

OpenScape 4000 V8 OpenScape 4000 CSTA and Phone Services

Service Documentation

A31003-H3180-S106-2-7620

Provide feedback to further optimize this document to edoku@unify.com.

As reseller please address further presales related questions to the responsible presales organization at Unify or at your distributor. For specific technical inquiries you may use the support knowledgebase, raise - if a software support contract is in place - a ticket via our partner portal or contact your distributor.

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Copyright © Unify Software and Solutions GmbH & Co. KG 08/2017
Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany

All rights reserved.

Reference No.: A31003-H3180-S106-2-7620

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

OpenScape 4000 CSTA and Phone Services - Content

1 Introduction	5
2 General overview	7
2.1 OpenScape 4000 V7 Maximum Values	7
2.2 CSTA application connection	7
3 Requirements	9
3.1 Hardware Requirements	9
3.2 Software Requirements	9
3.2.1 Operating System	9
3.2.2 Supported Software	9
3.3 Configuration Batch Description	9
3.4 Configuration Requirements	10
4 Port List	11
5 OpenScape 4000 CSTA – Introduction	13
5.1 Application Environment	13
5.2 Portal – IP Address Configuration	15
5.3 New features	18
5.3.1 New features in OpenScape 4000 V7	18
5.3.1.1 Discontinuation of the CSTA Licensing	18
5.3.1.2 Further enhancements for the OpenScape 4000 – OpenScape UC interaction	19
5.3.2 Important News in V7 R2	20
5.3.2.1 Circuit connectivity	20
5.3.2.2 General enhancements	21
5.3.2.3 Security relevant changes	21
5.4 CBAdmin – Configuration and Management	22
5.4.1 Connectivity Adapter Instance	22
5.4.2 Status – Connection Check	27
5.4.3 Logging	28
5.4.3.1 Connectivity Adapter logs	28
5.4.3.2 Download	29
5.4.3.3 Component log properties	30
5.4.4 Statistics	30
5.4.5 Phone Service UI	33
5.4.6 Settings	34
5.4.6.1 User/Password	34
5.4.6.2 CBAdmin – Trusted IP Addresses	34
5.4.6.3 HTTPS Connection	35
5.4.7 Circuit Interface Connectivity Application	37
5.4.7.1 General Description	37
5.4.7.2 Configuration	38
5.4.8 Advanced Configuration	39
5.4.9 Additional Supported Services via OpenScape 4000 Assistant	41
5.4.10 Special Settings	42
5.4.10.1 Concept of “Presentation Indicator for Devices” in CSTA Events	42
5.4.10.2 Delayed CSTA Response Features	43
5.4.10.3 Support of the Offered mode of the Alerting state	43

5.4.10.4	Delivering deviceIDs in E.164 Format (SFR international)	44
5.4.10.5	Enhancements for supporting OpenScape UC	45
5.4.10.6	Special Settings to Application Connection	49
5.4.10.7	Special setting to deliver physical answering device information via OpenScape 4000 CSTA	50
5.4.10.8	Umlaut Characters	51
5.4.10.9	Hunt Group Behavior	51
5.4.10.10	UserToUser Info	51
5.4.10.11	Usage with OpenSape Contact Center (OSCC)	52
5.5	Fault management	52
6	Phone Services – Introduction	53
6.1	Overview	53
6.1.1	EasyLookup	53
6.1.2	EasySee	55
6.1.3	EasyMail	55
6.1.4	EasyShare	56
6.1.5	EasyUC	57
6.2	Structure	59
6.3	Requirements	61
6.4	Configuration	62
6.4.1	Configuration Steps	62
6.4.2	AMO Configuration OpenScape 4000 V7	62
6.4.3	OpenScape 4000 CSTA	63
6.5	LDAP Connection Configuration for EasyLookup	72
6.5.1	CCS Configuration	72
6.5.2	CCS LDAP Configuration	73
6.5.3	Phone Services with Multiple LDAP Servers	76
6.5.4	Configuration Example: Web Page Design	78
6.6	Suspension	79
6.7	OpenScape 4000 Phone Services Client Application or OpenScape 4000 PSCA (prev. XCI Tray)	81
	List of Figures	85
	List of Tables	87
	Index	89

1 Introduction

OpenScape 4000 CSTA...

- is a protocol converter, which converts the internal **OpenScape 4000 ACL** (Application Connectivity Link) protocol into a standardized CSTA III protocol, based on the encoding types ASN.1 (Abstract Syntax Notation One) and XML (eXtensible Markup Language).

The software can be installed as a OpenScape 4000 V7 integrated installation.

- is a product integrated to the OpenScape 4000 System that on top of providing independent solutions, merges the advantages of OpenScape (formerly HiPath) CAP V3.0 and CAP Inside V1.
 - CSTA III, ASN.1 and CSTA III, XML support following the standard ECMA -269 (9th edition, 2011)
 - High performance interface
 - OpenScape 4000 Phone Services
 - Integrated to the system's HBR mechanism
 - Configuration management via Web interface

2 General overview

2.1 OpenScape 4000 V7 Maximum Values

Based on **OpenScape 4000 V7 Memory Allocation**, the following maximum values affect the maximum number of supported ACL-C – OpenScape 4000 CSTA connections:

AMO DIMSU: ECCS 50

AMO DIMSU: APPL 98

AMO XAPPL: SUBAPPL 32 (Restriction of the system: upper 16, i.e. 17-32 can be used by CSTA applications.)

AMO DIMSU: ACDMONID 5000

See the AMO description for more details.

NOTE: One Connectivity Adapter can support 4 application links simultaneously and maximum of 8 Connectivity Adapters supported.

2.2 CSTA application connection

1 CSTA link

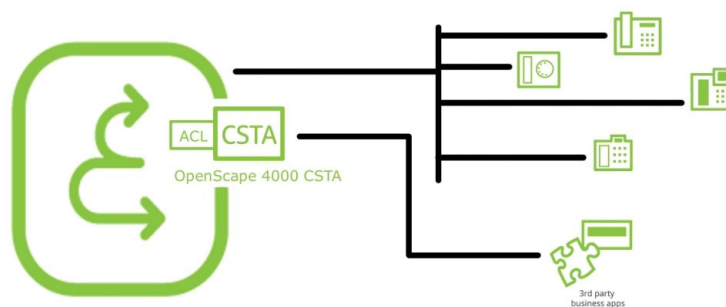


Figure 1 Scenarios - One CSTA link

CSTA applications can connect to the OpenScape 4000's built-in CSTA interface.

A maximum of 4 CSTA links per process – Connectivity Adapter (CA)

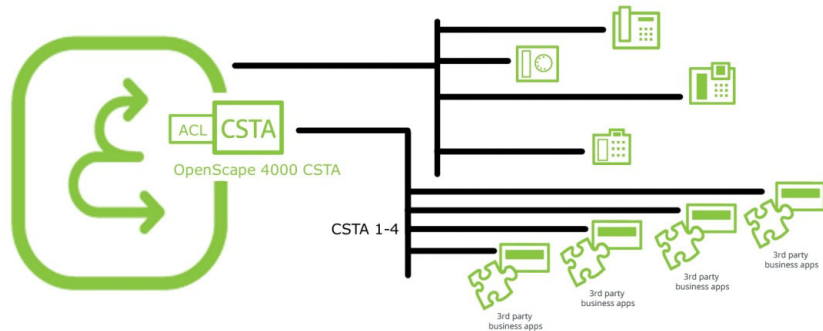


Figure 2 Scenarios - Four CSTA links per process

Maximum 4 applications can use the same Connectivity Adapter.

Maximum 8 (16) Connectivity Adapters on a system

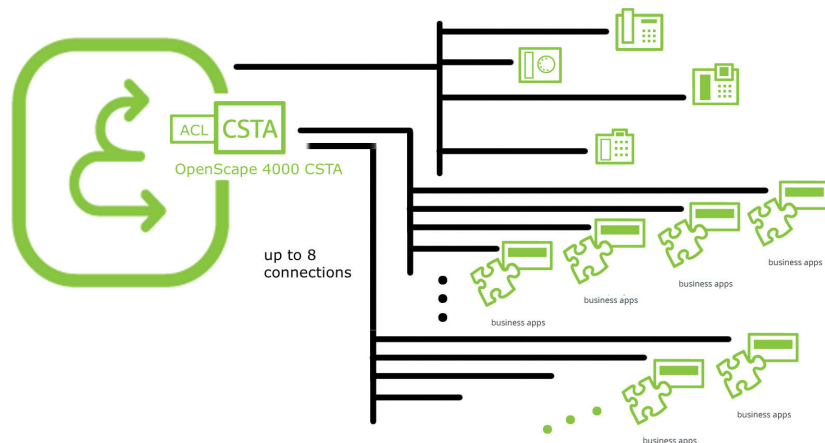


Figure 3 Maximum 8 Connectivity Adapters per system

Starting V7 R2, in case of enough physical memory on the hardware the CSTA VM can have more memory than usual (i.e. 2GB instead of 786 MB). It is checked and if the adequate amount of memory is available on the VM, the maximal number of Connectivity Adapters is 16. Please be aware that in case of any fall back, the system will not delete any CA-s. Any recovery (e.g. changing the faulty physical memories or deleting the least necessary connectivity adapters) must be done manually.

