512000</li> <li>• 614400</li> <li>• 716800.</li> </ul>

AuthorizedInterceptType	The highest authorised interception type given in an authorisation. Possible values: 1 = Interception-Related Information (IRI) 2 = Mobile-originated Communication Content (CC) 3 = IRI and mobile-originated CC 4 = Mobile-terminated CC 5 = IRI and mobile-terminated CC 6 = All CC 7 = IRI and all CC
AuthorizedOptions	The highest authorised processing options given in an authorisation. Possible values: 1 = IRI browsing 2 = IRI and CC file transfer 3 = IRI browsing, and IRI and CC file transfer
BackupDate	The backup date in the format dd.mm.yyyy. This is used in the backup if the backup interval is once a month.
BackupInterval	The backup interval. Possible values: 1 = Never 2 = on defined weekdays (the parameter Weekday is used) 900 = every 15 minutes 1800 = every 30 minutes 3600 = every hour 7200 = every 2 hours 21600 = every 6 hours 43200 = every 12 hours 86400 = every day 2419200 = every month
BackupTime	The backup time in the format hh:mm.
CGI	The cell global identifier or service area identifier. A maximum of 16 characters, only decimal numbers are allowed.
Cleanup	The status of the cleanup. This parameter is not in use in LIG Release 4, but is kept for backwards compatibility reasons. Possible values: <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
CLICompatibility	The CLI compatibility value, which defines the CLI command set version. For example, the value 3 means that the CLI accepts

	only LIG3 CLI commands and the CLI responds are as in LIG3. This does not affect the cliadmin shell functionality. An integer, the range is 2-4.
DeleteLogs	Deletes the user's log files locally on the LIC, therefore no log files are transferred. Possible values: <ul style="list-style-type: none"> <li>on</li> <li>off</li> </ul>
DeliveryIdStart	The delivery function ID start number used in the interception correlation number. An integer, the value range is 1-65535.
Description	A textual description for FTC; from 1 to 50 characters.
EndTime	The end time of the authorisation, in the format hh:mm, where the hours (hh) can be 00 - 23 and the minutes (mm) 00 – 59. For example, '23:00' is a legal value, but not '24:30' or '00:60'
Filename	Defines the name of the license file, for example, <code>license.txt</code> . From 1 to 80 characters. The license files must always be located in the <code>/var/etc/license</code> directory.
FileTransfer	The status of the alarm, logs, and statistics transfer and cleanup. Possible values: <ul style="list-style-type: none"> <li>ENABLED</li> <li>DISABLED</li> </ul>
FileTransferStatus	The file transfer status. Possible values: <p>0 = OK</p> <p>1 = failed</p>
FTCID	The FTC identifier, which has the format <code>&lt;account&gt;-&lt;seq&gt;</code> (for example, <code>leauser-3</code> ). From 1 to 50 characters.
FTCIDCC	The FTC identifier to be used for transferring CC data. From 1 to 50 characters.
FTCIDIRI	The FTC identifier to be used for transferring IRI data. From 1 to 50 characters.
FtpMode	The FTP mode. Possible values: <p>1 = active</p> <p>0 = passive</p>
FwdAddrCC	The IPv4 or IPv6 forwarding address of CC data, in decimal notation. For example, '123.234.2.2' and '22.131.128.34' are legal, but not 'my.host.net.com'.
FwdAddrIRI	The IPv4 or IPv6 forwarding address of IRI data, in decimal notation. For example, '123.234.2.2' and '22.131.128.34' are legal, but not 'my.host.net.com'.
FwdAddr	The IPv4 or IPv6 forwarding address of CC and IRI data, in decimal notation. For example, '123.234.2.2' and '22.131.128.34' are legal, but not 'my.host.net.com'.

FwdDelayCC	The forwarding delay of CC data in seconds. Legal values are 10, 30, 60, 120, 300, 600, 900, 1800, 3600, 7200, 43200, and 86400.
FwdDelayIRI	The forwarding delay of IRI data in seconds. Legal values are 10, 30, 60, 120, 300, 600, 900, 1800, 3600, 7200, 43200, and 86400.
FwdDelay	The forwarding delay of CC and IRI data. Legal values are 10, 30, 60, 120, 300, 600, 900, 1800, 3600, 7200, 43200, and 86400.
FwdPasswd1	The forwarding password; from 6 to 8 characters.
FwdPasswd2	The forwarding password for verification; from 6 to 8 characters. This must have the same value as FwdPasswd1.
FwdPasswdCC	The forwarding password for CC data; from 6 to 8 characters.
FwdPasswdIRI	The forwarding password for IRI data; from 6 to 8 characters.
FwdPathCC	The forwarding path of CC data; from 1 to 80 characters. The legality of the value depends on the operating system of the destination.
FwdPathIRI	The forwarding path of IRI data; from 1 to 80 characters. The legality of the value depends on the operating system of the destination.
FwdPath	The forwarding path of CC and IRI data; from 1 to 80 characters. The legality of the value depends on the operating system of the destination.
FwdSizeCC	The forwarding size of CC data in bytes. The legal values are 50000, 100000, 250000, and 500000.
FwdSizeIRI	The forwarding size of IRI data in bytes. Legal values are 50000, 100000, 250000, and 500000.
FwdSize	The forwarding size of CC and IRI data in bytes; legal values are 50000, 100000, 250000 and 500000.
FwdUsernameCC	The forwarding username for CC data; from 3 to 8 characters. The legality of the value depends on the operating system of the destination.
FwdUsernameIRI	The forwarding username for IRI data; from 3 to 8 characters. The legality of the value depends on the operating system of the destination.
FwdUsername	The forwarding username for CC and IRI data; from 3 to 8 characters. The legality of the value depends on the operating system of the destination.
IAId	The identifier of an interception area. The format is <LIC-SEQ>, where LIC is the LIC code (unsigned integer) and SEQ is the sequence number in the LIC (unsigned integer). For example '1-234' and '222-1' are legal values.
IAName	The name of the interception area. The Administrator can define

	interception areas, a maximum of 30 characters.
IAType	The type of Location Dependent Interception (LDI). This parameter is not in use in LIG Release 4, but is kept for backwards compatibility reasons. Available when CLI compatibility is set to 3. Possible values:  0 = Not used 1 = LDI-
IdentifierPairs	The size of the internal table used in an MSISDN to IMSI conversion. This parameter is not in use in LIG Release 4, but is kept for backwards compatibility reasons.
IMEI	The IMEI number; from 14 to 15 digits. Only numbers are allowed, for example, '12345678901234' is a legal value. The check sum (15 <sup>th</sup> ) bit is not used in the target criteria even if it is included in the value.
IMSI	The IMSI number; from 6 to 15 digits. Only numbers are allowed, for example, '1234567890' and '098765' are legal values
IMSIPrefetch	The IMSI prefetch time; from 0 - 30 seconds. This parameter is not in use in LIG Release 4, but is kept for backwards compatibility reasons.
InterceptionOptionsIRI	The actual processing options given by the LEA for an IRI delivery when activating an interception. Possible values:  2 = Browsing 4 = File transfer 5 = Secure file transfer 6 = Browsing and file transfer 7 = Browsing and secure file transfer 12 = File transfer defined by FTCs 14 = Browsing and file transfer defined by FTCs 16 = strFTP 18 = Browsing and strFTP
InterceptionOptions	The actual processing options given by the LEA when activating an interception (for both CC and IRI if IRI options not separately defined). Possible values:  2 = Browsing 4 = File transfer 5 = Secure file transfer 6 = Browsing and file transfer 7 = Browsing and secure file transfer 12 = File transfer defined by FTCs

	<p>14 = Browsing and file transfer defined by FTCs</p> <p>16 = strFTP</p> <p>18 = Browsing and strFTP</p> <p>20 = ULIC</p> <p>The value 20 can be used only for CC data transfer.</p>
InterceptType	<p>The actual interception type given by the LEA when activating an interception. The InterceptType cannot be higher than the AuthorizedInterceptType given in the corresponding authorisation. Legal values are from 1 to 7:</p> <p>1 = IRI</p> <p>2 = Mobile-originated CC</p> <p>3 = IRI and mobile-originated CC</p> <p>4 = Mobile-terminated CC</p> <p>5 = IRI and mobile-terminated CC</p> <p>6 = All CC</p> <p>7 = IRI and all CC</p>
IPPool	<p>The status of the IP pool functionality of an AA user. Possible values:</p> <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
IPpoolAddr	<p>The IP address in the IP address pool, the IPv4 or IPv6 address.</p>
IPpoolSubnetBits	<p>The netmask of an IP address. The value can be in the range 0 – 128.</p>
IsActive	<p>The status of the interception. If the listed interception is active, the value is 1, otherwise the value is 0.</p> <p>0 = inactive</p> <p>1 = active</p>
LAI	<p>The location area identifier, MCC+MNC+LAC. Only numbers are allowed.</p>
LDI	<p>Location dependent interception. Possible values:</p> <p>1 = Enabled</p> <p>0 = Disabled</p>
LEALogLife	<p>The maximum log lifetime (in seconds) for the LEA log files. Possible values:</p> <ul style="list-style-type: none"> <li>• 86400</li> <li>• 172800</li> <li>• 345600</li> </ul>

	<ul style="list-style-type: none"> <li>• 604800</li> <li>• 1209600</li> <li>• 1814400</li> <li>• 2419200</li> <li>• 3024000</li> <li>• 3628800</li> <li>• 4233600</li> <li>• 4838400</li> </ul>
LEALogSize	<p>The maximum log size (in bytes) for the LEA log files. Possible values:</p> <ul style="list-style-type: none"> <li>• 51200</li> <li>• 76800</li> <li>• 102400</li> <li>• 153600</li> <li>• 204800</li> <li>• 256000</li> <li>• 307200</li> <li>• 409600</li> <li>• 512000</li> <li>• 614400</li> <li>• 716800.</li> </ul>
LEARrealname	<p>Explanatory text about an LEA user; from 1 to 30 characters. For example, the LEA user's real name without spaces.</p>
LEAUserStatus	<p>The status of an LEA user. Possible values:</p> <ul style="list-style-type: none"> <li>• ACTIVE</li> <li>• DEACTIVE</li> </ul>
LEAUsername	<p>An LEA user account, 3 to 8 characters. For example, 'lea123' or 'police'.</p>
LIBaddr	<p>The IPv4 address of an LIB, in decimal notation. For example, '123.234.2.2' and '22.131.128.34' are legal, but not 'my.host.net.com'.</p>
LIBLoad	<p>LIB load balancing. Possible values:</p> <p>1 = On</p> <p>0 = Off</p>
LicenseType	<p>1 = normal</p> <p>2 = testbed</p>

LicensedInterceptions	The maximum number of simultaneous interceptions, an integer value.
LicensedLIEs	The maximum number of network element connections (connections to LIE), an integer value.
LICID	The LIC identifier. A numeric string from 1 to 2147483646.
LICIPv4	The LIC IPv4 address.
LICIPv6	The LIC IPv6 address.
LICMain	The status of the main LIC process. Possible values: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>
LIEDescription	A detailed description of the LIE (textual description).
LIESupportedTargets	The target types supported by the LIE, the bitmask as an integer value. Each bit tells whether the activation of an appropriate target is supported by the LIE. <ul style="list-style-type: none"> <li>• 1st bit is set if IMSI is supported.</li> <li>• 2nd bit is set if MSISDN is supported.</li> <li>• 3rd bit is set if IMEI is supported.</li> <li>• 4th bit is set if SIP URI is supported.</li> <li>• 5th bit is set if TEL URI is supported.</li> </ul> For example, value 31 indicates that the LIE supports all targets. Value 3 indicates that the LIE supports the IMSI and MSISDN.
LIEType	Detailed type of LIE. Possible values: <ul style="list-style-type: none"> <li>0 = Unknown</li> <li>1 = 2G</li> <li>2 = 3G</li> <li>3 = IMM2</li> <li>4 = IMM3</li> </ul>
LIGRelease	The licensed LIG version. A textual presentation, for example, 'LIG4.0'.
LogLevel	The maximum severity allowed for log messages. Possible values: 1-5.
MCC	The mobile country code, 3 digits. For example, '358'.
MCCMNC	The mobile country code and the mobile network code concatenated. A numerical string from 5 to 6 digits. For example, '35835'.
MessageTransmission Limit	Defines the upper limit for internal messages that the LIC will send to the other network elements at a time. This parameter is not in use in LIG Release 4, but is kept for backwards

	compatibility reasons.
MSISDN	The mobile subscriber international ISDN number; from 6 to 20 digits. Only numbers are allowed, for example, '3583512345678' is legal but not '+3583512345678'
NE	The IPv4 or IPv6 address of a network element, in decimal notation. For example, '123.234.2.2' and '22.131.128.34' are legal, but not 'my.host.net.com'.
NEStatus	The connection status of a network element. Legal values are: 0 = unknown 1 = broken 2 = not responding 3 = connection working 4 = establishing connection 5 = unlicensed
NEType	The network element type. Legal values (text strings) are: <ul style="list-style-type: none"> <li>• GGSN</li> <li>• SGSN</li> <li>• LIB</li> <li>• CPS</li> </ul>
NewPassword1	The new password; from 6 to 20 characters.
NewPassword2	The new password for verification; from 6 to 20 characters. This must have the same value as NewPassword1.
OldPassword	The old password; from 6 to 20 characters.
OnOff	The status of a process or a feature. Possible values: <ul style="list-style-type: none"> <li>• on</li> <li>• off</li> </ul>
OpID	The operator identifier; from 1 to 16 characters.
OnTheFly	Support for changing interception type on the fly. Possible values: 1 = Enabled 0 = Disabled
Password1	The password; from 6 to 20 characters.
Password2	The password for verification; from 6 to 20 characters. This must have the same value as Password1.
Port	The listening port of the network element. An integer value within the range 1 – 65535.
Protocol	The protocol used, valid values are: 1 = LIPv1

	2 = LIPv2
QueryType	The query type, legal values are: ACT = list all active interceptions DEA = list all inactive interceptions ALL = list all interceptions UNI = list all uninitialised interceptions
RAI	The routing area identifier, a numerical string of 14 digits.
ReqId	The request identifier of the authorisation; the format is <LIC-SEQ>, where LIC is the LIC code (unsigned integer) and SEQ is the sequence number in the LIC (unsigned integer). This is shown in the list of authorisations. For example, '1-234' and '222-1' are legal values.
RootPublicKey	The SSH root user public key, a maximum of 1200 characters.
SessionEndedDelay	Defines how many seconds the LIC will wait until it forwards the MS Detach event to the LIB. This parameter is not in use in LIG Release 4, but is kept for backwards compatibility reasons.
SAI	The service area identifier, a numerical string of 15 or 16 digits.
SGSNData	Defines the data collection in the SGSN. The allowed values are:  0 = The SGSN collects IRI and CC from all targets.  1 = The SGSN collects all CC and IRI data only if the target is roaming and the GGSN is not in the same backbone as the SGSN, that is, the GGSN does not collect CC data. If the target is not roaming or the GGSN is not in the same backbone as the SGSN, the SGSN does not collect CC data and it does not collect some parts of the IRI data, which can be received from the GGSN. The parts of IRI data, which are not collected in the GGSN, are always collected in the SGSN.  2 = IRI data is collected from all users. The SGSN collects CC data only if the target is roaming and the GGSN is not in the same backbone network as the SGSN.
SIPURI	SIP Uniform Resource Identifier. A character string with a maximum of 256 characters.
SSHHostKey	The SSH host public key, a maximum of 1200 characters.
SSHHostKeyCC	The SSH host public key for CC data, a maximum of 1200 characters.
SSHHostKeyIRI	The SSH host public key for IRI data, a maximum of 1200 characters.
StartTime	The start time of the authorisation, in the format hh:mm. The hours (hh) can be 00 - 23 and the minutes (mm) 00 – 59, for example, '23:00' is a legal value, but not '24:30' or '00:60'.
StatisticsConfiguration	A bit mask which defines LIC statistics collection / filtering

	<p>configuration, 12 characters. The value is a sum of individual bits. The meaning of each bit:</p> <p>LEA traffic total                    000000000001</p> <p>LEA traffic by data type            000000000011</p> <p>LEA interception total              000000000100</p> <p>LEA by interception type          000000001100</p> <p>AA traffic total                      000000010000</p> <p>AA traffic by data type            000000110000</p> <p>AA interception total              000001000000</p> <p>AA by interception type          000011000000</p> <p>Admin traffic total                000100000000</p> <p>Admin traffic by type              001100000000</p> <p>Admin interception total         010000000000</p> <p>Admin by interception type      110000000000</p> <p>Only the bit for traffic total or traffic by data type should be set (if any) for each user. Only the bit for interception total or by interception type should be set (if any) for each user. For example, 110100000101 defines the following configuration: Admin by interception, Admin traffic total, LEA interception total, and LEA traffic total.</p>
Status	The return value of a command. This contains a three-digit code followed by an explanatory text; see Chapter 2.6, <i>Return values</i> .
TELURI	The telephony uniform resource locator. A character string with a maximum of 256 characters.
TransferMethod	The transfer method. Legal values are FTP (file transfer with FTP) or SCP (secure file transfer).
TransmissionProtocol	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• FTP</li> <li>• SCP</li> <li>• strFTP</li> <li>• ULIC</li> </ul>
TunnelEndedDelay	Defines how many seconds the LIC will wait until it forwards the PDP context deactivation event to the LIB. This parameter is not in use in LIG Release 4, but is kept for backwards compatibility reasons.
ULICPort	The ULIC port number, the value should be within the range 1024-65535.
UniqueID	The LIC unique identifier, in the format <LICID><MCC><MNC>. The MCC is left-padded with zeros if it consists of only two digits. For example, 11016040 (LICID = 11, MCC = 16, MNC =

	035) and 12355050 (LICID = 12, MCC = 355, MNC = 035).
Username	The LEA username, AA username, or 'audit' or 'admin' ; from 3 to 8 characters.
ValidFrom	The date the authorisation takes effect. The format is dd.mm.yyyy, where day (dd) can be 01 - 31, month (mm) 01 - 12, and year (yyyy) is given with four digits. For example, '26.09.2001'.
ValidTo	The date the authorisation ends. The format is dd.mm.yyyy, where day (dd) can be 01 - 31, month (mm) 01 - 12, and year (yyyy) is given with four digits. For example, '26.09.2001'.
WarningTime	The license expiry warning time in days. The value should be within the range 1-365.
WarrantID	The warrant identifier. The AA can define a warrant identifier for giving detailed information about an authorisation. This is included in the intercept data sent to the LEA. A maximum of 80 characters.
Weekday	The weekdays on which a backup is made. A bit mask given as 7 characters. The nth least significant bit is set if, and only if, the backup is taken on the nth weekday (Monday is the first weekday). For example, 1000101 means that the backup is taken on Monday, Wednesday, and Sunday. Using the first letter of each day, the meaning of each bit is defined as SSFTWTM.

## 2.6 Return values

Return values are shown in the CLI output using the Status parameter. The values contain a three-digit code followed by an explanatory text. If an error has occurred (the return value is not Ok), the databases are not updated. The following table lists the possible return values.

Table 2. CLI return values

Error code	Explanation text
100	LICError - Syntax error
101	LICError - Unknown command
102	LICError - illegal parameter value
103	LICError - No match in database
104	LICError - access denied
105	LICError - Internal error

106	LICInfo - Waiting for a command extension
107	LICError – System configuration error
108	LICError – Unlicensed action
109	LICError – Value already defined
200	Ok

The return values are described in detail below. If more than one error occurs, only the first error in the input command line is detected.

**100LICError - syntax error**

The syntax of the command line contains an error. The return value is not used in LIG Release 4.

**101LICError - unknown command**

The command line does not start with a defined CLI command (the command is not in the configuration file). The command that caused the error is displayed in the output.

```
CLI# 1234?Ausername=moe&ReqId=1-102
1234?Ausername=moe&ReqId=1-102&Status=101LICError -
unknown command
```

**102LICError - illegal parameter value**

An illegal value was given for a parameter. The parameter with the illegal value is displayed in the output. (In this example, the ReqID parameter contains invalid input characters.) If mandatory parameters have not been defined, this error message is shown, but the value field is empty.

```
CLI# 3?AAUsername=aa1&ReqId=1-a23
3?ReqId=1-a23&Status=102LICError - illegal parameter value
```

**103LICError - no match in the database**

No entry in the database was found matching the query criteria.

```
CLI# 3?AAUsername=aa16&ReqId=1-123
3?Status=103LICError - no match in the database
```

**104LICError - access denied**

The user has no right to access the data, or the required data for the interception is still missing. In this example, ReqID 1-123 has been authorised by aa2, so aa1 cannot access the data. (Additional information may be displayed in some cases.)

```
CLI# 3?AAUsername=aa1&ReqId=1-123
```

```
3?Status=104LICError - access denied
```

### 105LICError - internal error

The CLI has experienced an unspecified internal error. Such errors rarely occur.

```
CLI# 3?AAUsername=aa1&ReqId=1-123
```

```
3?Status=105LICError - internal error
```

### 106LICInfo - waiting for a command extension

The CLI is waiting for a command extension after encountering a command extension string ('&&') at the end of the command.

```
20?AAUsername=aa123&LEAUsername=lea10000&Password1=password
&Password2=password&AlarmUsername=amples&&&
```

```
Status=106LICInfo - Waiting for command extension
```

```
AlarmPasswd1=selpma&AlarmPasswd2=selpma&AlarmPath=/alarms/m
y_alarms&AlarmAddr=2.3.4.5&LEARealname=correct_name
```

```
20?Status=200Ok
```

### 107LICError – System configuration error

An error situation due to incorrect configuration caused the command to fail.

An example of such situation is when the CLI user has tried to add an IMS interception but there is no CPS network element configured in the system.

```
81?SIPURI=test@test.com&LIBaddr=1.2.3.4&AuthorizedOptions=1
&ValidFrom=04.04.2004&StartTime=00:00&ValidTo=04.04.2006&En
dTime=01:00&WarrantID=test&InterceptionOptions=2&InterceptT
ype=1&AuthorizedInterceptType=1&FwdAddrCC=2.3.4.5&FwdDelayC
C=10&FwdSizeCC=50000&FwdUsernameCC=leatest&FwdPasswordCC=pa
sswd&FwdPathCC=/home/leatest&LEAUsername=leatest
```

```
81?NEType=CPS&Status=107LICError - System configuration
error
```

### 108LICError – Unlicensed action

The CLI user has tried to configure unlicensed values for variables. The licensed number of the network connections has already been configured, and adding a new one is not allowed, or the maximum number of active interceptions has been reached.

```
81?AAUsername=aa1&IMSI=123123123&LEAUsername=lea1&LIBaddr=1
.2.3.4&AuthorizedOptions=1&ValidFrom=21.01.2005&StartTime=2
1:20&ValidTo=21.02.2006&EndTime=21:23&WarrantID=warrant&Int
erceptionOptions=2&InterceptType=1&AuthorizedInterceptType=
1
```

```
81?No more active interceptions allowed&Status=108LICError
- Unlicensed action Status=200Ok
```

**109LICError – Value already defined**

The CLI (cliadmin) user has tried to configure a value, which can be defined only once, for example, the LIC IP address

```
222?LICIPv4=111.111.111.111
```

```
222?LICIPv4=&Status=109LICError - Value already defined
```

**200Ok**

The command has been successfully executed. In this example, the AA has created a new LEA user account.

```
CLI#
```

```
20?AAUsername=aa123&LEAUsername=lea10000&Password1=password  
&Password2=password&AlarmUsername=amples&AlarmPasswd1=selpm  
a&AlarmPasswd2=selpma&AlarmPath=/alarms/my_alarms&AlarmAddr  
=2.3.4.5&LEARealname=correct_name20?Status=200Ok
```

# 3 CLI commands

The CLI provides a set of commands for the Administrator, AA, and/or LEA.

## 3.1 Overview of CLI commands

Depending on the command, different input parameter-value pairs have to be given at the command line. The valid parameters are listed for each command. The command line must include all the listed parameter-value pairs except those marked as optional. For example, in command 1 (authorise LEA), it is possible to give the International Mobile Subscriber Identity (IMSI) **or** Mobile Subscriber International ISDN Number (MSISDN) **or** International Mobile Station Equipment Identity (IMEI) **or** Session Initiation Protocol Universal Resource Identifier (SIP URI) **or** Telephone Universal Resource Identifier (TEL URI).

The command line must not include any parameter-value pairs other than the pairs mentioned. All commands end with a line terminator.

The release number of the command line interface is shown at the beginning of the Telnet session. Currently the release number is 4.

Each command definition includes a brief description, any preconditions, the command number, input and output parameters, possible return values, and at least one example.

## 3.2 Command numbers

Because of its machine-to-machine nature, the CLI uses numbers instead of names for commands. The CLI supports a set of commands for the Administrator, AA, and LEA users. Some commands are for both the AA and LEA users. There is also a set for all users (AA, LEA, and Administrator).

Number 0 is reserved for the help command for all users.

Numbers 1 - 79 are reserved for AA user commands (1 - 19 are for authorisation management and 20 - 30 for user management commands).

Numbers 80 - 99 are reserved for combined LEA and AA user commands.

Numbers 100 - 199 are reserved for LEA user commands.

Numbers 200-207 are reserved for Administrator commands.

Numbers 1000 - 1099 are reserved for commands for all users.

Numbers 208 - 240 are reserved for Administrator commands using `cliadmin`. Only the CLI Admin user can run the new Administrator commands 208-233.

The following table lists the commands currently supported. A more detailed description of each command can be found in Chapters 3.5 –3.10.

Table 3. Currently supported CLI commands

Command	Action	CLI	CLI Admin
0	Help	x	x
<b>AA</b>			
1	Authorise an interception	x	
2	List current authorisations	x	
3	View details of an authorisation	x	
4	Modify the validity period of an authorisation	x	
5	Revoke an authorisation	x	
6	List existing LIBs	x	
7	Redefine the LIB for an interception	x	
20	Create a new LEA user	x	
21	List current LEA users	x	
22	Remove an LEA user account	x	
23	Create an LIB account for an LEA user	x	
24	Remove an LEA user's LIB account	x	
25	List an LEA user's LIB accounts	x	
26	Activate/deactivate an LEA user	x	
30	Add/Remove IP pool addresses	x	
<b>Combined AA and LEA</b>			

<b>Command</b>	<b>Action</b>	<b>CLI</b>	<b>CLI Admin</b>
80	Set default values for a current CLI user	x	
81	Create and activate an interception	x	
82	Deactivate and remove an interception	x	
83	Modify an interception	x	
84	View details of an interception / List all authorisations	x	
85	Show the default values for a current CLI user	x	
86	Remove a CLI user's default values	x	
87	Deactivate and remove all interceptions in the LIC	x	
88	View details of all interceptions	x	
89	Exit the CLI session and close the Telnet connection	x	
90	List IP pool addresses	x	
<b>LEA</b>			
100	List interceptions	x	
101	Activate an interception	x	
102	Deactivate an interception	x	
103	Change the options of an interception (when the same IRI & CC destinations are used)	x	
104	View details of an interception	x	
105	Change the options of an interception (when different IRI and CC destinations are used)	x	
106	Set strFTP delivery options	x	
107	Show strFTP delivery options	x	
108	Add FTC	x	
109	Modify FTC	x	
110	Remove FTC	x	
111	View FTC	x	
<b>Administrator</b>			
200	View the general configuration of the	x	x

Command	Action	CLI	CLI Admin
	LIC		
201	View the status of LIC processes	x	x
202	List current AA users	x	x
203	View the backup configuration	x	x
204	Perform the backup procedure	x	x
205	Define a new interception area	x	x
206	Set Loadbalancing On / Off	x	x
207	Set IP pool On / Off	x	x
<b>Administrator using cliadmin</b>			
208	View license configuration		x
220	Initialise license		x
221	Manage license configuration		x
222	Manage general configuration		x
223	Manage statistics configuration		x
224	Manage backup configuration		x
225	Manage LIC processes		x
226	Add network element		x
227	Remove network element		x
228	Create an AA user		x
229	Modify AA user		x
230	Remove an AA user		x
231	Set alarm mode		x
232	Send alarm		x
233	Regenerate password		x
<b>AA, LEA, and Administrator</b>			
1000	Change the password	x	x
1001	Change the alarm configuration	x	x
1002	Exit the CLI session and close the Telnet connection	x	x
1003	Show the root user's SSH public key	x	x
1004	View all network elements (NE)	x	x
1005	Show the alarm configuration	x	x

---

Command	Action	CLI	CLI Admin
1006	Execute a no operation command	x	x
1007	List interception areas	x	x
1008	View details of the interception area	x	x

### 3.3 Default values

It is possible to define default values for parameters for a normal CLI user. The default values are not supported for the CLI Admin user. The default values are for each CLI user, so all normal CLI users can have their own default values set for certain parameters. This is done to avoid needless typing of parameters.

If a default value is defined for some parameter, for example, the value for the LEAUsername parameter, it does not have to be given in the command line. However, if LEAUsername is given in the command line and a default value has been set into the system, the command line value is used instead.

---

#### Note

If a default value is defined for some parameter, it is **always** used in all commands where applicable when the parameter is not given in the command line.

---

### 3.4 Parameter conditionality in commands

All parameter-value pairs are conditional. This means that each parameter-value pair can have a different status in each command. The following table lists all the possible status conditions. Each status condition has an abbreviation, which is used for the command descriptions in Chapter 3.7, *Commands for the AA*, to Chapter 10, *Commands for the Administrator*. Each input parameter for a command will have its possible conditions listed in parentheses, for example:

Input parameters:

- AAUsername (M, D)

This means the AAUsername parameter-value pair is mandatory (M) in the command line input, but if a default value is defined (D), it can be left out of the input.