3 Requirements

3.1 Hardware Requirements

OpenScope 4000 CSTA VM is an integrated part of OpenScope 4000 Communication System starting Version 6 and installs with the Communication System.

3.2 Software Requirements

3.2.1 Operating System

Integrated OpenScope 4000 CSTA is a VM having a Novell SuSE Linux Enterprise Server (SLES) 10 SP4 (V7 R0), SLES 11 SP3 (V7 R1) or SLES 11 SP4 (V7 R2) running as an operation system.

3.2.2 Supported Software

IBM Java 6 is used for the integrated OpenScope 4000 CSTA versions up till V7 R1 and IBM Java 7 in V7 R2.

3.3 Configuration Batch Description

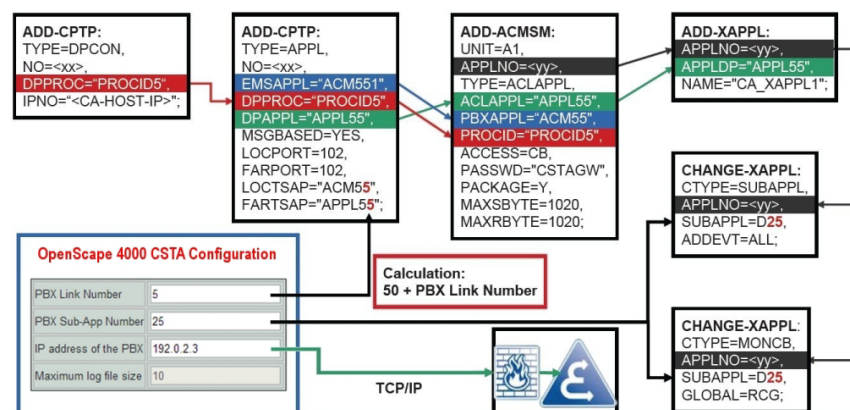


Figure 4 Configuration batch description

Figure 4 on Page 9 and the following description give an overview of the configuration added (automatically) for the Connectivity Adapters' PBX connections. Relevant memory allocation (points 1-2) is configured only at installation, the connection (points 4-9) is configured automatically for each Connectivity Adapter.

1. Maximum number of ACL-C applications is set at setting up the default connectivity adapter:

AMO-DIMSU parameter: ECCS:

2. Maximum number of monitored devices is also set

AMO-DIMSU parameter ACDMONID, number of monitored id sets (e.g. acdagents -only acd-g). The maximum number of permitted monitored device sets. Any attempt by the application to set more monitoring points than permitted by the maximum number of monitored devices will be rejected.

3. Call processing timers must be set

AMO-CTIME, customer-specific CP1 timers, switching unit manages the call processing timers, which are evaluated by the MakeCall requests.

4. Initial communication ACL-C Link is configured

AMO-CPTP, communication parameters for tcp/ip connection (as ACL-C identifier only) TYPE: DPCON

5. Application interface parameters (transport address)

AMO-CPTP, communication parameters for tcp/ip connection TYPE: APPL

6. ACL Manager parameters

AMO-ACMSM, ACL manager communication parameter APPLTYP= ACLAPPL

7. XAPPL application

AMO-XAPPL, DVA -application ACL

8. XAPPL sub-application parameters

AMO-XAPPL, CTYPE: SUBAPPL.

9. XAPPL monitored elements

AMO-XAPPL, CTYPE: MONCB.

3.4 Configuration Requirements

From HiPath 4000 V6 all CSTA applications must use the CA4000 adaptor of the integrated OpenScope 4000/HiPath 4000 CSTA via customer LAN port. This includes HiPath CAP V3.0 when used. Applications using direct ACL connectivity via Atlantic LAN are no longer supported.

4 Port List

The OpenScape 4000 CSTA has a default configuration. A Connectivity Adapter (CA) instance (`CA4000_Default`) is configured automatically during the installation.

This default CA has four application connections configured, which listen on the following ports:

- 1040 (used as default in OSCC, Xpressions, DTB, Genesys, CICA and several other applications)
- 2205 (used as default in e.g. VAS-B)
- 2209 (used as default in e.g. VAS-B, HiCALL)
- 27535 (used as default in e.g. DTB Light)

This default configuration is created only once when the CSTA is installed and is not touched again. It is therefore possible to change it and upgrades do not overwrite it.

5 OpenScape 4000 CSTA – Introduction

OpenScape 4000 CSTA is part of the image installation of a OpenScape 4000 V7 installation. The following facilities are available:

- CBAAdmin Web server **single sign on** access via OpenScape 4000 Assistant
- Default configuration of the first Connectivity Adapter instance during the installation (CA4000_DEFAULT)
- Automatic AMO configuration, based and initialized on a new Connectivity Adapter configuration
- Graphical user interface based hotfix and minor release update through OpenScape 4000 Assistant (Software Activation)
- OpenScape Backup and Restore support for configuration data only

5.1 Application Environment

Daemons

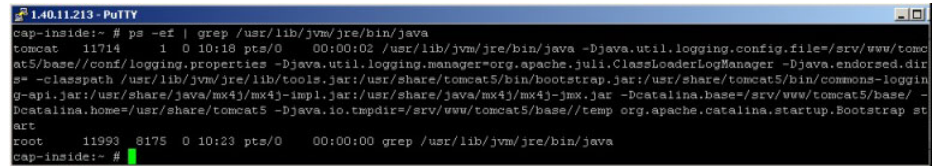
The processes are started automatically when the system reboots.

The daemons exist in `/etc/init.d/`:

- `/etc/init.d/tomcat5` (on V7 R0) and `/etc/init.d/tomcat6` (on V7 R1 and R2)
 - `{start|stop|status|try-restart|restart|force-reload|reload|probe}`
 - The daemon is started at run level: 3 | 5
- `/etc/init.d/CSTA`
 - `{start|stop|status|try-restart|restart|force-reload|reload}`
 - The daemon is started at run level: 2 | 3 | 5

Active processes

The OpenScape 4000 CSTA Web Administration Server starts at run level 3 – 5. The daemon name is `tomcat5` or `6` for V7R0 and V7R1-R2 respectively . A new process is responsible for this: `java`.



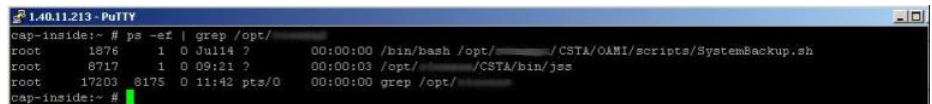
```
cap-inside:~ # ps -ef | grep /usr/lib/jvm/jre/bin/java
tomcat 11714 1 0 10:18 pts/0 00:00:02 /usr/lib/jvm/jre/bin/java -Djava.util.logging.config.file=/srv/www/tomcat5/base/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.endorsed.dirs=-classpath /usr/lib/jvm/jre/lib/tools.jar:/usr/share/tomcat5/bin/bootstrap.jar:/usr/share/tomcat5/bin/commons-logging-api.jar:/usr/share/java/mx4j-impl.jar:/usr/share/java/mx4j-jmx.jar -Dcatalina.base=/srv/www/tomcat5/base/ -Dcatalina.home=/usr/share/tomcat5 -Djava.io.tmpdir=/srv/www/tomcat5/base/temp org.apache.catalina.startup.Bootstrap start
root 11993 8175 0 10:23 pts/0 00:00:00 grep /usr/lib/jvm/jre/bin/java
cap-inside:~ #
```

Figure 5 java process

This Web server listens on port 443, 8081 and 8080.

As before, the process `jss` is started.