Table 4. Conditions of input parameter-value pairs

Abbreviation	Condition
D	The default value can be used if it has been defined.
M	A mandatory parameter.
MF	Mandatory if FTP is used.
MFC	Mandatory if FTP is used and CC is collected.
MFI	Mandatory if FTP is used and IRI is collected.
MS	Mandatory if SCP is used.
MSC	Mandatory if SCP is used and CC is collected.
MSI	Mandatory if SCP is used and IRI is collected.
MUC	Mandatory if ULIC is used for CC.
O	Optional

### 3.5 Missing parameters in commands

A parameter in a command can be mandatory (M) or optional (O). In some commands the parameter is conditional, that is, a parameter is mandatory depending on some other parameters.

If a mandatory parameter is missing, the CLI does not execute the command and returns an error code.

If an optional parameter is missing, the CLI executes the command normally using other parameters found in the command line or in the default values file if applicable.

---

#### Note

If a command has only optional parameters, the command succeeds even if there are no parameters given.

---



---

#### Note

All the parameter names and values are case sensitive. If an optional parameter is mistyped, the command is executed as if the parameter was omitted.

---

### 3.6 Modified and new commands in release 4

Modified and new commands in release 4 are described below. In the case of modified commands, the Changes field defines the difference in the usage and/or parameters of the commands between CLI Release 3 and CLI Release 4.

Table 5. Modified and new CLI commands

Command	Status	Changes
0 – Help	Modified	New commands have been added to the output.
1 - Authorise an interception	Modified	SIPURI and TELURI can now be used as input parameters, the IAType parameter has been removed.  The command number has been added as the start of the output.
2 – List current interceptions	Modified	SIPURI and TELURI have been added to the output.
3 – View details of an authorisation	Modified	SIPURI and TELURI output parameters have been added, the IAType output parameter has been removed.
4 – Modify the validity period of an authorisation	Modified	The validity period can be also shortened.
20 – Create a new LEA user	Modified	Support for LEA user inheritance has been removed.
30 – Add /Remove IP pool addresses	Modified	AAUsername is now a mandatory parameter.
81 – Create and activate an interception	Modified	SIPURI and TELURI can now be used, the IAType parameter has been removed. ULICPort has been added as input.
83 – Modify an existing interception	Modified	The IAId and AType parameters have been removed.
84 – View details of an interception / List all interceptions	Modified	SIPURI and TELURI output parameters have been added, the IAType parameter has been removed from the output.
88 – View details of all interceptions	Modified	SIPURI, TELURI and Port output parameters have been added, the IAType parameter has been removed from the output. The ULICPort output parameter has been added.
100 – List interceptions of LEA user	Modified	SIPURI and TELURI output parameters have been added.
101 – Activate	Modified	The ValidFrom, ValidTo, StartTime, and EndTime parameters

interception		can now be used for defining the activation start and end date and time.
103 – Change interception settings	Modified	The FTCLd and ULICPort parameters have been added. The functionality has changed so that in LIG4 the FTCLdCC and FTCLdIRI parameters have precedence over other transfer configuration parameters.
104 – View details of an interception	Modified	The SIPURI, TELURI, FTCLdCC, and FTCLdIRI output parameters have been added. The IAType output parameter has been removed. The ULICPort output parameter has been added.
105 – Change interception settings	Modified	Support for the FTCLdCC and FTCLdIRI input parameters has been added. The ULICPort input parameter has been added.
108 – Add FTC	New	Used to add new FTC.
109 – Modify FTC	New	Used to modify the existing FTC.
110 – Remove FTC	New	Used to remove the existing FTC.
111 – View FTC	New	Used to view the parameters of the existing FTC.
200 – View the general configuration of the LIC	Modified	The MCCMNC, DeliveryIdStart, LIBLoad, LDI, FtpMode, and CLICompatibility parameters have been added. The SessionEndedDelay, TunnelEndedDelay, MessageTransmissionLimit, IdentifierPairs, and IMSIPrefetch parameters have been removed.
201 – View the status of LIC processes	Modified	The Cleanup output parameter has been removed.
202 – List current AA users	Modified	The IPPool output parameter has been added.
203 – View backup configuration	Modified	The TransferMethod output parameter has been added.
205 – Define a new interception area	Modified	Support for new interception area types has been added. The IAId output parameter has been added.
208 – View license configuration	New	Used by the Admin to view the LIG licence properties.
220 – Initialise license	New	Used by the CLI Admin user to initialise the LIG licence.
221 – Manage license configuration	New	Used by the CLI Admin user to change the LIG licence-related setting.
222 – Manage general configuration	New	Used by the CLI Admin user to change general configuration parameters.

223 – Manage statistics configuration	New	Used by the CLI Admin user to change the statistics configuration.
224 – Manage backup configuration	New	Used by the CLI Admin user to change the backup configuration.
225 – Manage LIC processes	New	Used by the CLI Admin user to manage the status of LIC processes.
226 – Add a network element	New	Used by the CLI Admin user to add new network element(s).
227 – Remove a network element	New	Used by the CLI Admin user to remove a network element.
228 – Create AA user	New	Used by the CLI Admin user to create a new AA user.
229 – Modify AA user	New	Used by the CLI Admin user to modify the AA user.
230 – Remove an AA user	New	Used by the CLI Admin user to remove the AA user.
231 – Set administrator alarm mode	New	Used by the CLI Admin user to set the Administrator user's alarm mode.
232 – Send alarm	New	Used by the CLI Admin user to send alarms.
233 – Generate a new password	New	Used by the CLI Admin user to generate a new password for the AA or LEA user.
1001 – Change alarm configuration	Modified	The DeleteLogs parameter has been added.
1004 – View all network elements	Modified	New output parameters have been added: Port, OnTheFly, Protocol, LIEType, LIEDescription, and LIESupportedTargets. The name of the command has been changed (does not affect input or output)
1005 – Show alarm configuration	Modified	New output parameters have been added: FileTransferStatus and DeleteLogs.
1008 – View details of the interception area	Modified	New output parameters have been added: MCC, MCCMNC, LAI, and IAId.

## 3.7 Commands for the AA

### 1 - Authorise an interception

Description: The AA can use this command to authorise an LEA user to intercept a target. The IAId parameter is used only if the authorisation is for a location dependent interception.

Preconditions:

- The Administrator has created the AA user account using the LIC web interface.
- The AA user has created the LEA user account.
- A Lawful Interception Browser (LIB) account has been created for the LEA user in the current LIBaddr.

Command number: 1

Input parameters:

- AAUsername (M, D)
- IMSI or MSISDN or IMEI or SIPURI or TELURI (M for one; if more than one is given, the first one read is used)
- LEAUsername (M, D)
- LIBaddr (M, D)
- AuthorizedInterceptType (M, D)
- AuthorizedOptions (M, D)
- ValidFrom (M, D)
- StartTime (M, D)
- ValidTo (M, D)
- EndTime (M, D)
- WarrantID (M)
- IAId (O)

Output parameters:

- ReqId

Return values: 102, 103, 104, 105, 107, 108, or 200

CLI#

```
1?AAUsername=aatest1&IMSI=123123123&LEAUsername=leatest1&LIBaddr=1.2.3.4&AuthorizedInterceptType=7&AuthorizedOptions=3&ValidFrom=21.02.2005&StartTime=21:20&ValidTo=21.02.2007&EndTime=21:21&WarrantID=testwarrant
```

```
1?ReqId=100-195&Status=200Ok
```

## 2 - List current authorisations

Description: The AA can use this command to list its current authorisations.

Preconditions: The Administrator has created the AA user account using the LIC web interface.

Command number: 2

Input parameter: AAUsername (M, D)

Output parameters (for each authorisation):

- ReqId
- IMSI and MSISDN and IMEI and SIPURI and TELURI
- LEAUsername
- LIBaddr

Return values: 102, 103, 104, 105 or 200

CLI# **2?AAUsername=aa judge**

```
2?ReqId=100-44&IMSI=12312344&MSISDN=&IMEI=&SIPURI=&TELURI=&LEAUsername=lea judge&LIBaddr=1.2.3.4&ReqId=100-45&IMSI=12312344&MSISDN=&IMEI=&SIPURI=&TELURI=&LEAUsername=lea judge&LIBaddr=1.2.3.4&ReqId=100-46&IMSI=&MSISDN=&IMEI=12312344&SIPURI=&TELURI=&LEAUsername=lea judge&LIBaddr=1.2.3.4&ReqId=100-47&IMSI=&MSISDN=12312344&IMEI=&SIPURI=&TELURI=&LEAUsername=lea judge&LIBaddr=1.2.3.4&
```

```
Status=2000k
```

## 3 - View details of an authorisation

Description: The AA can use this command to view the details of one of its authorisations.

Preconditions:

- The Administrator has created the AA user account using the LIC web interface.
- The AA user has authorised a target with ReqId.

Command number: 3

Input parameters:

- AAUsername (M, D)
- ReqId (M)

Output parameters:

- ReqId
- IMSI and MSISDN and IMEI and SIPURI and TELURI
- ValidFrom

- ValidTo
- StartTime
- EndTime
- AuthorizedOptions
- AuthorizedInterceptType
- LEAUsername
- LIBaddr
- WarrantID
- IAId

Return values: 102, 103, 104, 105, or 200

CLI# **3?AAUsername=aa\_judge&ReqId=100-44**

```
3?ReqId=100-44&IMSIO=12312344&MSISDN=&IMEI=&ValidFrom=21.01.2005&ValidTo=21.03.2007&StartTime=21:20&EndTime=21:30&AuthorizedOptions=3&AuthorizedInterceptType=7&LEAUsername=leajudge&LIBaddr=1.2.3.4&WarrantID=<Warrant_identifier_here>&IAId=&IAType=&Status=200Ok
```

#### 4 - Modify the validity period of an authorisation

Description: The AA can use this command to modify the period of validity for one of its authorisations. If the interception is active, the command also automatically sets the active period end time to the same value as the validity period end time.

Preconditions:

- The Administrator has created the AA user account using the LIC web interface.
- The AA user has authorised a target with ReqId.

Command number: 4

Input parameters:

- AAUsername (M, D)
- ReqId (M)
- ValidTo (M)
- EndTime (M)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

CLI#

```
4?AAUsername=aa_judge&ReqId=100-44&ValidTo=21.03.2006&EndTime=21:23
```

```
4?Status=200Ok
```

### 5 - Revoke an authorisation

Description: The AA users can use this command to revoke one of their authorisations.

Preconditions:

- The Administrator has created the AA user account using the LIC web interface.
- An AA user has authorised a target with ReqId.

Command number: 5

Input parameters:

- AAUsername (M, D)
- ReqId (M)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

```
CLI# 5?AAUsername=aa judge&ReqId=100-44
5?Status=200Ok
```

### 6 - List Lawful Interception Browsers

Description: This command generates a list of existing LIBs.

Preconditions: None

Command number: 6

Input parameters: None

Output parameter (for each LIB): LIBAddr

Return values: 104, 105, or 200

```
CLI# 6
6?LIBAddr=1.2.3.4&LIBAddr=2.3.4.5&LIBAddr=3.4.5.6&Status=200Ok
```

### 7 - Redefine LIB for an interception

Description: The AA can use this command to redefine the LIB used for an interception.

Preconditions:

- ReqId exists.
- The ReqId does not have LIBAddr.

Command number: 7

Input parameters:

- AAUsername (M, D)

- ReqId (M)
- LIBaddr (M, D)

Output parameters: None

Return values: 104, 105, or 200

```
CLI# 7?AAUsername=aajudge&ReqId=100-48&LIBaddr=1.2.3.4
7?Status=200Ok
```

## 20 - Create a new LEA user

Description: The AA can use this command to create a new LEA user account.

Preconditions:

- The Administrator has created the AA user account using the LIC web interface.
- The new LEA username is not currently in use.
- The maximum number of LEA user accounts has not been reached.

Command number: 20

Input parameters:

- AAUsername (M, D)
- LEAUsername (M)
- Password1 (M)
- Password2 (M)
- LEARealname (M)

Output parameters: None

Return values: 102, 103, 104, 105 or 200

```
CLI#
20?AAUsername=aajudge&LeAUsername=leajudge&Password1=leajud
ge&Password2=leajudge&LEARealname=leajudge_1
20?Status=200Ok
```

## 21 - List current LEA users

Description: The AA can use this command to list current LEA users.

Preconditions: The Administrator has created the AA user account using the LIC web interface.

Command number: 21

Input parameter: AAUsername (M, D)

Output parameters (for each LEA):

- LEAUsername
- LEARealname
- LEAUserStatus

Return values: 104, 105, or 200

CLI# **21?AAUsername=aa judge**

```
21?LEAUsername=leajudge&LEARealname=leajudge_1&LEAUserStatus=ACTIVE&LEAUsername=leaoop&LEARealname=leajudge_2&LEAUserStatus=DEACTIVE&Status=200Ok
```

## **22 - Remove an LEA user account**

Description: The AA can use this command to remove an LEA user account.

Preconditions:

- The Administrator has created the AA user.
- LEAUsername exists and was created by the AA user .

Command number: 22

Input parameters:

- AAUsername (M, D)
- LEAUsername (M, D)

Output variables: None

Return values: 102, 103, 104, 105, or 200

CLI# **22?AAUsername=aa judge&LEAUsername=leaoop**

```
22?Status=200Ok
```

## **23 - Create an LIB account for the LEA**

Description: The AA user who created the LEA user account can use this command to create an LIB account for an LEA.

Preconditions:

- LEAUsername exists.
- At least one LIBaddr exists and LEAUsername does not yet have an account.

Command number: 23

Input parameters:

- LEAUsername (M, D)
- LIBaddr (M, D)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

```
CLI# 23?LEAUsername=leajudge&LIBaddr=1.2.3.4
23?Status=2000k
```

#### 24 - Remove an LEA user's LIB account

Description: The AA user who created the LEA user account can use this command to delete an LEA user's LIB account.

Preconditions:

- LEAUsername exists.
- LEAUsername has an LIB account.

Command number: 24

Input parameters:

- LEAUsername (M, D)
- LIBaddr (M, D)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

```
CLI# 24?LEAUsername=leajudge&LIBaddr=1.2.3.4
24?Status=2000k
```

---

#### Note

If an LIB account is deleted, all of the LEA user's interceptions with that particular LIBaddr will be deactivated and they must be reconfigured manually after using this command.

---

#### 25 - Show LEA user's LIB accounts

Description: The AA user who created the LEA user account can use this command to display the LIB accounts of an LEA user.

Preconditions: LEAUsername exists.

Command number: 25

Input parameters: LEAUsername (M, D)

Output parameter (for each LIB account):

- LIBaddr

Return values: 102, 103, 104, 105, or 200

```
CLI# 25?LEAUsername=leajudge
25?LIBaddr=1.2.3.4&LIBaddr=2.3.4.5&Status=2000k
```

### 26 - Activate/deactivate an LEA user

Description: The AA user who created the LEA user account can use this command to activate or deactivate the LEA user. The deactivated LEA user cannot access the LIG system.

Preconditions: LEAUsername exists.

Command number: 26

Input parameters:

- AAUsername (M, D)
- LEAUsername (M, D)
- LEAUserStatus (M)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

```
CLI# 26?LEAUsername=lea_judge&LeaUserStatus=DEACTIVE
26?Status=200Ok
```

### 30 - Add/Remove IP pool addresses

Description: The AA user who created the LEA user account can use this command to add or remove an IP address range into the IP address pool of an LEA user. IP address ranges can be used to restrict the destinations where the LEA users can forward data. The address range is defined by a network or a host IP address and a subnetmask. A single host can be designated for the LEA user by setting the IPpoolSubnetBits parameter to the maximum length (number of bits) of address.

Preconditions: LEAUsername exists and the IP pool functionality has been enabled for the AA user by the Administrator

Command number: 30

Input parameters:

- AAUsername (M, D)
- LEAUsername (M, D)
- IPpoolAddr (M)
- IPpoolSubnetBits (M)
- OnOff (M)

Output parameters: None

Return values: 102, 105, or 200

```
CLI#
30?AAUsername=aa1&LEAUsername=lea1&IPpoolAddr=127.0.0.0&IPp
oolSubnetBits=24&OnOff=on
30?Status=200Ok
```

**Note**

When the CLI finds a conflicting address in the FwdAddr, FwdAddrIRI, or FwdAddrCC fields, or in the address field of the FTC specified by FTCTIdIRI or FTCTIdCC, error 102 (Illegal parameter value) is returned.

---

## 3.8 Combined AA and LEA commands

### 80 - Set default values for the current CLI user

Description: This command sets the default values for the current CLI user. The default values for one or several parameters can be set with the same command. If the same parameter name is given many times, the first parameter-value pair is stored into the database, and the other occurrences are ignored. (The default values can be deleted with the command 86.) The values given in the command line will be used as the new default values.

Preconditions: None

Command number: 80

Input parameters (all optional):

- AAUsername (O)
- LEAUsername (O)
- LIBaddr (O)
- AuthorizedInterceptType (O)
- AuthorizedOptions (O)
- InterceptionOptions (O)
- InterceptionOptionsIRI (O)
- InterceptType (O)
- ValidFrom (O)
- ValidTo (O)
- StartTime (O)
- EndTime (O)
- AlarmAddr (O)
- AlarmPath (O)
- AlarmUsername (O)
- AlarmPasswd1 (O)

- AlarmPasswd2 (O)
- FwdAddrIRI (O)
- FwdAddrCC (O)
- FwdPathIRI (O)
- FwdPathCC (O)
- FwdUsernameIRI (O)
- FwdUsernameCC (O)
- FwdPasswordIRI (O)
- FwdPasswordCC (O)
- FwdDelayIRI (O)
- FwdDelayCC (O)
- FwdSizeIRI (O)
- FwdSizeCC (O)
- SSHHostKey (O)
- SSHHostKeyCC (O)
- SSHHostKeyIRI (O)

---

**Note**

Default values can be set for any of the parameters listed above.

---

Output parameters: None

Return values: 102, 103, 104, 105, or 200

CLI#

```
80?AAUsername=aaCli&LEAUsername=leaCli&LIBaddr=10.100.196.6
```

```
80?Status=200Ok
```

**81 - Create and activate an interception**

Description: This command is used to create and activate an interception.

Preconditions: Command 106 must be executed before an interception using strFTP can be activated.

Command number: 81

Input parameters:

- AAUsername (M, D)
- IMSI or MSISDN or IMEI or SIPURI or TELURI (M)
- LEAUsername (M, D)

- LIBaddr (M, D)
- AuthorizedOptions (M, D)
- ValidFrom (M, D)
- StartTime (M, D)
- ValidTo (M, D)
- EndTime (M, D)
- WarrantID (M)
- InterceptionOptions (M, D)
- InterceptionOptionsIRI (O, D; input is required if a different transfer method is used for IRI data)
- InterceptType (M, D)
- AuthorizedInterceptType (M, D)
- FwdPathCC (MFC, MSC, D)
- FwdPathIRI (MFI, MSI, D)
- FwdUsernameCC (MFC, MSC, D)
- FwdUsernameIRI (MFI, MSI, D)
- FwdPasswordCC (MFC, D)
- FwdPasswordIRI (MFI, D)
- FwdAddrCC (MFC, MSC, D)
- FwdAddrIRI (MFI, MSI, D)
- FwdDelayCC (MFC, MSC, D)
- FwdDelayIRI (MFI, MSI, D)
- FwdSizeCC (MFC, MSC, D)
- FwdSizeIRI (MFI, MSI, D)
- SSHHostKeyCC (MSC, D)
- SSHHostKeyIRI (MSI, D)
- IAId (O)
- ULICPort (MUC)

Output parameter: ReqId

Return values: 102, 103, 104, 105, 107, or 200

Example 6. (IRI and CC data use the FTP transfer method)

```
CLI#  
81?AAUsername=aatest1&IMSI=123123123&LEAUsername=leatest1&L
```

```
IBaddr=1.2.3.4&AuthorizedOptions=3&ValidFrom=21.01.2005&StartTime=21:20&ValidTo=21.02.2007&EndTime=21:23&WarrantID=warrant&InterceptionOptions=6&InterceptType=7&AuthorizedInterceptType=7&FwdPathCC=./&FwdPathIRI=./&FwdUsernameCC=CCuser&FwdUsernameIRI=IRIuser&FwdPasswordCC=CCpass&FwdPasswordIRI=IRIpass&FwdAddrCC=1.2.3.4&FwdAddrIRI=2.3.4.5&FwdDelayCC=10&FwdSizeCC=50000&FwdDelayIRI=10&FwdSizeIRI=50000
```

```
81?ReqId=100-197&Status=200Ok
```

Example 7. (IRI and CC data use the SCP transfer method)

CLI#

```
81?AAUsername=aatest1&IMSI=123123123&LEAUsername=leatest1&LIBaddr=1.2.3.4&AuthorizedOptions=3&ValidFrom=21.01.2005&StartTime=21:20&ValidTo=21.02.2007&EndTime=21:23&WarrantID=warrant&InterceptionOptions=7&InterceptType=7&AuthorizedInterceptType=7&FwdPathCC=./&FwdPathIRI=./&FwdUsernameCC=CCuser&FwdUsernameIRI=IRIuser&FwdAddrCC=1.2.3.4&FwdAddrIRI=2.3.4.5&SSHHostKeyCC=CCkey&SSHHostKeyIRI=IRIkey&FwdDelayCC=10&FwdSizeCC=50000&FwdDelayIRI=10&FwdSizeIRI=50000
```

```
81?ReqId=100-199&Status=200Ok
```

Example 8. (CC data transferred with SCP, and IRI data transferred using the FTP)

CLI#

```
81?AAUsername=aatest1&IMSI=123123123&LEAUsername=leatest1&LIBaddr=1.2.3.4&AuthorizedOptions=3&ValidFrom=21.01.2005&StartTime=21:20&ValidTo=21.02.2007&EndTime=21:23&WarrantID=warrant&InterceptionOptions=7&InterceptionOptionsIRI=6&InterceptType=7&AuthorizedInterceptType=7&FwdPathCC=./&FwdPathIRI=./&FwdUsernameCC=CCuser&FwdUsernameIRI=IRIuser&FwdPasswordIRI=IRIpass&FwdAddrCC=1.2.3.4&FwdAddrIRI=2.3.4.5&SSHHostKeyCC=CCkey&FwdDelayCC=10&FwdSizeCC=50000&FwdDelayIRI=10&FwdSizeIRI=50000
```

```
81?ReqId=100-201&Status=200Ok
```

Example 9. (creating and activating an interception with the strFTP)

CLI#

```
81?AAUsername=aatest1&IMSI=123123123&LEAUsername=leatest1&LIBaddr=1.2.3.4&AuthorizedOptions=3&ValidFrom=21.01.2005&StartTime=21:20&ValidTo=21.02.2007&EndTime=21:23&WarrantID=warrant&InterceptionOptions=16&InterceptType=7&AuthorizedInterceptType=7
```

```
81?ReqId=100-202&Status=200Ok
```

**82 - Deactivate and remove an interception**

Description: This command deactivates and removes an interception.

Preconditions:

- Active interception exists for ReqId.
- AAUsername and LEAUsername exists.

Command number: 82

Input parameters:

- AAUsername (M, D)
- LEAUsername (M, D)
- ReqId (M)

Output parameters: None

Return values: 102, 103, 104, 105 or 200

```
CLI# 82?AAUsername=aatest1%LEAUsername=leatest1&ReqId=100-32
```

```
82?Status=200Ok
```

**83 - Modify an existing interception**

Description: With this command the user can change the interception parameters when the interception is active. The interception type may be changed during an active interception. However, the transferring method cannot be altered when the interception is active.

Preconditions: The interception ReqId exists. Command 106 must be executed before an interception using strFTP can be activated.

Command number: 83

Input parameters (optional parameters are entered only if the value changes):

- AAUsername (M, D)
- ReqId (M)
- LEAUsername (M, D)
- FwdAddrIRI (O)
- InterceptType (O)
- FwdAddrCC (O)
- FwdDelayCC (O)
- FwdDelayIRI (O)
- FwdPasswordIRI (O)
- FwdPasswordCC (O)
- FwdSizeCC (O)

- FwdSizeIRI (O)
- FwdUsernameIRI (O)
- FwdUsernameCC (O)
- FwdPathCC (O)
- FwdPathIRI (O)
- SSHHostKeyCC (O)
- SSHHostKeyIRI (O)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

```
CLI# 83?AAUsername=aatest1&LEAUsername=leatest1&ReqId=5-32&FwdPathIRI=.
```

```
83?Status=200Ok
```

#### **84 - Detailed view of an interception / List all interceptions for the used AA user**

Description: This command lists detailed information about an interception. If the ReqId variable is not given in the command, all interceptions for the given AA user are listed (without full details).

Preconditions: None

Command number: 84

Input parameters:

- AAUsername (M, D)
- LEAUsername (M if ReqId is given, D)
- ReqId (M if LEAUsername is given)

Output parameters for each interception if ReqId is not given:

- ReqId
- IMSI
- MSISDN
- IMEI
- SIPURI
- TELURI
- LEAUsername
- LIBaddr

Output parameters if ReqId is given:

- ReqId

- IMSI
- MSISDN
- IMEI
- SIPURI
- TELURI
- ValidFrom
- ValidTo
- StartTime
- EndTime
- AuthorizedOptions
- AuthorizedInterceptType
- InterceptType
- IsActive
- LIBaddr
- InterceptionOptions
- InterceptionOptionIRI
- FwdPathCC
- FwdPathIRI
- FwdUsernameCC
- FwdUsernameIRI
- WarrantID
- FwdAddrCC
- FwdAddrIRI
- FwdDelayCC
- FwdDelayIRI
- FwdSizeCC
- FwdSizeIRI
- SSHHostKeyCC
- SSHHostKeyIRI
- IAId

Return values: 102, 103, 104, 105, or 200

**Example 10. With ReqID**

```
CLI# 84?AAUsername=aatest1&LEAUsername=leatest1&ReqId=100-201

84?ReqId=100-201&IMSI=123123123&IMEI=&MSISDN=&SIPURI=&TELURI=&ValidFrom=21.01.2005&ValidTo=21.02.2007&StartTime=21:20&EndTime=21:23&AuthorizedOptions=3&AuthorizedInterceptType=7&InterceptType=7&IsActive=1&LIBaddr=1.2.3.4&InterceptionOptions=7&InterceptionOptionsIRI=6&FwdPathCC=./&FwdPathIRI=./&FwdUsernameCC=CCuser&FwdUsernameIRI=IRIuser&WarrantID=warrant&FwdAddrCC=1.2.3.4&FwdAddrIRI=2.3.4.5&SSHHostKeyCC=newCCKey&SSHHostkeyIRI=newCCKey&IAId=& Status=2000k
```

**Example 11. Without ReqID**

```
CLI# 84?AAUsername=aatest1

84?ReqId=100-196&IMSI=123123123&MSISDN=&IMEI=&SIPURI=&TELURI=&LEAUsername=leatest1&LIBaddr=1.2.3.4&ReqId=100-197&IMSI=123123123&MSISDN=&IMEI=&SIPURI=&TELURI=&LEAUsername=leatest1&LIBaddr=1.2.3.4&ReqId=100-201&IMSI=123123123&MSISDN=&IMEI=&SIPURI=&TELURI=&LEAUsername=leatest1&LIBaddr=1.2.3.4& Status=2000k
```

**85 - Show default values of a CLI user**

Description: This command displays the default values for the current CLI user.

Preconditions: None

Command number: 85

Input parameters: None

Output parameters: any default values set for the current CLI user

Return values: 103 or 200

```
CLI# 85

85?AAUsername=aa1&LEAUsername=leal&Status=2000k
```

**86 - Remove a CLI user's default values**

Description: This command deletes all the default values for the current CLI user.

Preconditions: None

Command number: 86

Input parameters: None

Output parameters: None

Return values: 103 or 200

CLI# 86

86?Status=2000k

### **87 - Deactivate and remove all authorisations in the LIC**

Description: This command deactivates and removes all authorisations in the LIC.

Preconditions: None

Command number: 87

Input parameters: None

Output parameters: the deleted request IDs (ReqID)

Return values: 105 or 200

CLI# 87

87?ReqId=1-16&ReqId=1-2&ReqId=1-1002&Status=2000k

### **88 - View details of all interceptions**

Description: This command displays the details of all interceptions.

Preconditions: One or more interceptions exist.