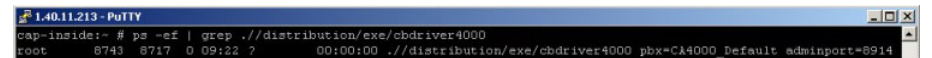
A `bash` process is also active for supporting communication to Assistant, periodic saving of the config and hotfix state, periodic check of the availability of NFS share on System and several self-checking abilities.



```
cap-inside:~ # ps -ef | grep /opt/
root 1876 1 0 Jul14 2 00:00:00 /bin/bash /opt/ /CSTA/OAMI/scripts/SystemBackup.sh
root 8717 1 0 09:21 2 00:00:03 /opt/ /CSTA/bin/jss
root 17203 8175 0 11:42 pts/0 00:00:00 grep /opt/
cap-inside:~ #
```

Figure 6 bash process

By default, the Connectivity Adapter instance **CA4000_Default** is created automatically during the rpm installation. It includes the complete OpenScape 4000 ACL AMO configuration.



```
cap-inside:~ # ps -ef | grep ./distribution/exe/cbdriver4000
root 8743 8717 0 09:22 2 00:00:00 ./distribution/exe/cbdriver4000 pbx=CA4000_Default adminport=8914
cap-inside:~ #
```

Figure 7 cbdriver4000 process

NOTE: For each additional Connectivity Adapter instance configured via the Web server, an individual `cbdriver4000` process is also started.

OpenScape 4000 CSTA IP configuration

As for the OpenScape 4000 Platform Administration (Portal) and OpenScape 4000 Assistant, the OpenScape 4000 CSTA needs its own IP address in the customer LAN.

An independent connection is configured on the other side for internal communication. Another process is therefore started to link the internal Web services to another NIC.

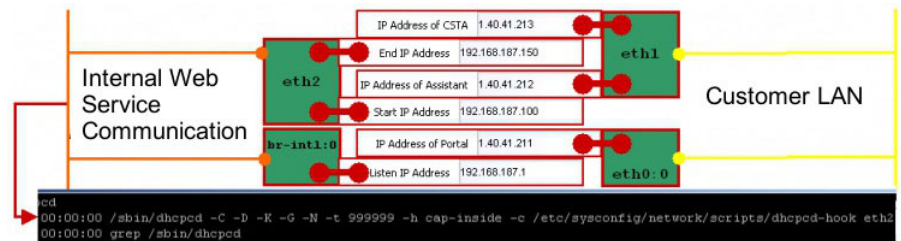


Figure 8 Internal WEB Service Communication

The Portal also has connections to both LAN networks.

A third network interface card is configured to support internal Atlantic LAN communication. The CA instance uses this interface to establish a link to the CMS (Communication Management System).

The Portal also has a connection to the ATL LAN network.

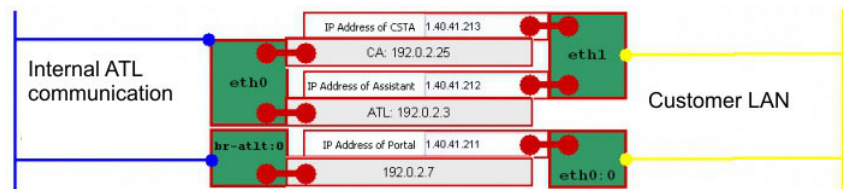


Figure 9 Internal Communication

5.2 Portal – IP Address Configuration

Log on to **OpenScope 4000 V6 Assistant** and select:

Expert Mode > Platform Portal

Component	Version	System Start date/time
Platform	V7 R0.9.0	2013-10-04 11:55
Assistant	V7 R0.12.0	2013-10-04 12:00
RMX	V7 R0.9.0	2013-10-04 10:00
CSTA	V7 R0.203.0	2013-10-04 12:00
SoftGate on Platform	L0-TATA1.006-007	
OpenScope FM	7 R0.68.9	

Important Hints
3 years license for SLES Upgrade Protection will expire in 95 days. 2013-10-08 10:02:57

Figure 10 Connect to OpenScope 4000 Platform Administration (Portal)

Select **System** to configure the OpenScope 4000 CSTA IP address.



Figure 11 System

Select **LAN Wizard** to configure the OpenScape 4000 CSTA IP address.

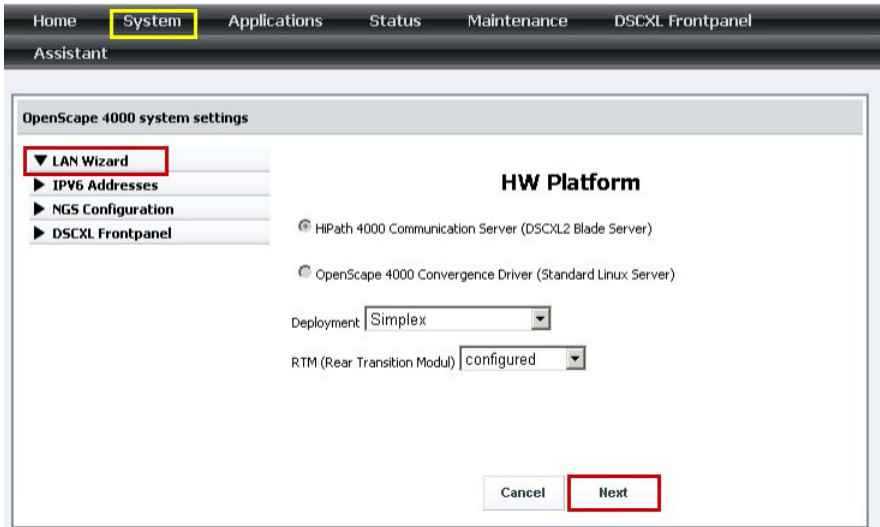


Figure 12 System - LAN Wizard - Step 1

Press **Next**.

Figure 13 System - LAN Wizard - Step 2

Enter the OpenScape 4000 CSTA IP address.

Figure 14 System - LAN Wizard - Step 3

All OpenScape 4000 CSTA applications must use this IP address to establish a connection to the integrated OpenScape 4000 CSTA.

Press **Next**.

▼ LAN Wizard

▶ IPv6 Addresses

▶ NGS Configuration

▶ DSCXL Frontpanel

Internal LAN

Listen IP Address

192.168.187.1

Start IP Address

192.168.187.100

End IP Address

192.168.187.150

Netmask

255.255.255.0

System

Corosync Network

10.0.187.0

Multicast IP Address

226.94.1.1

Multicast Port

5405

System Name Node

linux-os4000v6-server

Back

Cancel

Finish

Figure 15 System - LAN Wizard - Step 4

Press **Finish**.

HomeSystemApplicationsStatusMaintenanceDSCXL Frontpanel

Assistant

OpenScape 4000 system settings

▼ LAN Wizard

▶ IPv6 Addresses

▶ NGS Configuration

▶ DSCXL Frontpanel

Action successfully completed.

Installation Log File

Figure 16 Wizard complete

5.3 New features

5.3.1 New features in OpenScape 4000 V7

5.3.1.1 Discontinuation of the CSTA Licensing

License control for CSTA is removed in V7. However the CSTA functionality will be continued in V7 license check for CSTA connectivity has been cut off. The CSTA license has been removed in the ordering tools, CLS and OpenScape 4000 V7 license check. The free 10 CSTA users in OpenScape 4000 Base license has also been removed. This also means that no license highlighting is available in the GUI.

5.3.1.2 Further enhancements for the OpenScape 4000 – OpenScape UC interaction

General behaviour

Interaction with the OpenScape UC application requires a fully application controlled service handling and a switching function with support of early release mechanism. In order to fulfill these requirements several basic changes were made to provide this kind of interface and in the meanwhile keep the original CSTA modell intact.

The new event mapping and service handling mechanism is designed for UC application. It is highly different from the already existing monitoring, so a careful configuration is needed. The configured values are checked against the version of the OpenScape 4000 CSTA and they might be overwritten according to the released feature set if used on an older version. The UC relevant configuration parameters are listed in the following table:

Name	Description	Default value in Connectivity Adapter	Comments
E164_NUMBER_FORMAT	Support E.164 number format. Monitoring can be started with the convenient number type only.	0 (off)	Available from V6 R2.13, CSTA HF R13.200.2
OFFERED_TO_BOTH_SIDE	Send the Offered event to the calling party.	0 (off)	
DIVERTED_TO_BOTH_SIDE	Send the Diverted event to the calling party	0 (off)	
ONS_MONITORING	Recognise and map the binding info, choose the ONS number and use it as monitored device	0 (off)	
MAP_REMOTE_FEATURE	Map the Call Information event as if it had been a state event	0 (off)	

Tabelle 1 Configuration parameters in Connectivity Adapter

The initial steps of the interworking were already introduced in the OpenScape 4000 CSTA V1 R11/ R13. These are the following:

- Offer the incoming call's control to monitoring applications: see [Section 5.4.10.3, "Support of the Offered mode of the Alerting state"](#)
- Enhance the supported number formats: see [Section 5.4.10.4, "Delivering deviceIDs in E.164 Format \(SFR international\)"](#)
- Provide DIVERTED event also for the calling side [Section 5.4.10.5, "OFFERED and DIVERTED events for the calling side"](#) (developed for V7 but merged back to R13)

The features listed below are implemented for the V7.