Command number: 88

Input parameters: None

Output parameters for each interception:

- ReqId
- AAUsername
- LEAUsername
- IMSI and MSISDN and IMEI and SIPURI and TELURI
- ValidFrom
- ValidTo
- StartTime
- EndTime
- AuthorizedOptions
- AuthorizedInterceptType
- InterceptType
- IsActive
- FwdDelayCC
- FwdSizeCC
- FwdDelayIRI

- FwdSizeIRI
- LIBAddr
- InterceptionOptions
- InterceptionOptionsIRI
- FwdPathCC
- FwdPathIRI
- FwdUsernameCC
- FwdUsernameIRI
- WarrantID
- FwdAddrCC
- FwdAddrIRI
- SSHHostKeyCC
- SSHHostKeyIRI
- ULICPort
- IAId

Return values: 102, 103, 104, 105, or 200

CLI# 88

```
88?ReqId=444-
4&AAUsername=aal&LEAUsername=lea1&IMSI=1000000100002&IMEI=&
MSISDN=&SIPURI=&TELURI=&ValidFrom=17.04.2005&ValidTo=17.05.
2007&StartTime=12:00&EndTime=12:00&AuthorizedOptions=3&Auth
orizedInterceptType=7&InterceptType=7&IsActive=1&LIBAddr=&I
nterceptionOptions=6&InterceptionOptionsIRI=6&FwdPathCC= ./d
ata/cc&FwdPathIRI= ./data/iri&FwdUsernameCC=user1&FwdUsernam
eIRI=user1&WarrantID=warrant4&FwdAddrCC=10.30.20.40&FwdAddr
IRI=10.30.20.40&SSHHostKeyCC=&SSHHostKeyIRI=&IAId=&ReqId=44
4-2&AAUsername=aal&LEAUsername=lea1&IMSI=1000000100001&IMEI
=&MSISDN=&SIPURI=&TELURI=&ValidFrom=17.04.2005&ValidTo=17.0
5.2007&StartTime=11:39&EndTime=11:39&AuthorizedOptions=3&Au
thorizedInterceptType=7&InterceptType=7&IsActive=1&LIBAddr=
&InterceptionOptions=6&InterceptionOptionsIRI=6&FwdPathCC= ./
/data/cc&FwdPathIRI= ./data/iri&FwdUsernameCC=user2&FwdUsern
ameIRI=user2&WarrantID=warrant2&FwdAddrCC=10.30.20.40&FwdAd
drIRI=10.30.20.40&SSHHostKeyCC=&SSHHostKeyIRI=&IAId=&ReqId=
444-3&AAUsername=aal&LEAUsername=lea1&IMSI=&IMEI=&MSISDN=10
00000100001&SIPURI=&TELURI=&ValidFrom=17.04.2005&ValidTo=17
.05.2007&StartTime=11:42&EndTime=11:42&AuthorizedOptions=3&
AuthorizedInterceptType=7&InterceptType=7&IsActive=1&LIBAdd
r=&InterceptionOptions=6&InterceptionOptionsIRI=6&FwdPathCC
= ./data/cc&FwdPathIRI= ./data/iri&FwdUsernameCC=user1&FwdUse
rnameIRI=user1&WarrantID=MSISDN&FwdAddrCC=10.30.20.40&FwdAd
drIRI=10.30.20.40&SSHHostKeyCC=&SSHHostKeyIRI=&IAId=&ReqId=
444-5&AAUsername=aal&LEAUsername=lea2&IMSI=1000000100002&IM
```

```
EI=&MSISDN=&SIPURI=&TELURI=&ValidFrom=17.04.2005&ValidTo=17.05.2007&StartTime=15:22&EndTime=15:22&AuthorizedOptions=3&AuthorizedInterceptType=7&InterceptType=7&IsActive=1&LIBaddr=10.100.10.22&InterceptionOptions=6&InterceptionOptionsIRI=6&FwdPathCC=./data/cc&FwdPathIRI=./data/iri&FwdUsernameCC=ville&FwdUsernameIRI=user3&WarrantID=aaaa4a2&FwdAddrCC=10.30.20.40&FwdAddrIRI=10.30.20.40&SSHHostKeyCC=&SSHHostKeyIRI=&IAId=111-1&Status=2000k
```

### 89 - Exit the CLI session

Description: This command exits the CLI session and closes the Telnet connection.

Preconditions: None

Command number: 89

Input parameters: None

Output parameters: None

Return value: 200

```
CLI# 89
89?Status=2000k
```

### 90 - List IP pool addresses

Description: An LEA user and the AA user who created the LEA user account can use this command to list the address range(s) in an IP pool designated to the LEA user.

Preconditions: LEAUsername exists and the IP pool functionality has been enabled for the AA user by the Administrator.

Command number: 90

Input parameters:

- LEAUsername (M, D)

Output parameters:

- IPpoolAddr
- IPpoolSubnetBits

Return values: 102, or 200

```
CLI# 90?LEAUsername=lea1
90?IPpoolAddr=127.0.0.0&IPpoolSubnetBits=24&Status=2000k
```

## 3.9 Commands for the LEA

### 100 - List interceptions

Description: The LEA user can use this command to list interceptions. QueryType specifies what kind of interceptions are printed out.

Preconditions: LEAUsername exists.

Command number: 100

Input parameters:

- LEAUsername (M, D)
- QueryType (M)

Output parameters (for each interception):

- ReqId
- IMSI and MSISDN and IMEI and SIPURI and TELURI
- IsActive

Return values: 102, 103, 104, 105, or 200

```
CLI# 100?LEAUsername=lea_judge&QueryType=ALL
```

```
100?ReqId=100-196&IMSI=123123123&IMEI=&MSISDN=&SIPURI=&TELURI=&IsActive=0&ReqId=100-197&IMSI=123123123&IMEI=&MSISDN=&SIPURI=&TELURI=&IsActive=1&ReqId=100-201&IMSI=123123123&IMEI=&MSISDN=&SIPURI=&TELURI=&IsActive=1&Status=200Ok
```

### 101 - Activate interception

Description: The LEA can use this command to activate an interception. By specifying the ValidFrom, ValidTo, StartTime, and Endtime parameters the LEA can define the start and end date, and the time of the active interception period.

Preconditions:

LEAUsername exists.

The authorisation ReqId is valid.

LEAUsername has been authorised to intercept target ReqId.

LEAUsername has set the interception settings for ReqId (command 103 or 105).

The licmain process is running.

Command number: 101

Input parameters:

- LEAUsername (M, D)

- ReqId (M)
- ValidFrom (O)
- ValidTo(O)
- StartTime(O)
- EndTime (O)

---

**Note**

None or all four of the ValidFrom, ValidTo, StartTime, and Endtime parameters have to be defined.

If none of the ValidFrom, ValidTo, StartTime, and Endtime parameters are defined, the values defined by the AA user are used by default. For more information, see command 1, Authorise an interception.

---

Output parameters: None

Return values: 102, 103, 104, 105, 107, 108, or 200

```
CLI# 101?LEAUsername=lea1&ReqId=100-48
```

```
101?Status=200Ok
```

**102 - Deactivate interception**

Description: The LEA user can use this command to deactivate an active interception.

Preconditions:

- LEAUsername exists.
- LEAUsername has an active interception ReqId.

Command number: 102

Input parameters:

- LEAUsername (M, D)
- ReqId (M)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

```
CLI# 102?LEAUsername=lea_judge&ReqId=100-48
```

```
102?Status=200Ok
```

**103 - Change interception settings**

Description: The LEA user can use this command to change the settings for an interception that uses the same destination for CC and IRI data. If strFTP is

used, strFTP parameters have to be first defined for the LEA with the command 106.

In LIG4 the recommended values for InterceptionOptions are 12 and 14.

Preconditions:

- LEAUsername exists.
- LEAUsername has an interception ReqId.
- Corresponding FTCs have been created if parameters FTCLdIRI or FTCLdCC are used.

Command number: 103

Input parameters:

- LEAUsername (M, D)
- ReqId (M, D)
- FwdAddr (MF, MS)
- FwdDelay (M, D)
- FwdPasswd1 (MF)
- FwdPasswd2 (MF)
- FwdSize (M, D)
- InterceptType (M, D)
- FwdUsername (MF, MS)
- FwdPath (MF, MS)
- InterceptionOptions (M, D)
- SSHHostKey (MS)
- FTCLdCC (O)
- FTCLdIRI (O)
- ULICPort (MUC)

---

**Note**

FTP is used if InterceptionOptions has the value 4 or 6, and Secure Copy (SCP) is used if the value is 5 or 7. strFTP is used if the value is 16 or 18. ULIC is used if the value is 20. Value 20 is allowed only for CC interceptions. When the value is 12 or 14, the FTC configuration defines the used protocol. ULIC FTC cannot be assigned to parameter FTCLdIRI

---

Output parameters: None

Return values: 102, 103, 104, 105, or 200

**Example 12. Using FTCs**

```
CLI#
103?LEAUsername=lea1&ReqId=100-260&InterceptionOptions=14&InterceptType=5&FTCCid=lea1-1&FTCIDIRI=lea1-1
103?Status=2000k
```

**Example 13. Using FTP and LIG3 compatibility mode**

```
CLI#
103?LEAUsername=leajudge&ReqId=100-48&FwdAddr=23.23.23.23&FwdPasswd1=passwd&FwdPasswd2=passwd6InterceptType=4&FwdUsername=leajudg&FwdPath=./&InterceptionOptions=4
103?Status=2000k
```

**Example 14. Using SSH (SCP) and LIG3 compatibility mode**

```
CLI#
103?LEAUsername=leajudge&ReqId=100-48&FwdAddr=23.23.23.23&InterceptType=4&FwdUsername=leajudg&FwdPath=./&InterceptionOptions=5&SSHHostKey=<SSH host key of the destination>
103?Status=2000k
```

**Example 15. Using strFTP and LIG3 compatibility mode**

```
CLI#
103?LEAUsername=leajudge&ReqId=100-48&InterceptType=7&InterceptionOptions=16
103?Status=2000k
```

**104 - View details of an interception**

Description: The LEA user can use this command to view the details of an interception.

Preconditions:

- LEAUsername exists.
- LEAUsername has an interception ReqId.

Command number: 104

Input parameters:

- LEAUsername (M, D)
- ReqId (M)

Output parameters:

- ReqId
- IMSI and MSISDN and IMEI and SIPURI and TELURI
- ValidFrom
- ValidTo
- StartTime
- EndTime
- AuthorizedOptions
- AuthorizedInterceptType
- InterceptType
- IsActive
- LIBAddr
- InterceptionOptions
- InterceptionOptionsIRI
- FwdDelayCC
- FwdDelayIRI
- FwdPathCC
- FwdPathIRI
- FwdSizeCC
- FwdSizeIRI
- FwdUsernameCC
- FwdUsernameIRI
- WarrantID
- FwdAddrCC
- FwdAddrIRI
- SSHHostKeyCC
- SSHHostKeyIRI
- ULICPort
- IAId
- FTCTidCC
- FTCTidIRI

Return values: 102, 103, 104, 105, or 200

CLI# **104?LEAUsername=leal&ReqId=96-26001**

```
104?ReqId=96-26001&IMSI=123425123434&IMEI=&MSISDN=&SIPURI=&
TELURI=&ValidFrom=16.08.2005&ValidTo=16.09.2005&StartTime=1
```

```
2:48&EndTime=12:48&AuthorizedOptions=3&AuthorizedInterceptType=5&InterceptType=5&IsActive=0&FwdDelayCC=10&FwdSizeCC=50000&FwdDelayIRI=10&FwdSizeIRI=50000&LIBaddr=1.2.3.4&InterceptionOptions=18&InterceptionOptionsIRI=18&FwdPathCC= ./&FwdPathIRI= ./&FwdUsernameCC=user&FwdUsernameIRI=user&WarrantID=warrant&FwdAddrCC=2.3.4.5&FwdAddrIRI=2.3.4.5&IAId=&FTCIDCC=leal-1&FTCIDIRI=leal-1&Status=200Ok
```

### 105 - Change interception settings

Description: The LEA can use this command to change the settings of an interception that uses different destinations for CC and IRI data.

In LIG4 the recommended values for InterceptionOptions (and InterceptionOptionsIRI) are 12 and 14.

Preconditions:

- LEAUsername exists.
- LEAUsername has an interception ReqId.
- If the value in InterceptionOptions (or InterceptionOptionsIRI) is 16 or 18, strFTP parameters have to be first defined for the LEA with the command 106.
- Corresponding FTCs have been created if parameters FTCIdIRI or FTCIdCC are used.

Command number: 105

Input parameters:

- LEAUsername (M, D)
- ReqId (M)
- FwdAddrCC (MFC, MSC, D)
- FwdAddrIRI (MFI, MSI, D)
- FwdDelayCC (MFC, MSC, D)
- FwdDelayIRI (MFI, MSI, D)
- FwdPasswordCC (MFC, D)
- FwdPasswordIRI (MFI, D)
- FwdSizeCC (MFC, MSC, D)
- FwdSizeIRI (MFI, MSI, D)
- InterceptType (M, D)
- FwdUsernameCC (MFC, MSC, D)
- FwdUsernameIRI (MFI, MSI, D)
- FwdPathCC (MFC, MSC, D)
- FwdPathIRI (MFI, MSI, D)

- InterceptionOptions (M, D)
- InterceptionOptionsIRI (O, D)
- SSHHostKeyCC (MSC, D)
- SSHHostKeyIRI (MSI, D)
- FTCCidCC (O)
- FTCCidIRI (O)
- ULICPort (MUC)

---

**Note**

File Transfer Protocol (FTP) is used if InterceptionOptions or InterceptionOptionsIRI has the value 4 or 6, and SCP is used if InterceptionOptions or InterceptionOptionsIRI has the value 5 or 7. strFTP is used if InterceptionOptions or InterceptionOptionsIRI has the value 16. ULIC is used if the value is 20 (only for CC). When the value is 12 or 14, the FTC configuration defines the used protocol. If either of parameters interceptionOptions or interceptionOptionsIRI contain value 12 or 14, both parameters must contain either the value 12 or 14. ULIC FTC cannot be assigned to parameter FTCCidIRI.

---

---

**Note**

If both parameters SSHHostKeyCC and SSHHostKeyIRI are defined and the key is very long, the command may not work correctly even if the command extension functionality is used (because the command maximum length has been exceeded). In such cases, use parameters FTCCidCC and FTCCidIRI, and value 12 or 14 in InterceptionOptions and InterceptionOptionsIRI

---

Output parameters: None

Return values: 102, 103, 104, 105, or 200

**Example 16. Using FTCs**

```
CLI# 105?LEAUsername=lea1&ReqId=96-26001&InterceptionOptions=12&InterceptType=5&FTCCidCC=lea1-1&FTCCidIRI=lea1-1
105?Status=200Ok
```

**Example 17. Using FTP transfer for CC and IRI data; browsing enabled for IRI**

```
CLI#
105?LEAUsername=lea judge&ReqId=100-47&FwdAddrCC=23.23.23.23&FwdAddrIRI=24.24.24.24&FwdPasswordCC=CCpass&FwdPasswordIRI
```

```
=IRIpass&InterceptType=7&FwdUsernameCC=CCuser&FwdUsernameIRI=IRIuser&FwdPathCC=CCpath&FwdPathIRI=IRIpath&InterceptionOptions=4&InterceptionOptionsIRI=6&FwdDelayCC=10&FwdSizeCC=5000&FwdDelayIRI=10&FwdSizeIRI=50000
```

```
105?Status=200ok
```

Example 18. Using FTP transfer for CC data and SCP for IRI data

```
CLI#
```

```
105?LEAUsername=leatest1&ReqId=100-201&FwdAddrCC=1.2.3.5&FwdAddrIRI=2.3.4.5&FwdDelayCC=60&FwdDelayIRI=60&FwdSizeCC=250000&FwdSizeIRI=250000&FwdPasswordCC=CCpass&InterceptType=7&FwdUsernameCC=CCuser&FwdUsernameIRI=IRIuser&FwdPathCC=CCpath&FwdPathIRI=IRIpath&InterceptionOptions=6&InterceptionOptionsIRI=5&SSHHostKeyIRI=IRIkey
```

```
105?Status=200ok
```

Example 19. Using strFTP transfer

```
CLI#
```

```
105?LEAUsername=leatest1&ReqId=100-201&InterceptType=7&InterceptionOptions=16
```

```
105?Status=200ok
```

### 106 - Set strFTP parameters

Description: The LEA user can use this command to set the parameters for strFTP transfers.