- One number feature controlled dynamically by the application: see [Section 5.4.10.5, "ONS based monitoring using the binding information"](#)
- Device search based on a user defined list: see [Section 5.4.10.5, "Dynamic device list in the Accept Call request"](#)
- Provide state transitions of the remote side: see [Section 5.4.10.5, "Remote features"](#)
- Enhance Single Step Transfer service: see [Section 5.4.10.5, "Single Step Transfer for the consulting party"](#) and [Section 5.4.10.5, "Seamless Handover by Single Step Transfer"](#)
- Send Offered events also to the calling side: see [Section 5.4.10.5, "OFFERED and DIVERTED events for the calling side"](#)
- Enhance Deflect call service: see [Section 5.4.10.5, "Deflect of the second call"](#)
- Emulate an early release mechanism for Deflect, Call Forward No Reply and Single Step Transfer scenarios: see [Section 5.4.10.5, "Support the early release mechanism for Deflect, Call Forward No Answer and Single Step Transfer scenarios"](#)
- Enhance group call functionalities for the Offered mode: see [Section 5.4.10.5, "Offered mode for Hunt Group members and ACD Agents"](#)
- Provide a special CSTA flow for the Hunt Group calls where the next destination is sent to the application before the call is actually offered to it: see [Section 5.4.10.5, "Special CSTA flow for the Hunt Group calls"](#)

5.3.2 Important News in V7 R2

5.3.2.1 Circuit connectivity

Several enhancements were made in OpenScape 4000 CSTA in order to support Circuit connectivity.

Connectivity adapter was enhanced:

- to support short tag XML (ECMA 323 Annex D)
- with new functionality “DoNotDisturb with Snooze Duration
- with new private elements and services needed for the Circuit client’s registration
- with the support of EPID (endpoint identifier for the physical used device)
- with Extended Services Permitted private element for Seamless Handover
- to provide / support Centralized Call Log handling
- to support private data format similar to that of OpenScape Voice in order to provide a more common CSTA interface towards Circuit

The changes of the CSTA interface can be seen in more details in the Application Developer’s Guide.

A new application named Circuit Interface Connectivity Application (CICA) was implemented in order to handle the several thousands of Circuit connections and to act as one standard CSTA application toward Connectivity Adapter. See general description in [Section 5.4.7, “Circuit Interface Connectivity Application”](#).

5.3.2.2 General enhancements

The logging of all “CSTA processes” was enhanced to use syslog when it is necessary to send an SNMP trap about the logged event. See [Section 5.5, “Fault management”](#) and the OpenScape 4000 V7 system’s and Assistant’s documentation for further information.

A new log housekeeping mechanism is introduced, the backup logfiles are stored in compressed format. See [Section 5.4.3, “Logging”](#) for more details.

Starting V7 R2 a performance monitoring tool is part of the installation.

The maximal number of the connectivity adapters can be 16 if the system is installed on a hardware where the CSTA VM can have enough (more than 1.5 GB) memory. See also [Page 8](#).

CSTA XML interface of the Connectivity Adapter was enhanced with support of the accented and cyrillic characters provided in the user’s name information (PERSI-NAME) in the CSTA events. The character set supported in CorNet-TS is converted to UTF8.

5.3.2.3 Security relevant changes

Support of TLS 1.2 is enabled by default. SSL V3 is not supported anymore.

5.4 CBAdmin – Configuration and Management

5.4.1 Connectivity Adapter Instance

Log on to **OpenScope 4000 V7 Assistant** and select:
Expert Mode > CSTA

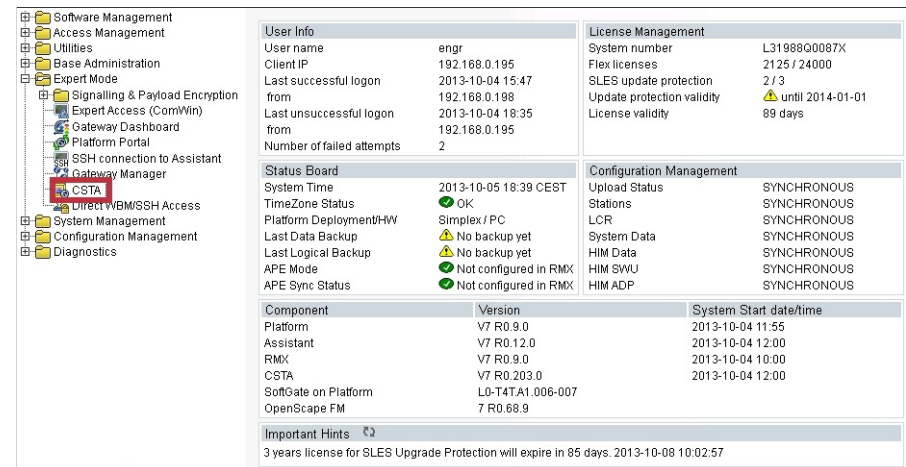


Figure 17 Connect to OpenScope 4000 CSTA

The CA instance **CA4000_Default** is created and configured automatically during the installation.



Figure 18 Connectivity Adapter List - Select Connectivity Adapter

To display the default connection parameters, press **Select Connectivity Adapter**.

CA4000_Default Configuration

[advanced](#)

PBX Link Number	5
PBX Sub-App Number	25
Maximum log file size	10

☐ UC functionality
☐ E.164 number format
☐ Offered to both side
☐ Diverted to both side
☐ ONS monitoring
☐ Map remote feature

Offered mode ☐

Configured applications	
app_1040	<input type="button" value="edit"/> <input type="button" value="delete"/>
app_2205	<input type="button" value="edit"/> <input type="button" value="delete"/>
app_2209	<input type="button" value="edit"/> <input type="button" value="delete"/>
app_27535	<input type="button" value="edit"/> <input type="button" value="delete"/>

Status: RUNNING

Update Device List

Figure 19 Configuration - CA4000_Default Configuration

The default connection parameters are:

- **PBX-Link Number:** 5
- **PBX Sub-App Number:** 25

Configured applications:

- **app_1040:** Port 1040
- **app_27535:** Port 27535
- **app_2205:** Port 2205
- **app_2209:** Port 2209

To add a new CA instance, click **Add New Connectivity Adapter**.

[Settings](#) | [Connectivity Adapter List](#) | [Log](#) | [Advanced Configuration](#) | [CICA](#) | [Phone Services UI](#) | [Logout](#)

Select Connectivity Adapter



Figure 20 Connectivity Adapter List - Add New Connectivity Adapter

A new CA instance can be connected only to the same OpenScape 4000 V6.

Add New Connectivity Adapter



Figure 21 Add CA

Enter the name of the new CA Instance and press the button **Add CA**. Please keep in mind that the Connectivity Adapter's name must be shorter than 28 characters

To configure the ACL link connection parameters, select the new CA instance name and press **Select Connectivity Adapter**.

Enter new and not yet existing (used) **PBX-Link Number**, **PBX Sub-Appl Number**, e.g.

- **PBX-Link Number:** 6
- **PBX Sub-Appl Number:** 26

[Settings](#) | [Connectivity Adapter List](#) | [Configuration](#) | [Status](#) | [Log](#) | [Advanced Configuration](#) | [Statistics](#) | [Version](#) | [CICA](#) | [Phone Services UI](#) | [Logout](#)

CA4000_New_CA Configuration

[advanced](#)

PBX Link Number	<input type="text"/>
PBX Sub-App Number	<input type="text"/>
Maximum log file size	10

☐ UC functionality
☐ E.164 number format
☐ Offered to both side
☐ Diverted to both side
☐ ONS monitoring
☐ Map remote feature

Offered mode: ☐ Change

[Link or subapp link isn't defined.](#)

Configured applications

Status: RUNNING

Update Device List

Figure 22 Configuration - Modify

If you address the integrated OpenScape 4000 based on the entered values, the ACL link AMO configuration will be performed automatically.

Press **Modify**.

To add a new OpenScape 4000 CSTA application link, press **Add new application**.

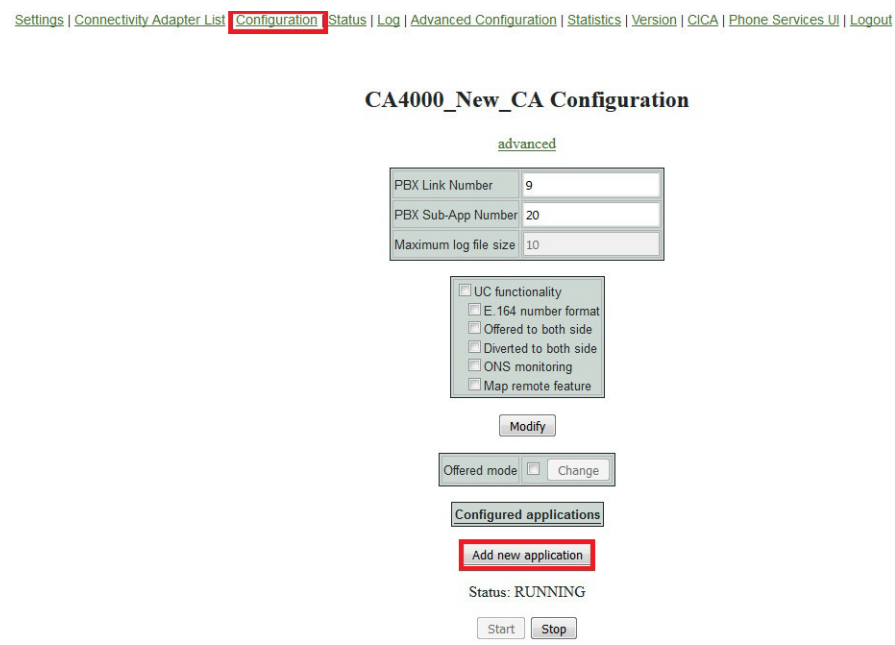


Figure 23 Configuration - Add new application

- Enter new **Application Name**.
- Enter new and not yet existing (used) **TCP-Port**.

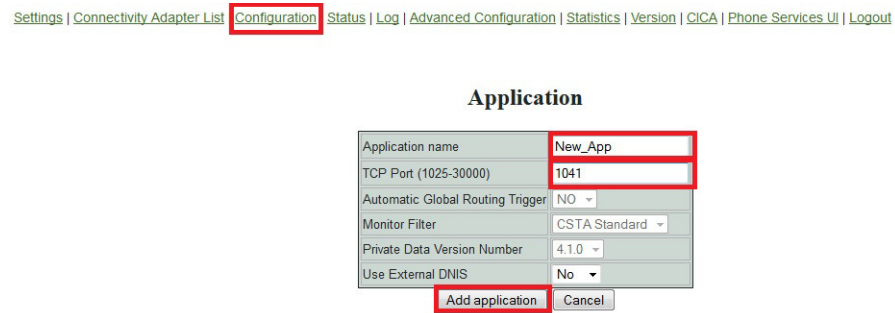


Figure 24 Configuration - Add application

The new CA instance listens on the given port and only one OpenScape 4000 CSTA application can establish a link to this port.

Press **Add application**.

The new application link will be displayed in the **Configured applications** list.

CA4000_New_CA Configuration



[advanced](#)

PBX Link Number	9
PBX Sub-App Number	20
Maximum log file size	10

☐ UC functionality
☐ E.164 number format
☐ Offered to both side
☐ Diverted to both side
☐ ONS monitoring
☐ Map remote feature

Modify

Offered mode ☐ Change

Configured applications
New_App  

Add new application

Status: RUNNING

Start Stop

Update Device List

Update Device List

Figure 25 Configuration - New application added

5.4.2 Status – Connection Check

The CA instance **Status** shows the **PBX Link** to be assigned as **ConnectedAndActive** if the ACL connection to the OpenScape 4000 is up and running.

[Settings](#) | [Connectivity Adapter List](#) | [Configuration](#) | **Status** | [Log](#) | [Advanced Configuration](#) | [Statistics](#) | [Version](#) | [CICA](#) | [Phone Services UI](#) | [Log](#)

CA4000_New_CA Status

PBX Link: ConnectedAndActive
New_App: Disconnected

Figure 26 Status - PBX Link

Also the link status of the application connection is shown. Since the application is not configured yet the connection is inactive.

5.4.3 Logging

General logfiles of the CSTA VM are logged into a `Logs` directory in the installation folder. This is an independent partition mounted to this path. Every Connectivity Adapter instance uses an own subfolder named after itself in the `Logs/Connections` directory. The default max log file size of the Connectivity Adapters is set to 10 MB and can be modified via the GUI. The other logfiles have further possible settings. A new feature in V7 R2 that those log messages that are relevant from security's or availability's point of view are logged through `syslog` daemon and are able to send messages through SNMP.

5.4.3.1 Connetivity Adapter logs

Logging have been changed in V7R2. [Figure 27 on Page 28](#) shows the possibilities for V7 R0 and R1. In V7 R2 the content of the former Debug, System and Error ligfiles are included in one file named `logger.x.log`. The trace logs' content didn't change, but due to a logrotation and keeping the last 5 compressed logfiles, its name was changed to `trace.x.log`. The `x` in the logfiles' name refers to this and should be between (including) 0 and 5 where 0 is the actually written file. The other logfiles are stored in compressed format. The GUI of the new logging is shown on [Figure 28 on Page 29](#).

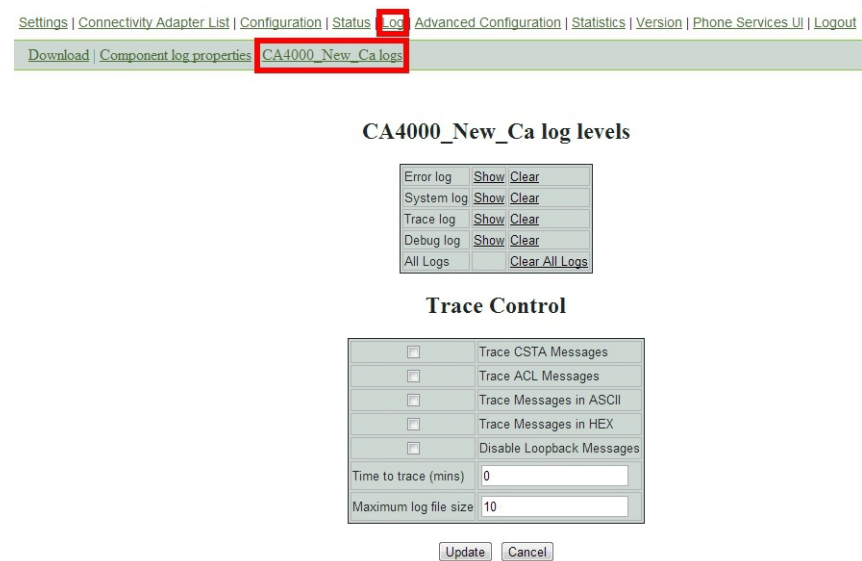


Figure 27

Log - Show/Clear up till version V7 R1

Settings | Connectivity Adapter List | Configuration | Status | **Log** | Advanced Configuration | Statistics | Version | CICA | Phone Services UI | Logout
Download | Component log properties | Cica log properties | **CA4000_New_CA logs**

CA4000_New_CA log levels

Log	Show	Clear
Trace	Show	Clear
All Logs	Clear All Logs	

Trace Control

<input type="checkbox"/>	Trace CSTA Messages
<input type="checkbox"/>	Trace ACL Messages
<input type="checkbox"/>	Trace Messages in ASCII
<input type="checkbox"/>	Trace Messages in HEX
<input type="checkbox"/>	Disable Loopback Messages
Time to trace (mins)	0
Maximum log file size	10
Maximum trace file size	10

Figure 28 Log - Show / Clear in V7 R2

- **Show**

Press **Show** to get an online log file output.

- **Clear**

Press **Clear** to delete the log file contents.

- **Trace Control**

The ACL/CSTA conversation trace can be enabled for a certain time.

Select the messages you would like to be written to the `trace.log`.

Set the time **Time to trace (mins)** till this trace has to be active.

- **Maximum file size**

Sets the maximum file size for the log and trace files in megabytes. By default this is set to 10 MB in V7 R1 and earlier versions, in V7 R2 the logger's default maximum size is 2 MB, the trace's is 10 MB. The available maximal size depends strongly on the number of the used connectivity adapters, the traffic and specific requirements. **Never use maximal size bigger than 20 MB without consulting CSTA GVS or Development!**

- **Update**

Press **Update** to save your trace and log file size settings.

5.4.3.2 Download

The complete configuration of all CA instances and all associated log files can be downloaded via the Admin webpage.