Preconditions: LEAUsername exists.

Command number: 106

Input parameters:

- LEAUsername (M, D)
- FwdAddrCC (M)
- FwdAddrIRI (M)
- FwdPathCC (M)
- FwdPathIRI (M)
- FwdUsernameCC (M)
- FwdUsernameIRI (M)
- FwdPasswordCC (M)
- FwdPasswordIRI (M)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

CLI#

```
106?LEAUsername=lea judge&FwdAddrCC=3.4.5.6&FwdAddrIRI=2.3.4
.5&FwdPathCC=CCPath&FwdPathIRI=IRIpath&FwdUsernameCC=CCjeps
&FwdUsernameIRI=Jeps&FwdPasswordCC=CCpass&FwdPasswordIRI=IR
Ipass
```

```
106?Status=200Ok
```

### 107 - Show strFTP parameters

Description: The LEA user can use this command to display the strFTP parameters.

Preconditions: LEAUsername exists.

Command number: 107

Input parameter: LEAUsername (M, D)

Output parameters:

- FwdAddrCC
- FwdPathCC
- FwdUsernameCC
- FwdPasswordCC
- FwdAddrIRI
- FwdPathIRI
- FwdUsernameIRI
- FwdPasswordIRI

Return values: 102, 103, 104, 105, or 200

CLI# **107?LEAUsername=lea1**

```
107?FwdAddrCC=1.2.3.4&FwdPathCC=/home/lea1/cc&FwdUsernameCC
=lea1&FwdPasswordCC=lea1&FwdAddrIRI=1.2.3.4&FwdPathIRI=/hom
e/lea1/iri&FwdUsernameIRI=lea1&FwdPasswordIRI=ara&Status=20
0Ok
```

### 108 – Add FTC

Description: The LEA user can use this command to add a new FTC.

Preconditions: LEAUsername exists.

Command number: 108

Input parameter:

- LEAUsername (M, D)
- FwdAddr (M)

- FwdPath (M)
- FwdUsername (M)
- FwdPasswd1 (M)
- FwdPasswd2 (M)
- SSHHostKey (M if TransmissionProtocol is ssh)
- TransmissionProtocol (M)
- ULICPort (M if TransmissionProtocol is ULIC)
- FwdDelay (M if TransmissionProtocol is not ULIC)
- FwdSize (M if TransmissionProtocol is not ULIC)
- Description (O)

Output parameters:

- FTCTid

Return values: 102, 104, 105 or 200

---

### Note

There may be only two FTCs using Streaming FTP for each LEA (with indexes 1 or 2).

---

#### Example 20. Adding ULIC FTC

```
CLI#
108?LEAUsername=lea1&FwdAddr=1.2.3.4&TransmissionProtocol=ULIC&ULICPort=55555
108?FTCTid=lea1-13&Status=200ok
```

#### Example 21. Attempt to add StrFTP FTC when two StrFTP FTCs are already defined

```
CLI#
108?LEAUsername=lea1&FwdAddr=1.2.3.1&TransmissionProtocol=StrFTP&FwdUsername=user&FwdPasswd1=passwd&FwdPasswd2=passwd&FwdPath=./&FwdDelay=10&FwdSize=50000
108?FTCTid=1&FTCTid=2&Status=104LICError - access denied
```

### 109 – Modify FTC

Description: The LEA user can use this command to modify the existing FTC.

Preconditions: The LEA user exists and has an FTC with FTCTid.

Command number: 109

Input parameter:

- LEAUsername (M)
- FTCTid (M)
- FwdAddr (O)
- FwdPath (O)
- FwdUsername (O)
- FwdPasswd1 (O)
- FwdPasswd2 (M if FwdPasswd1 is defined)
- SSHHostKey (O)
- ULICPort (O)
- Description (O)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

Example 22.

```
CLI# 109?LEAUsername=lea1&FTCTid=lea1-17&Description=ULICFTC
109?Status=200Ok
```

### 110 – Remove FTC

Description: The LEA user can use this command to remove an existing FTC.

Preconditions:

- The LEA user exists and has an FTC with FTCTid.
- FTC is not used in any interception

Command number: 110

Input parameters:

- LEAUsername (M)
- FTCTid (M)

Output parameters: None

Return values: 102, 103, 104, 105 or 200

```
CLI# 110?FTCTid=lea1-17&LEAUsername=lea1
110?Status=200Ok
```

**111 – View FTC**

Description: The LEA user can use this command to view the parameters of the existing FTC.

Preconditions: The LEA user exists and has an FTC with FTCId.

Command number: 111

Input parameters:

- LEAUsername (M)
- FTCId (M)

Output parameters:

- FwdAddr
- FwdPath
- FwdUsername
- SSHHostKey
- TransmissionProtocol
- ULICPort
- FwdDelay
- FwdSize
- Description

Return values: 102, 103, 104, 105, or 200

```
CLI# 111?LEAUsername=lea1&FTCId=lea1-16
```

```
111?FwdAddr=1.2.3.4&FwdPath=&FwdUsername=&TransmissionProtocol=ULIC&ULICPort=45345&FwdDelay=&FwdSize=&Description=description&Status=2000k
```

## 3.10 Commands for the Administrator

**200 - View the general configuration of the LIC**

Description: The Administrator can use this command to view the general configuration of the LIC.

Preconditions: None

Command number: 200

Input parameter: None

Output parameters:

- OpID

- MCCMNC
- DeliveryIdStart
- LICID
- LICIPv4
- LICIPv6
- Port
- SGSNData
- AdLogLife
- AdLogSize
- AuditLogLife
- AuditLogSize
- AALogLife
- AALogSize
- LEALogLife
- LEALogSize
- LogLevel
- LIBLoad
- LDI
- FtpMode
- CLICompatibility

Return values: 102, 103, 104, 105, or 200

CLI# 200

```
200?OpID=lemon&MCCMNC=37766&DeliveryIdStart=1&LICID=96&LICIPv4=123.45.67.8&LICIPv6=&Port=50096&SGSNData=0&AdLogLife=900&AdLogSize=102400&AuditLogLife=0&AuditLogSize=51200&AALogLife=0&AALogSize=51200&LEALogLife=86400&LEALogSize=51200&LogLevel=3&LIBLoad=0&LDI=1&FTPMode=0&CLICompatibility=4&Status=2000k
```

### **201 - View the status of the LIC processes**

Description: The Administrator can use this command to view the status of the LIC processes.

Preconditions: None

Command number: 201

Input parameter: None

Output parameters:

- LICMain
- AlarmHandler
- FileTransfer

Return values: 105 or 200

CLI# 201

```
201?LICMain=ENABLED&AlarmHandler=ENABLED&FileTransfer=ENABLED&Status=200Ok
```

### 202 - List current AA users

Description: The Administrator can use this command to list current AA users.

Preconditions: None

Command number: 202

Input parameter: None

Output parameters (for each AA):

- AAUsername
- AARealName
- AAUserStatus
- IPPool

Return values: 104, 105, or 200

CLI# 202

```
202?AAUsername=judge&AARealName=dread&AAUserStatus=ACTIVE&IPPool=Enabled&AAUsername=op&AARealName=operator&AAUserStatus=DEACTIVE&IPPool=Enabled&Status=200Ok
```

### 203 - View the backup configuration

Description: The Administrator can view the backup configuration with this command.

Preconditions: None

Command number: 203

Input parameter: None

Output parameters:

- FwdAddr
- FwdPath
- FwdUserName
- BackupInterval
- BackupDate

- BackupTime
- Weekday
- TransferMethod

Return values: 105, 200, or 203

CLI# 203

```
203?FwdAddr=123.4.5.6&FwdPath=/var/admin/libackup&FwdUserNa  
me=admin&BackupInterval=0&BackupDate=&BackupTime=12:00&Week  
day=1000101&TransferMethod=FTP&Status=200Ok
```

#### **204 - Perform the backup procedure**

Description: The Administrator can make a backup immediately with this command.

Preconditions: The backup configuration has been defined.

Command number: 204

Input parameter: None

Output parameters: None

Return values: 104, 105, or 200

CLI# 204

```
204?Status=200Ok
```

#### **205 - Define a new interception area**

Description: The Administrator can use this command to define interception areas, which are used in location dependent interceptions. The interception area is a set of Cell Global Identifications (CGIs), Routing Area Identifiers (RAIs), Service Area Identifiers (SAIs), Mobile Country Codes (MCCs), combined Mobile Country Code and Mobile Network Codes (MCCMNCs), or Location Area Identifiers (LAIs). At least one CGI, RAI, SAI, MCC, MCCMNC, or LAI must be part of the interception area. Only one cell item type (CGI, RAI, SAI, MCC, MCCMNC, LAI) is allowed in one definition.

Preconditions: None.

Command number: 205

Input parameters:

- IAName (M, D)
- CGI (the parameter is given 0-n times)
- RAI (the parameter is given 0-n times)
- SAI (the parameter is given 0-n times)
- MCC (the parameter is given 0-n times)
- MCCMNC(the parameter is given 0-n times)

- LAI (the parameter is given 0-n times)

Output parameters: IAId

Return values: 102, 103, 104, 105, or 200

Example 23. IA defined with CGIs

```
CLI#  
205?IAName=Helsinki&CGI=2400124252624731&CGI=2400124252764822&  
CGI=2400124252834245  
205?IAId=1-1&Status=200Ok
```

Example 24. IA defined with MCC

```
CLI# 205?IAName=Finland&MCC=358  
205?IAId=1-2&Status=200Ok
```

### **206 - Set Loadbalancing On / Off**

Description: The Administrator can use this command to enable or disable the LIB load balancing functionality. If the load balancing functionality is enabled, the LIB is assigned to an interception, with automatic selection based on the number of interceptions in the LIBs.

Preconditions: None.

Command number: 206

Input parameters:

- OnOff (M)

Output parameters: None

Return values: 102 or 200

```
CLI# 206?OnOff=on  
206?Status=200Ok
```

### **207 - Set IP pool On / Off**

Description: The Administrator can use this command to enable or disable the IP pool functionality for an AA user.

Preconditions: AA user exists.

Command number: 207

Input parameters:

- AAUsername (M, D)
- OnOff (M)

Output parameters: None

Return values: 102 or 200

```
CLI# 207?AAUsername=aal&OnOff=on  
207?Status=200Ok
```

## 3.11 Commands for the Administrator using CLI Admin

### 208 – View License configuration

Description: The Administrator can use this command to view LIG license properties.

Command number: 208

Input parameters: None

Output parameters:

- Filename
- LIGRelease
- LicenseType
- UniqueId
- LicensedLIEs
- LicensedInterceptions
- ValidFrom
- ValidTo
- WarningTime

Return values: 105 or 200

Example 25.

```
cliadmin# 208
```

```
208?Filename=license2.txt&LIGRelease=LIG4.0&LicenseType=1&UniqueId=96037766&LicensedLIEs=11&LicensedInterceptions=10&ValidFrom=02Aug2005&ValidTo=15Sep2005&WarningTime=14days&Status=200Ok
```

### 220 – Initialise License

Description: The Administrator can use this command to initialise the LIG licence.

Preconditions: The licence file has to exist in the `/var/etc/license` directory.

Command number: 220

Input parameters:

- Filename (M)

Output parameters: None

Return values: 102 or 200

Example 26.

```
cliadmin# 220?Filename=license.txt
220?Status=200Ok
```

### **221 – Manage License Configuration**

Description: The Administrator can use this command to manage the LIG licence configuration

Command number: 221

Input parameters:

- WarningTime (M)

Output parameters: None

Return values: 102 or 200

```
cliadmin# 221?WarningTime=21
221?Status=200Ok
```

### **222 – Manage General Configuration**

Description: The Administrator can use this command to manage General configuration.

Command number: 222

Input parameters:

- LICIPv4 (O)
- LICIPv6 (O)
- Port (O)
- OpID (O)
- MCCMNC (O)
- DeliveryIDStart (O)
- LICID (O)

- SGSNData (O)
- FtpMode (O)
- LIBLoad (O)
- LDI (O)
- CLICompatibility (O)
- LogLevel (O)
- AALogSize (O)
- AALogLife (O)
- AdLogSize (O)
- AdLogLife (O)
- AuditLogSize (O)
- AuditLogLife (O)
- LEALogSize (O)
- LEALogLife (O)

Output parameters: None

Return values: 102, 109, or 200

---

#### **Note**

Parameters LICIPv4, LICIPv6, OpID, MCCMNC, DeliveryIDStart, LICID, and LDI can be defined only once. If any of these parameters have to be redefined, the LIC has to be re-installed.

---

#### Example 27. Changing AuditLogLife

```
cliadmin# 222?AuditLogLife=172800
222?Status=200Ok
```

#### Example 28. Trying to redefine OpID

```
cliadmin# 222?OpID=sanet
222?OpID=&Status=109LICError - Value already defined
```

### **223 – Manage Statistics Configuration**

Description: The Administrator can use this command to manage statistics configuration.

Command number: 223

Input parameters:

- StatisticsConfiguration(M)

Output parameters: None

Return values: 102 or 200

Example 29.

```
cliadmin# 223?StatisticsConfiguration=110100000101
223?Status=200Ok
```

## 224 – Manage Backup Configuration

Description: The Administrator can use this command to manage backup configuration.

Command number: 224

Input parameters:

- FwdAddr (O)
- FwdPath (O)
- FwdUsername (O)
- Password1 (O)
- Password2 (O)
- TransferMethod (O)
- SSHHostKey (O)
- BackupInterval (O)
- BackupDate (M if BackupInterval is 2419200 meaning one month)
- BackupTime (M if BackupInterval is -2 or greater than zero)
- Weekday (M if BackupInterval is -2)

Output parameters: None

Return values: 102 or 200

Example 30.

```
cliadmin# 224?Password1=passwd&Password2=passwd&FwdPath= ./
224?Status=200Ok
```

## 225 – Manage LIC Processes

Description: The Administrator can use this command to manage LIC process statuses.

Command number: 225

Input parameters:

- LICMain
- AlarmHandler
- FileTransfer

Output parameters: None

Return values: 102 or 200

Example 31.

```
cliadmin# 225?LICMain=DISABLED
225?Status=200Ok
```

### **226 – Add a network element**

Description: The Administrator can use this command to add a new network element.

Command number: 226

Input parameters:

- NE (M)
- NEType (M)
- Port (M)
- OnTheFly (O, not applicable if NEType is LIB or CPS)
- Protocol (M, LIPv1 is valid if NEType is SGSN or GGSN, LIPv2 is valid if NEType is LIB or CPS)

Output parameters: None

Return values: 102 or 200

Example 32.

```
cliadmin# 226?NE=1.2.3.6&NEType=SGSN&Port=50088&OnTheFly=1&
Protocol=1
226?Status=200Ok
```

### **227 – Remove a network element**

Description: The Administrator can use this command to remove a network element.