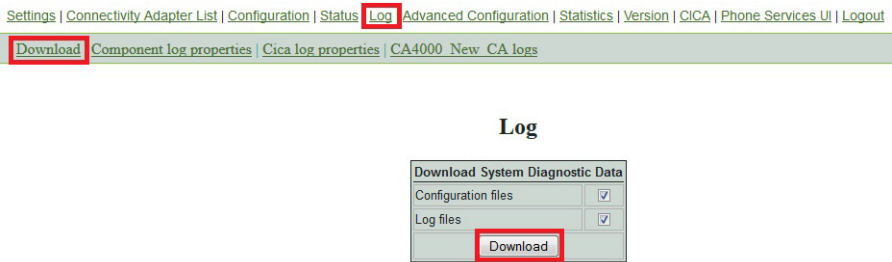


Figure 29 Log - Data download

Make your selection and press **Download** to get the zip file `CiSysdiag.zip`.

5.4.3.3 Component log properties

The log level (**Log level**), number of backup files (**Backup files count**) and log file size (**Max file size**) can be set for the different OpenScape 4000 CSTA system components at the Component log properties. If any component's maximal size or the number of the stored backups need to be changed it is strongly recommended to lessen the space requirements for one or more other components' logs in order to fit into the same final sum.

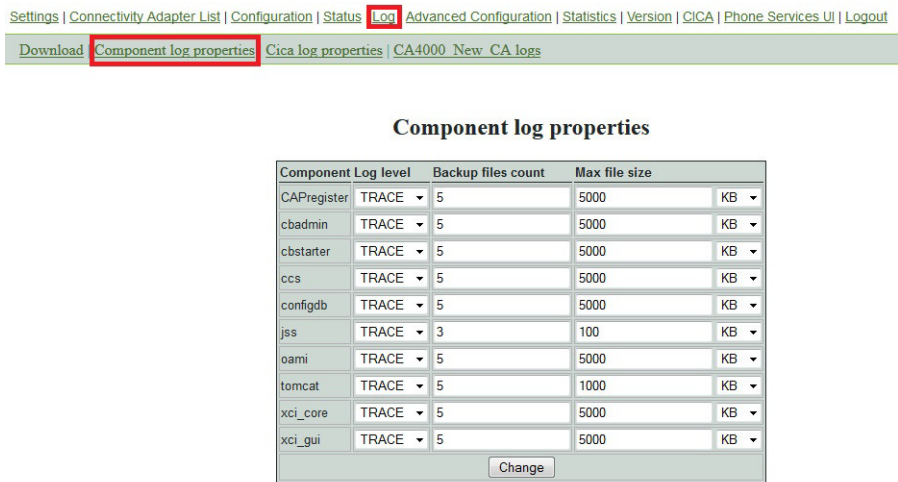


Figure 30 Component log properties

5.4.4 Statistics

Detailed information about ACL/CSTA is shown in **Statistics**.

[Settings](#) | [Connectivity Adapter List](#) | [Configuration](#) | [Status](#) | [Log](#) | [Advanced Configuration](#) | **Statistics** | [Version](#) | [CICA](#) | [Phone Services UI](#) | [Logout](#)

CA4000_New_CA Statistics

[Refresh](#)

[Clear All Stats](#)

Statistics from: Thu Jul 09 11:37:02 CEST 2015
To: Thu Jul 09 13:18:08 CEST 2015

Link Status	
PBX Layer 2 UP	Y
PBX Layer 4 UP	Y
PBX Layer 7 UP	Y
ACL Link Event Stream Up	Y

Connectivity Adapter -- PBX Communication		
	Received	Sent
ACL Msgs	490	411
Avg ACL Msgs/sec	0	0
Peak Avg ACL Msgs/sec	5	0
Peak Avg ACL Msgs/sec at	Thu Jul 09 11:37:07 CEST 2015	Thu Jul 09 11:37:04 CEST 2015

OSI/TCP (Layer4) Statistics		
	Received	Sent
Connection confirmations	1	0
Connection requests	0	1
Disconnection requests	0	0
Data frames	489	411

Figure 31 Statistics

- Link Status**

This section provides information about the status of the various PBX layers.

Definition of the fields:

Field	Explanation
PBX Layer 2 Up	Indicates whether or not the PBX link is up and functioning at the physical level. Possible values are Y or N. N – The PBX link is down. Y – The PBX link is up.
PBX Layer 4 Up	Indicates whether or not the PBX link is up and functioning at the transport level. Possible values are Y or N. N – The PBX link is down. Y – The PBX link is up.
PBX Layer 7 Up	Indicates whether or not the PBX link is up and functioning at the application level. Possible values are Y or N. N – The PBX link is down. Y – The PBX link is up.
ACL Link Event Stream UP	Indicates whether or not the PBX event stream is up. Possible values are Y or N. N – The PBX link is down or the event stream is disabled. Y – The PBX link is up and the event stream is enabled.

Table 2 Statistics - Link Status" section

- Connectivity Adapter – PBX Communication**

This section provides information about the status of the PBX link between the CTI server and the OpenScape 4000

Definition of the fields:

Field	Explanation
ACL Msgs	The total number of ACL messages the OpenScape 4000 CSTA application has received from and sent to the application running on the LAN.
Avg ACL Msgs/sec	The average number of ACL messages per second, that are sent to and received from the OpenScape 4000 CSTA application.
Peak Avg ACL Msgs/sec	The highest number of ACL messages per second, that are sent and received from the OpenScape 4000 CSTA application since the last clearing.
Peak ACL Msgs at	The date and time peak when ACL message traffic occurred.

Table 3 Statistics - "PBX Communication" section

- Application link

For each configured application link, one section is shown. The corresponding section provides statistics relating to the application link and the number of messages sent to and received from the OpenScape 4000 CSTA application. The statistics interval is indicated by the **Statistics from** and **To** date and time.

Definition of the fields:

Field	Explanation
Link Status	Indicates the link status. Possible values are: Disconnected – The CSTA link is down. Active – The CSTA link is up and messages have been transferred within the last 60 seconds . Established – The CSTA link is up but messages haven't been transferred within the last 60 seconds. Missing heartbeat – The CSTA link is up but heartbeats sent from the application are outstanding.
Monitor IDs in use	The number of monitor IDs currently allocated and in use. A monitor ID is a cross-reference identifier that the HiPath 4000 CSTA software assigns to each OpenScape 4000 CSTA application that has requested a Start Monitor. The monitor ID is used to correlate which events are associated with a specific Start Monitor request.
Active CSTA requests	The number of requests from the client application now being processed.

Table 4 Statistics - "Application" section

Field	Explanation
ACSE Enabled	Indicates status of ACSE session: Possible values are Y or N. Y – ACSE session successfully negotiated. N – ACSE session not established.
CSTA Msgs	The total number of application level messages the CA-Driver received from and sent to the OpenScape 4000 CSTA application running on the LAN.
CSTA Rejects	The number of CSTA requests rejected.
Avg CSTA Msgs/sec	The average number of CSTA messages sent per second to, and received from the OpenScape 4000 CSTA application.
Peak Avg CSTA Msgs/sec	The highest number of CSTA messages sent per second and received from the OpenScape 4000 CSTA application since the last clearing.
Peak Avg CSTA Msgs at	The date and time peak when CSTA message traffic occurred.

Table 4 Statistics - “Application” section

- More sections

The **OSI/TCP (Layer4) Statistics**, the **DB Statistics** and the **R.O.S.E.** (Remote Operations Service Element) **Statistics** sections are intended for the use of the engineering personnel.

5.4.5 Phone Service UI

The **Phone Service UI** opens a new window to configure and administer the **Connector** for the OpenScape 4000 Phone Services.

[Settings](#) | [Connectivity Adapter List](#) | [Configuration](#) | [Status](#) | [Log](#) | [Advanced Configuration](#) | [Statistics](#) | [Version](#) | [CICA](#) | **Phone Services UI** | [Logout](#)

CA4000_New_CA Configuration

[advanced](#)

PBX Link Number	9
PBX Sub-App Number	20
Maximum log file size	10

☐ UC functionality
☐ E. 164 number format
☐ Offered to both side
☐ Diverted to both side
☐ ONS monitoring
☐ Map remote feature

[Modify](#)

Figure 32 Phone Services UI

NOTE: This will be explained in Chapter 6, [Section 6.4, “Configuration”](#)

5.4.6 Settings

There are various CBAdmin specific settings that can be modified by customer preference.

5.4.6.1 User/Password

For instance the default user and password can be changed. At the initial installation this is Admin/Admin.

NOTE: As stated previously Single Sign On is used for accessing the CSTA GUI, however if the session expires, then it is possible to access the GUI again by using the above mentioned credentials, however it is **NOT RECOMMENDED**. If this happens we advise to use the SSO from Assisat's page again.



Settings

Change Administrator password	
Actual password	<input type="password"/>
New password	<input type="password"/>
Confirm password	<input type="password"/>

Figure 33 Change default user and password

5.4.6.2 CBAdmin – Trusted IP Addresses

In case OpenScope 4000 CSTA is used with CAP then it is required to configure the trusted IP list on the CBAdmin **Settings** page.

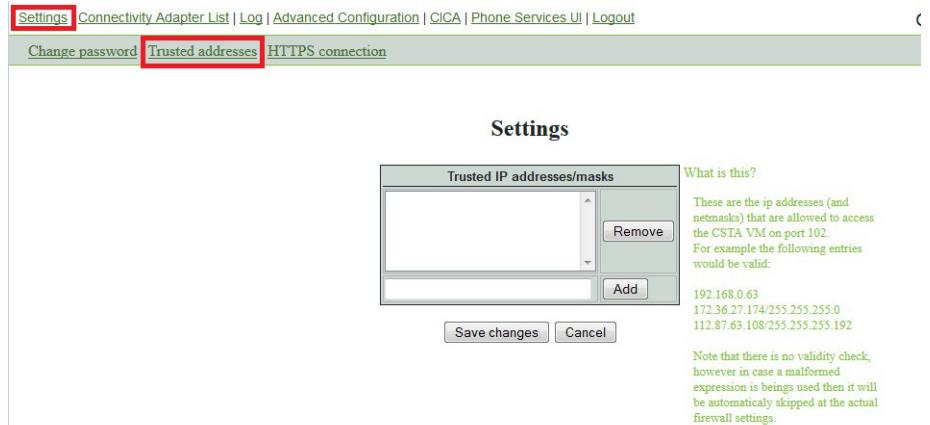


Figure 34 Trusted IP addresses

The IP addresses and/or ranges in this list are able to communicate with the RMX platform through the OpenScape 4000 CSTA VM. Later versions of CAP automatically try to register themselves into this list. But manual supervision is still required in case of malfunction.

The list can be freely modified by adding or removing entries. These modifications will be applied after saving the changes (button **Save changes**).

5.4.6.3 HTTPS Connection

OpenScape 4000 CSTA provides a feature to change the default certificate and private key that is used for communication through the https protocol.

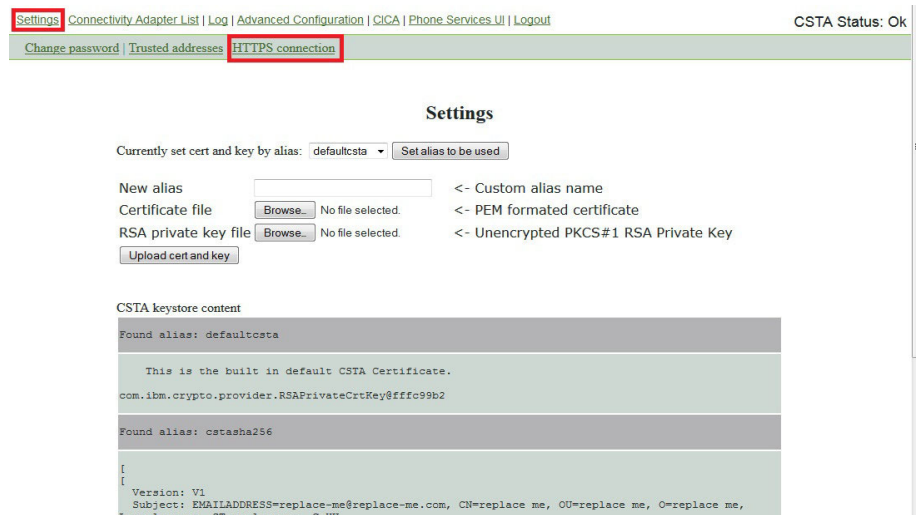


Figure 35 HTTPS Connections

Currently set cert and key by alias

As it says that it is the currently used certification and private key for https connections. To change this simply pick another alias from the drop down list and set it by clicking the button next to it. For the changes to take effect tomcat service must be restarted.

There are two built-in certificates/private keys in OpenScape 4000 CSTA under different aliases namely *defaultcsta* and *cstasha256*.

- defaultcsta

As the name suggests, *defaultcsta* is the default setting on every installation. The certificate and key pair represented by this alias is the same as in the previous versions, so if no change is needed, this default can be used without any compatibility problems.

- cstasha256

The *cstasha256* is a self-signed certificate and key pair, only available for temporary usage. The major difference to the *defaultcsta* is that this certificate only has “replace me” attributes, indicating that it should only be used, if the network’s security settings do not allow the usage of the previous defaultcsta certificate, since the *defaultcsta* certificate is signed by a stronger algorithm. When the *cstasha256* certificate is set, then previous versions of the OpenScape 4000 Phone Services software won’t be able to connect to OpenScape 4000 CSTA.

Upload cert and key

It is generally advised that every customer should use their own custom generated (and signed) certificates with the related private key.

With this in mind, OpenScape 4000 CSTA provides a way to upload these files into OpenScape 4000 CSTA’s own keystore. The certificate must be in PEM format and the RSA private key must be in unencrypted PKCS#1 format for a successful upload!

Both of these files are simple textfiles. PEM format certificates’ file structure should be (the number of chains can vary):

```
-----BEGIN CERTIFICATE-----  
<Primary SSL certificate>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Intermediate certificate>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Root certificate>  
-----END CERTIFICATE-----
```

For the RSA key, the file structure should be like the following:

```
---BEGIN RSA PRIVATE KEY-----  
<Private Key>  
-----END RSA PRIVATE KEY-----
```

After picking a unique alias name, select the corresponding files and click on **Upload**. If the upload was successful then the alias can now be selected from the drop down list **Currently set cert and key by alias** and can be set to use.

OpenScape 4000 CSTA keystore content

This is the full content of OpenScape 4000 CSTA's keystore grouped by aliases. Under every alias, detailed information can be seen relating to the certification and the private key (sensitive informations are blurred out on the screenshot).

IMPORTANT: In case custom certificate is used then it needs to be uploaded on the client machine's default java keystore, otherwise the OpenScape 4000 Phone Service Client Application won't be able to recognize the CSTA server as trusted, so connection won't be possible.

NOTE: In case of OpenScape 4000 V7 integrated OpenScape 4000 CSTA, the CBAAdmin and Phone Services graphical user interface is accessed through the OpenScape 4000 Assistant, therefore its certificate is being used as well. The communication with the OpenScape 4000 Phone Services (prev. XCI Tray) is still done using OpenScape 4000 CSTA's own certificate.

5.4.7 Circuit Interface Connectivity Application

5.4.7.1 General Description

In order to support the Circuit Connectivity in OpenScape 4000 V7 R2 a new layer has been introduced in the CSTA message processing. Circuit Interface Connectivity Application (CICA) runs on the CSTA VM, it connects to a Connectivity Adapter as one single normal CSTA application, it uses ACSE specifying its request for short tag XML (ECMA323 Annex D) and a private data set required for Circuit connections. Connectivity Adapter was enhanced to provide the short tag XML and distinguish the private data for Circuit. CICA serves a maximum 500 connections to virtual softgates (vHG3500) through VPN connection and provides a CSTA interface required by the CSTA over SIP. The

VPN tunneling is provided by the OpenScape 4000 Platform, it is invisible and uncontrollable for both ends of the connection. The general architecture is shown on [Figure 36 on Page 38](#).

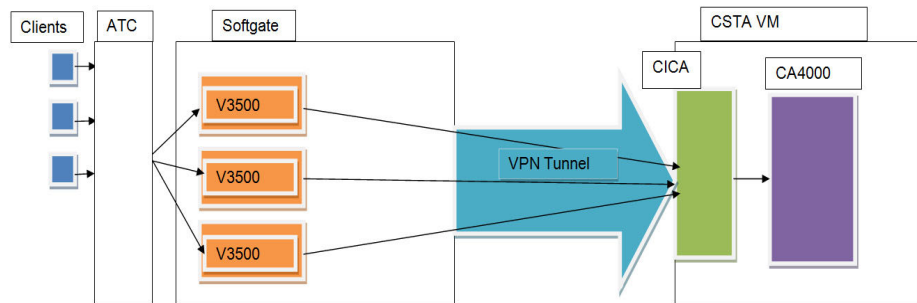


Figure 36 General architecture of the circuit connection

5.4.7.2 Configuration

[Settings](#) | [Connectivity Adapter List](#) | [Log](#) | [Advanced Configuration](#) | **CICA** | [Phone Services UI](#) | [Logout](#)

CICA Configuration

advanced

CA port:	1040
Auto start:	<input type="checkbox"/>

Modify

CICA is not Running

Start Stop

CICA tries by default to connect to Connectivity Adapter on port 1040. It can be modified by adding a port and pressing **Modify**.