Command number: 227

Preconditions: NE exists

Input parameters:

- NE (M)

Output parameters: None

Return values: 102 or 200

Example 33.

```
cliadmin# 227?NE=1.2.3.6
227?Status=200Ok
```

### **228 – Create AA user**

Description: The Administrator can use this command to add a new AA user.

Command number: 228

Input parameters:

- AAUsername (M)
- Password1 (M)
- Password2 (M)
- AARealName (M)

Output parameters: None

Return values: 102, 104, or 200

Example 34.

```
cliadmin# 228?AAUsername=aauser&Password1=passwd&Password2=
passwd&AARealName=realname
228?Status=200Ok
```

### **229 – Modify AA user**

Description: The Administrator can use this command to modify an AA user.

Command number: 229

Input parameters:

- AAUsername (M)
- AARealName (O)
- IPPool (O)

Output parameters: None

Return values: 102, 104, or 200

Example 35.

```
cliadmin# 229?AAUsername=aauser&IPPool=Enabled
229?Status=200Ok
```

### **230 – Remove AA user**

Description: The Administrator can use this command to remove an AA user.

Command number: 230

Input parameters:

- AAUsername (M)

Output parameters: None

Return values: 102 or 200

Example 36.

```
cliadmin# 230?AAUsername=aauser
230?Status=200Ok
```

### **231 – Set alarm mode**

Description: The Administrator can use this command to set an Administrator user's alarm mode.

Command number: 231

Input parameters:

- AlarmMode(M)

Output parameters: None

Return values: 102 or 200

Example 37.

```
cliadmin# 231?AlarmMode=3
231?Status=200Ok
```

### **232 – Send alarm**

Description: The Administrator can use this command to send a custom alarm (1014 LIC\_WEB\_GENERATED\_ALARM) to a user. The severity of the alarm is warning. For more details about alarms, see *Nokia LIG Release 4 Product Documentation: Reference Guide*.

Command number: 232

Input parameters:

- Username (M)
- AlarmSuppInfo (M)

Output parameters: None

Return values: 102, 103, or 200

Example 38.

```
cliadmin# 232?Username=audit&AlarmSuppInfo=
Service_break_on_20.11.2005.
232?Status=200Ok
```

### 233 – Generate a new password

Description: The Administrator can use this command to generate a new password for an AA or LEA user. When generating a new password for an LEA user, the parameter AAUsername defines the creator of the LEA user. The parameter NE defines the LIG network element (LIC/LIB) for which the new password is generated.

An alarm that contains the new password is sent to the specified AA or LEA user according to the AA or LEA user's alarm configuration. Another alarm is sent to LEA user's creator AA user to inform about the action (but the content of the new password is not included in this alarm). An alarm is also sent to the Audit user informing about the action (but the content of the new password is not included in this alarm).

Command number: 233

Input parameters:

- AAUsername (M)
- LEAUsername (M, if generating a new password for LEA user)
- NE (M)

Output parameters: None

Return values: 102 or 200

Example 39. Regenerating AA user's password

```
cliadmin# 233?AAUsername=aauser&NE=1.2.3.4
233?Status=200Ok
```

Example 40. Regenerating LEA user's password

```
cliadmin#
233?AAUsername=aauser&LEAUsername=leouser&NE=1.2.3.4
233?Status=200Ok
```

## 3.12 Commands for all users

### 0 - Help

Description: This command can be used to display a help text for authorised commands.

Preconditions: None

Command number: 0

Input parameters: None

Output variables: The help text with the command number replacing the parameter name and the description replacing the parameter value for each command. The command outputs the number and description of all commands.

Return value: 200

CLI# 0

```
0?0=Help Text&1=Authorise a LEA to intercept a
target&2=List current authorisations&3=Detailed view of an
authorisation&4=Prolong the validity period of an
authorisation&5=Revoke an authorisation&6=List lawful
interception browsers&7=Redefine LIB&20=Create a new LEA
user&21=List current LEA user&22=Remove LEA user
account&23=Create LIB account for a LEA user&24=Remove LEAs
LIB account&25=List LEAs LIB
accounts&26=Activate/deactivate an LEA user&30=Add/remove
IP pool address&80=Set default values for current CLI
user&81=Create and activate an interception&82=Deactivate
and remove an interception&83=Modify an existing
interception&84=Detailed view of an interception or List
all interceptions for AA user&85=Show the CLI user default
values&86=Remove CLI users default values&87=Deactivate and
revoke all authorisations in LIC&88=Detailed view of all
interceptions&89=Exit&90=list IP pool addresses&100=List
interception&101=Activate interception&102=Deactivate
interception&103=Change interception settings&104=Detail
view of an interception&105=Change interception
settings&106=Set strFTP parameters for LEA&107=Show strFTP
parameters&200=View general configuration of the
LIC&201=View the status of the LIC processes&202=List
current AA users&203=View backup configuration&204=Perform
the backup procedure&205=Define a new interception
```

```
area&206=set LIB loadbalancing&207=set IP pool&1000=Change
the password in LIC&1001=Change user alarm
configuration&1002=Exit&1003=Show LIC root user's public
key1004=Show NE status&1005=Show alarm
configuration&1006=Execute a no operation command&1007=List
interception areas&1008=View details of the interception
area&Status=2000k
```

### **1000 - Change the password in the LIC**

Description: With this command a CLI user may change their own password that is used to log in for the CLI session. CLI users can only change their own passwords, not any other CLI user's password.

With this command a CLI user may also change the LIG 'web' password of an AA/LEA user.

Preconditions:

- Username (AA/LEA or CLI user) exists.
- Username has a LIG 'web'/CLI password (OldPassword)

Command number: 1000

Input parameters:

- Username (M)
- OldPassword (M)
- NewPassword1 (M)
- NewPassword2 (M)

Output parameters: None

Return values: 102, 103, 104, 105, or 200

CLI#

```
1000?Username=aauser&OldPassword=password&NewPassword1=drow
ssap&NewPassword2=drowssap
```

```
1000?Status=2000k
```

### **1001 - Change the user alarm configuration**

Description: This command changes the alarm configuration for a user. The alarm configuration is also used to transfer logs and statistics.

Preconditions: Username (LEA or AA) exists.

Command number: 1001

Input parameters:

- Username (M)
- TransferMethod (M)
- AlarmPasswd1 (MF, D)

- AlarmPasswd2 (MF, D)
- AlarmPath (M, D)
- AlarmAddr (M, D)
- AlarmUsername (M, D)
- SSHHostKey (MS)
- DeleteLogs (M)

Output parameters: None

Return values are 102, 103, 104, 105, or 200

Example 41. For an LEA user; the FTP is used for alarm transfer

```
CLI#
1001?Username=leouser&TransferMethod=FTP&AlarmPasswd1=password&AlarmPasswd2=password&AlarmPath=/alarm/&AlarmAddr=1.2.3.4&AlarmUsername=user&DeleteLogs=0
1001?Status=200Ok
```

Example 42. For an AA user; the SCP is used for alarm transfer

```
CLI#
1001?Username=aauser&TransferMethod=SCP&AlarmPath=/alarm/&AlarmAddr=1.2.3.4&AlarmUsername=user&SSHHostKey=1024 37
1328932757086238279155353555432940631976250269761053
76859489993494341662626672475456916414725401369952375493998
58416146892717326110074760954337306218763740183584413302367
80298028036698986881409236086304902889269069470248330472900
37908196107691923128837363182636072812810640327025873765633
433781674089163706921&DeleteLogs=0
1001?Status=200Ok
```

### 1002 - Exit

Description: This command ends the CLI session and closes the Telnet connection.

Preconditions: None

Command number: 1002

Input parameters: None

Output parameters: None

Return value: 200

```
CLI# 1002
1002?Status=200Ok
```

**1003 - Show root user's public key**

Description: This command displays the LIC root user's public key, which is used for transferring alarms to the LEA using the SCP. (See *Nokia LIG Release 4 Product Documentation: Reference Guide* for more details.)

Preconditions: The LIC root user's public key exists

Command number: 1003

Input parameters: None

Output parameter: RootPublicKey

Return values: 104, 105, or 200

CLI# **1003**

```
1003?RootPublicKey=1024 37 13289327570862382791553535
55432940631976250269761053768594899934943416626266724
75456916414725401369952375493998584161468927173261100
74760954337306218763740183584413302367802980280366989
86881409236086304902889269069470248330472900379081961
07691923128837363182636072812810640327025873765633433
781674089163706921&Status=200OK
```

**1004 – View all network elements**

Description: This command shows all the network elements.

Preconditions: Network elements exist in the LIC NE database.

Command number: 1004

Input parameters: None

Output parameters:

- NE
- NEType
- NEStatus
- Port
- OnTheFly (only for SGSN and GGSN)
- Protocol
- LIEType
- LIEDescription
- LIESupportedTargets

Return values: 200

CLI# **1004**

```
1004?NE=2.3.4.5&NEType=LIB&NEStatus=3&Port=50001&Protocol=2
&LIEType=0&LIEDescription=Lawful Interception Browser,
version 4.0 (build
4.0-374)&LIESupportedTargets=&NE=2.3.4.6&NEType=GGSN&NEStat
us=3&Port=50002&OnTheFly=1&Protocol=1&LIEType=&LIEDescripti
on=&LIESupportedTargets=&NE=2.3.4.7&NEType=SGSN&NEStatus=3&
Port=50003&OnTheFly=0&Protocol=1&LIEType=&LIEDescription=&L
IESupportedTargets=&NE=2.3.4.86&NEType=CPS&NEStatus=3&Port=
50004&Protocol=2&LIEType=&LIEDescription=&LIESupportedTarge
ts=&Status=2000k
```

### 1005 - Show the alarm configuration

Description: This command displays the alarm configuration for a specified LIG username. The alarm configuration is also used to transfer logs and statistics.

Preconditions:

- The username exists.
- The alarm configuration has been defined.

Command number: 1005

Input parameter: Username (M)

Output parameters:

- AlarmUsername
- AlarmAddr
- AlarmPath
- TransferMethod
- SSHHostKey
- FileTransferStatus
- DeleteLogs

Return values: 102, 103, or 200

```
CLI# 1005?Username=leouser
```

```
1005?AlarmUsername=user&AlarmAddr=2.3.4.10&AlarmPath=./&Tra
nsferMethod=FTP&SSHHostKey=&FileTransferStatus=0&DeleteLogs
=off&Status=2000k
```

### 1006 - Execute a no operation command

Description: The CLI user can verify that the CLI is working by executing this command.

Preconditions: None.

Command number: 1006

Input parameters: None

Output parameters: None

Return values: 200

CLI# 1006

1006?Status=200Ok

### **1007 - List interception areas**

Description: The users can use this command to list all interception areas.

Preconditions: None

Command number: 1007

Input parameters: None

Output parameters (for each interception area):

- IAName
- IAId

Return values: 104, 105, or 200

CLI# 1007

1007?IAName=Helsinki&IAId=1-1&IAName=Finland&IAId=1-2&Status=200Ok

### **1008 - View details of the interception area**

Description: The users can use this command to view details of one interception area.

Preconditions: The interception area has been defined.

Command number: 1008

Input parameters:

- IAId (M)

Output parameters:

- IAId
- CGI
- RAI
- SAI
- MCC
- MCCMNC
- LAI

Return values: 102, 103, 104, 105, or 200

CLI# 1008?IAId=1-1

```
1008?IAId=1-1&CGI=2400124252624731&CGI=2400124252764822&CGI  
= 2400124252834245&Status=200Ok
```

```
CLI# 1008?IAId=1-2
```

```
1008?IAId=1-2&MCC=358&Status=200Ok
```



# 4

## Using CLI

The following sections demonstrate how the CLI is used. The command executions can be performed in the order they are presented.

### 4.1 Telnet session initialisation and the still alive command

The remote host sets up a Telnet connection to the LIC with the user account `ims` and executes command `1006` to verify that the system works:

```
>telnet mikro
```

```
IPSO (mikro) (ttypl)
```

```
login: ims
```

```
Password:
```

```
Last login: Wed Oct 5 09:09:40 from 172.21.24.92
```

```
IPSO 3.8NET-FCS5B #296: 12.11.2004 104800
```

```
LIC Command Line Interface version 4.0
```

```
CLI# 1006
```

```
1006?Status=200Ok
```

### 4.2 Creating AA user account and listing users

The CLI session with `cliadmin` user has been opened. The Administrator creates an AA user `aaCli` and then lists all the created AA users.

```
cliadmin# 228?AAUsername=aaCli&Password1=aaClix&Password2=
aaClix&AARealName=aa_real_name
228?Status=2000k
cliadmin# 202
202?AAUsername=aaCli&AARealName=aa_real_name&AAUserStatus=A
CTIVE&IPPool=Disabled&Status=2000k
```

## 4.3 Changing the password

The Administrator has created the AA user *aaCli* using command 228. The password is *aaClix*. The CLI session has been opened. In the first example the AA user changes the password from *aaClix* to *aaclix*.

```
CLI#
1000?Username=aaCli&OldPassword=aaClix&NewPassword1=aaclix&
NewPassword2=aaclix
1000?Status=2000k
```

In the second example, the CLI user changes the password of the current CLI user. The CLI user has logged in with the username *ims*.

```
CLI#
1000?Username=ims&OldPassword=imsoldx&NewPassword1=imsnewx&
NewPassword2=imsnewx
1000?Status=2000k
```

## 4.4 Changing the alarm configuration

The Administrator has created the AA user *aaCli* using command 228. The CLI session has been opened. The AA user sets new alarm configuration parameters.

```
CLI#
1001?Username=aaCli&TransferMethod=FTP&AlarmPasswd1=admin&A
larmPasswd2=admin&AlarmPath=./runtest&AlarmAddr=1.2.3.4&Ala
rmUsername=admin&SSHHostKey=&DeleteLogs=0
1001?Status=2000k
```

## 4.5 Showing the root user's public key

The CLI session to the LIC has been opened. The root user's public key is requested.

```
cliadmin#1003
1003?RootPublicKey=1024 37 132893275708623827915535
355543294063197625026976105376859489993 49434166262
667247545691641472540136995237549399858416146892717
3 2611007476095433730621876374018358441330236780298
02803669898688 140923608630490288926906947024833047
290037908196107691923128837 36318263607281281064032
7025873765633433781674089163706921&Status=2000k
```

## 4.6 Listing the LIBs

The CLI session to the LIC has been opened. The LIC has one LIB defined. The list of LIBs is requested.

```
CLI# 6
6?LIBaddr=1.2.3.4&Status=2000k
```