Check **Auto start** option if it is required that CICA starts automatically at service start and is controlled and restarted in case of stopping. This is the normal functionality of the application, in case of Circuit connectivity it needs to be set. In order to make your changes valid, press **Modify**.

A status field is also added, it checks the process's status when the page is reloaded. A possibility of manual starting and stopping is added. The process can be stopped even if Auto Start is checked, at this case it will be started automatically at next CSTA service startup.

5.4.8 Advanced Configuration

All of the configurations are stored in OpenScape 4000 CSTA's own database, and a graphical user interface is presented in case any modification is required.

IMPORTANT: This feature is for experienced administrators only!

[Settings](#) | [Connectivity Adapter List](#) | [Log](#) | **Advanced Configuration** | [Phone Services UI](#) | [Logout](#)

Advanced Configuration

Component type: Component:

Name	Value	Delete
ACL_SERVER_IP_ADDR	<input type="text" value="192.0.2.3"/>	<input type="checkbox"/>
GW_LINK_ID	<input type="text" value="100"/>	<input type="checkbox"/>
GW_SUBAPPL_ID	<input type="text" value="50"/>	<input type="checkbox"/>
GW_TRACE_CONTROL	<input type="text" value="0"/>	<input type="checkbox"/>
GW_TRACE_TIME_END	<input type="text" value="0"/>	<input type="checkbox"/>
KEEPALIVE	<input type="text" value="1"/>	<input type="checkbox"/>
KEEPALIVE_PROBES	<input type="text" value="5"/>	<input type="checkbox"/>
KEEPALIVE_TIME	<input type="text" value="120"/>	<input type="checkbox"/>
KEEPALIVE_TRIES	<input type="text" value="5"/>	<input type="checkbox"/>

Figure 37 Advanced Configuration - Component selection

Structure of the page:

Two listboxes are on the top of the page. With these, the user can select the configuration type (**Component type**) and the configuration (**Component**) to be edited. After the selection the page will reload, and it will show only the available configuration parameters and values in a table. The user can modify, delete or add entries.

The user can do more than one modifications at the same time and save them in one step.

Delete, modify or add entries

- Delete

The checkbox in the column **Delete** should be checked. The deletion will be maintained after **Save**.

- Modify

Modify the value in a chosen line. The modification will be maintained after **Save**.

- New setting

Push the button **Add line**, then a new line will appear in the configuration. The user should fill the name and the value. The modification will be maintained after **Save**. If the add line was a mistake, then the user can delete the new line before the save with the **Delete** button in the last column.

Save

After pressing **Save** the values of the configuration parameter are saved/deleted in the configuration database. The processes will "know" about the changes after restarting the adequate Connectivity Adapter in case of Connectivity Adapter configurations or the OpenScape 4000 CSTA service in case of all other configurations.

Export/Import:

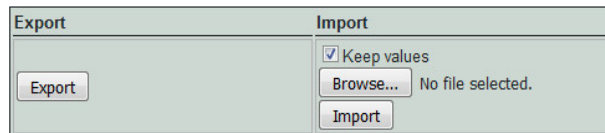


Figure 38 *Advanced Configuration - Export/Import*

There is a possibility to export/import only a part of the configuration or even the whole configuration.

- **Export**

Depending on the chosen configuration type and configuration, clicking the **Export** button will download the configuration (fully or partly) in a zip file. If nothing is selected then the whole configuration will be downloaded. If any of the components or the component types is chosen then the appropriate part will be downloaded.

Structure of the .zip file:

The main directories in the zip file are named after the component types. In these main directories are the files located that correspond to the related component. The files contain key-value pairs.

- **Import**

It is possible to import the above defined zip files. If the checkbox "**Keep values**" is unchecked, then the import process will first clear the old configuration and import the new ones only after that. If the checkbox is checked, the import process will keep the old values, and if it finds any key which is both in the zip file and in the database then it will update the old value.

For the modification to take effect the user needs to restart the OpenScape 4000 CSTA service and the tomcat service. If the config type is **ca4000** it is enough to restart the **Connectivity Adapter**. The application offers the possibility to restart it (or the user can do it later manually).

5.4.9 Additional Supported Services via OpenScope 4000 Assistant

After login on to **OpenScope 4000 Assistant** the following possibilities can be selected to be used in context of CSTA in the menu item **Software Management**:

- Backup & Restore
- Software Activation
- Software Transfer

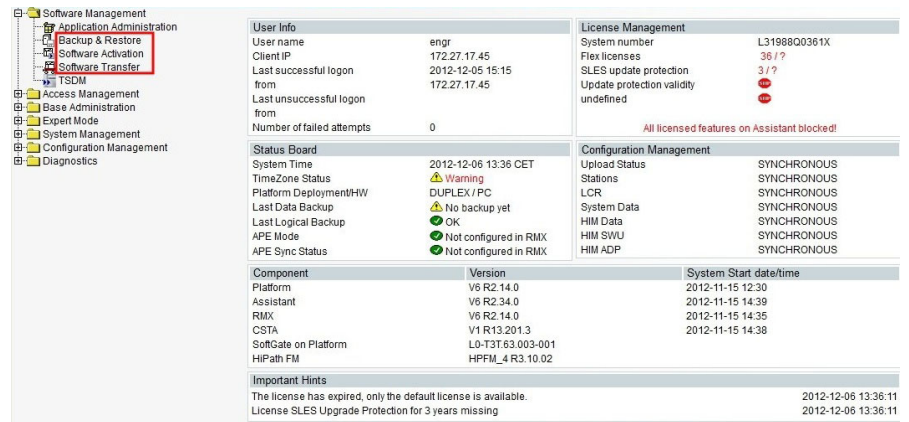


Figure 39 Connection to Backup & Restore, Software Activation/Transfer

Backup & Restore

The configuration parameters related to CSTA can be stored selecting **BEER_CSTA (CSTA configuration)** on the Backup/Restore GUI, menu item Backup, see Figure 40 on Page 41. The selected one of the stored backups can be restored using menu item Restore. Compatibility related topics should be checked in the Release Notes.

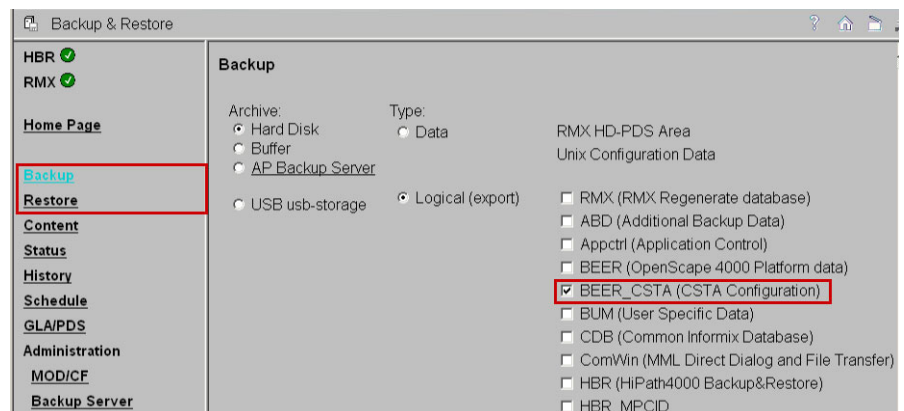


Figure 40 Backup & Restore - BEER_CSTA (configuration)

Software transfer and activation

These possibilities serve to the updating of the CSTA including upgrade and hotfixing. Detailed description can be found in the OpenScape 4000 Assistant's documentation.

There are some application specific settings that can be changed using the possibilities described in [Section 5.4.8, "Advanced Configuration"](#). We summarize these settings here.

5.4.10 Special Settings

5.4.10.1 Concept of "Presentation Indicator for Devices" in CSTA Events

To provide adaptable working cases for every application, Connectivity Adapter will have three different ways to handle the presentation indicator for devices. The different solutions can be activated in the configuration of Connectivity Adapter. The parameter **PRESENTATION_RESTRICTED** should be added and set to one of the following values:

- **normal**: to provide the old concept as it worked in the past. Acts following the settings on a device. This is the default behaviour.
- **ignore**: follow the setting on external dialling numbers but always show internal numbers.
- **private data**: restricted numbers will be sent in private data. In order to get this information about all hidden