## 4.7 Creating an LEA user account and listing LEA users

The CLI session has been opened. *aaCli* lists the LEA users the Authorising Authority (AA) has created (none at first), then creates the LEA user *leaCli* and lists the LEA users again. The AA then adds an LIB account to the created LEA user.

```
CLI# 21?AAUsername=aaCli
21?Status=2000k
CLI#
20?AAUsername=aaCli&LEAUsername=leaCli&Password1=leaCli&Pas
sword2=leaCli&LEARealname=LEA_for_CLI_use
20?Status=2000k
CLI# 21?AAUsername=aaCli
21?LEAUsername=leaCli&LEARealname=LEA_for_CLI_use&LEAUserST
atus=ACTIVE&Status=2000k
CLI# 23?LEAUsername=leaCli&LIBaddr=1.2.3.4
23?Status=2000k
```

## 4.8 Authorising an interception and listing authorisations

The Administrator has created the AA user *aaCli*. The CLI session has been opened. *aaCli* has created the LEA user *leaCli*. Now *aaCli* authorises *leaCli* to intercept a target and lists all current authorisations.

```
CLI# 1?AAUsername=aaCli&IMSI=1234567890&LEAUsername=leaCli&LIBaddr=1.2.3.4&AuthorizedInterceptType=7&AuthorizedOptions=3&ValidFrom=26.08.2005&StartTime=10:10&ValidTo=26.12.2005&EndTime=10:12&WarrantID=waid2
```

```
1?ReqId=222-11&Status=2000kCLI#
```

```
CLI# 2?AAUsername=aaCli
```

```
2?ReqId=222-11&IMSI=1234567890&MSISDN=&IMEI=&SIPURI=&TELURI=&LEAUsername=leaCli&LIBaddr=1.2.3.4&Status=2000k
```

```
CLI# 3?AAUsername=aaCli&ReqId=222-11
```

```
3?ReqId=222-11&IMSI=1234567890&MSISDN=&IMEI=&SIPURI=&TELURI=&ValidFrom=26.08.2005&ValidTo=26.12.2005&StartTime=10:10&EndTime=10:12&AuthorizedOptions=3&AuthorizedInterceptType=7&LEAUsername=leaCli&LIBaddr=1.2.3.4&WarrantID=waid2&IAId=&Status=2000k
```

## 4.9 Changing the validity period of an authorisation

The CLI session has been opened. *aaCli* has authorised *leaCli* to intercept a target. The request ID is 222-11. *aaCli* shortens the validity period of the authorisation and checks the result.

```
CLI# 4?AAUsername=aaCli&ReqId=222-11&ValidTo=26.11.2005&EndTime=10:12
```

```
4?Status=2000k
```

```
CLI# 3?AAUsername=aaCli&ReqId=222-11
```

```
3?ReqId=222-11&IMSI=1234567890&MSISDN=&IMEI=&SIPURI=&TELURI=&ValidFrom=26.08.2005&ValidTo=26.11.2005&StartTime=10:10&EndTime=10:12&AuthorizedOptions=3&AuthorizedInterceptType=7&LEAUsername=leaCli&LIBaddr=1.2.3.4&WarrantID=waid2&IAId=&Status=2000k
```

## 4.10 Listing interceptions

The CLI session has been opened. *aaCli* has authorised *leaCli* to intercept a target. The request ID is 222-11. *leaCli* lists its interceptions: first the active interceptions, then uninitialised interceptions, then all interceptions, and finally interception 222-11.

```
CLI# 100?LEAUsername=leaCli&QueryType=ACT
100?Status=200Ok
CLI# 100?LEAUsername=leaCli&QueryType=UNI
100?ReqId=222-11&IMSI=1234567890&IMEI=&MSISDN=&SIPURI=&
TELURI=&IsActive=0&Status=200Ok
CLI# 100?LEAUsername=leaCli&QueryType=ALL
100?ReqId=222-11&IMSI=1234567890&IMEI=&MSISDN=&SIPURI=&
TELURI=&IsActive=0&Status=200Ok
CLI# 104?LEAUsername=leaCli&ReqId=222-11
104?ReqId=222-11&IMSI=1234567890&IMEI=&MSISDN=&SIPURI=&
TELURI=&ValidFrom=26.08.2005&ValidTo=26.11.2005&StartTime=1
0:10&EndTime=10:12&AuthorizedOptions=3&AuthorizedInterceptT
ype=7&InterceptType=&IsActive=0&LIBaddr=1.2.3.4&Interceptio
nOptions=&InterceptionOptionsIRI=&WarrantID=waid2&IAId=&FTC
IdCC=&FTCIdIRI=&Status=200Ok
```

## 4.11 Creating File Transfer Configuration (FTC)

The CLI session has been opened. *leaCli* defines an FTC and then views it.

```
CLI# 108?LEAUsername=leaCli&FwdAddr=2.3.4.5&FwdPath=
./iriandcc&FwdUsername=user&FwdPasswd1=passwd&FwdPasswd2=
passwd&TransmissionProtocol=FTP&FwdDelay=10&FwdSize=50000&
Description=Combined_FTC_for_IRI_and_CC
108?FTCId=leaCli-3&Status=200Ok
CLI# 111?LEAUsername=leaCli&FTCId=leaCli-3
111?FwdAddr=2.3.4.5&FwdPath=./iriandcc&FwdUsername=user&
TransmissionProtocol=FTP&FwdDelay=10&FwdSize=50000&Descript
ion= Combined_FTC_for_IRI_and_CC&Status=200Ok
```

## 4.12 Changing interception settings

The CLI session has been opened. *aaCli* has authorised *leaCli* to intercept a target. The request ID is 222-11. *leaCli* defines the interception settings, which

is mandatory before activating the interception. *leaCli* then checks the result by listing the interception.

```
CLI# 103?LEAUsername=leaCli&ReqId=222-11&
InterceptionOptions=14&InterceptType=7&FTCIIdCC=leaCli-3&
FTCIIdIRI=leaCli-3
103?Status=2000k
CLI# 104?LEAUsername=leaCli&ReqId=222-11
104?ReqId=222-11&IMSI=1234567890&IMEI=&MSISDN=&SIPURI=&
TELURI=&ValidFrom=26.08.2005&ValidTo=26.11.2005&StartTime=1
0:10&EndTime=10:12&AuthorizedOptions=3&AuthorizedInterceptT
ype=7&InterceptType=7&IsActive=0&FwdDelayCC=10&FwdSizeCC=50
000&FwdDelayIRI=10&FwdSizeIRI=50000&LIBAddr=1.2.3.4&Interce
ptionOptions=14&InterceptionOptionsIRI=14&FwdPathCC=./irian
dcc&FwdPathIRI=./iriandcc&FwdUsernameCC=user&FwdUsernameIRI
=user&WarrantID=waid2&FwdAddrCC=2.3.4.5&FwdAddrIRI=2.3.4.5&
IAId=&FTCIIdCC=leaCli-3&FTCIIdIRI=leaCli-3&Status=2000k
```

## 4.13 Activating an interception

The CLI session has been opened. *aaCli* has authorised *leaCli* to intercept a target. The request ID is 222-11. *leaCli* has defined the interception settings. *leaCli* activates interception 222-11 and checks the result by viewing the interception.

```
CLI# 101?LEAUsername=leaCli&ReqId=222-11
101?Status=2000k
CLI# 104?LEAUsername=leaCli&ReqId=222-11
104?ReqId=222-11&IMSI=1234567890&IMEI=&MSISDN=&SIPURI=&
TELURI=&ValidFrom=26.08.2005&ValidTo=26.11.2005&StartTime=1
0:10&EndTime=10:12&AuthorizedOptions=3&AuthorizedInterceptT
ype=7&InterceptType=7&IsActive=1&FwdDelayCC=10&FwdSizeCC=50
000&FwdDelayIRI=10&FwdSizeIRI=50000&LIBAddr=1.2.3.4&Interce
ptionOptions=14&InterceptionOptionsIRI=14&FwdPathCC=./irian
dcc&FwdPathIRI=./iriandcc&FwdUsernameCC=user&FwdUsernameIRI
=user&WarrantID=waid2&FwdAddrCC=2.3.4.5&FwdAddrIRI=2.3.4.5&
IAId=&FTCIIdCC=leaCli-3&FTCIIdIRI=leaCli-3&Status=2000k

CLI# 100?LEAUsername=leaCli&QueryType=DEA
100?Status=2000k
CLI# 100?LEAUsername=leaCli&QueryType=ACT
100?ReqId=222-11&IMSI=1234567890&IMEI=&MSISDN=&SIPURI=&
TELURI=&IsActive=1&Status=2000k
```

## 4.14 Deactivating an interception

The CLI session has been opened. *aaCli* has authorised *leaCli* to intercept a target. The request ID is 222-11. *leaCli* has defined the interception settings and activated interception 222-11. *leaCli* deactivates interception 222-11 and checks the result by listing interceptions.

```
CLI# 102?LEAUsername=leaCli&ReqId=222-11
102?Status=200Ok
CLI# 100?LEAUsername=leaCli&QueryType=ALL
100?ReqId=222-11&IMSI=1234567890&IMEI=&MSISDN=&SIPURI=&
TELURI=&IsActive=0&Status=200Ok
CLI# 100?LEAUsername=leaCli&QueryType=DEA
100?ReqId=222-11&IMSI=1234567890&IMEI=&MSISDN=&SIPURI=&
TELURI=&IsActive=0&Status=200Ok
CLI# 100?LEAUsername=leaCli&QueryType=ACT
100?Status=200Ok
```

## 4.15 Revoking an authorisation

The CLI session has been opened. *aaCli* has authorised *leaCli* to intercept a target. The request ID is 222-11. *aaCli* revokes the interception and checks the result by listing the authorisations and then the interceptions of the *leaCli*.

```
CLI# 2?AAUsername=aaCli
2?ReqId=222-11&IMSI=1234567890&MSISDN=&IMEI=&SIPURI=&
TELURI=&LEAUsername=leaCli&LIBaddr=1.2.3.4&Status=200Ok
CLI# 5?AAUsername=aaCli&ReqId=222-11
5?Status=200Ok
CLI# 2?AAUsername=aaCli
2?Status=200Ok
CLI# 100?LEAUsername=leaCli&QueryType=ALL
100?Status=200Ok
```

## 4.16 Managing interception areas

To use location dependent interception, the users must define the interception areas. The CLI session has been opened. The user creates new interception areas

*Finland* and *Airport*. Then the user checks that the created interception areas are correct. Finally, the user creates a new location dependent authorisation.

```

CLI# 205?IAName=Finland&MCC=358
205?IAId=222-1&Status=200Ok
CLI# 1007
1007?IAName=Finland&IAId=222-1&IAName=Airport&IAId=222-
2&Status=200Ok
CLI# 1008?IAId=222-1
1008?IAId=222-1&MCC=358&Status=200Ok
CLI# 1008?IAId=222-2
1008?IAId=222-2&CGI=3582312345123453&CGI=3582312345123454&
CGI=3582312345123455&Status=200Ok
CLI# 1?AAUsername=aaCli&IMSI=1234567890&LEAUsername=leaCli&
LIBaddr=1.2.3.4&AuthorizedInterceptType=7&AuthorizedOptions
=3&ValidFrom=26.08.2005&StartTime=10:10&ValidTo=26.12.2005&
EndTime=10:12&WarrantID=waid3&IAId=222-1
1?ReqId=222-13&Status=200Ok

```

## 4.17 Removing an LEA user account

The CLI session has been opened. *aaCli* has created the LEA user *leaCli*. *leaCli* has no authorisations. *aaCli* removes *leaCli* and checks the result by listing the LEA users *aaCli* has created.

```

CLI# 21?AAUsername=aaCli
21?LEAUsername=leaCli&LEARrealname=LEA_for_CLI_use&LEAUserSt
atus=ACTIVE&Status=200Ok
CLI# 22?AAUsername=aaCli&LEAUsername=leaCli
22?Status=200Ok
CLI# 21?AAUsername=aaCli
21?Status=200Ok

```

## 4.18 Making a backup of the LIC

The CLI Admin session has been opened. First the backup configuration is created. Then the current backup configuration is checked, and then the backup of the LIC is made immediately.

```
cliadmin#  
224?FwdAddr=123.4.5.6&FwdPath=/var/admin/libbackup&FwdUserNa  
me=admin&BackupInterval=-2&BackupDate=&BackupTime=12:00&Wee  
kday=1000101  
224?Status=2000k  
cliadmin# 203  
203?FwdAddr=123.4.5.6&FwdPath=/var/admin/libbackup&FwdUserna  
me= tonmaki&BackupInterval=-  
2&BackupDate=31.08.2005&BackupTime=12:00  
&Weekday=0100101&Status=2000k  
cliadmin# 204  
204?Status=2000k
```

## 4.19 Adding a network element

The CLI admin session has been opened. The user adds a new network element (SGSN) and then views the configured network elements.

```
cliadmin#  
226?NE=1.2.3.6&NEType=SGSN&Port=50088&OnTheFly=1&Protocol=1  
226?Status=2000k  
cliadmin# 1004  
1004?NE=1.2.3.4&NEType=LIB&NEStatus=3&Port=50097&Protocol=2  
&LIEType=0&LIEDescription=Lawful Interception Browser,  
version 4.0 (build 4.0-  
396)&LIESupportedTargets=&NE=1.2.3.6&NEType=SGSN&NEStatus=1  
&Port=50088&OnTheFly=1&Protocol=1&LIEType=&LIEDescription=&  
LIESupportedTargets=&Status=2000k
```

## 4.20 Exiting a CLI session

The CLI session has been opened. The user exits the CLI session and closes the Telnet connection.

```
CLI# 1002  
Connection closed by foreign host.
```



**References**

1. Nokia LIG Release 4 Product Documentation: Reference Guide
2. Nokia LIG Release 4 Product Documentation: Auditor's Guide

**Glossary**

AA	Authorising Authority
ASCII	American Standard Code for Information Interchange
CC	Communication Content
CGI	Cell Global Identification
CLI	Command Line Interface
CPS	Connection Processing Server
FTP	File Transfer Protocol
FTC	File Transfer Configuration
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSN	GPRS Support Node
IA	Interception Area
IMEI	International Mobile Station Equipment Identity
IMM2	Nokia IMS Release 2
IMM3	Nokia IMS Release 3
IMS	IP Multimedia Core Network Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSO	Nokia (Ipsilon) Router Operating System
IRI	Interception-Related Information
IPv4	Internet Protocol, version 4
IPv6	Internet Protocol, version 6
LAC	Location Area Code
LAI	Location Area Identifier
LDI	Location dependent interception
LEA	Law Enforcement Agency
LI	Lawful Interception
LIB	Lawful Interception Browser
LIC	Lawful Interception Controller
LIE	Lawful Interception Extension
LIG	Lawful Interception Gateway

LIMS	Lawful Interception Management System
NE	Network Element
MCC	Mobile Country Code
MNC	Mobile Network Code
MS	Station
MSISDN	Mobile Subscriber International ISDN Number
PDP	Packet Data Protocol
RAI	Routing area identity
SAI	Service Area Identifier
SCP	Secure Copy
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SIP URI	SIP Uniform Resource Identifier
SNMP	Simple Network Management Protocol
SSH	Secure Shell
strFTP	Streaming FTP
TEL URI	Telephony Uniform Resource Locator
ULIC	UMTS LI Correlation header
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier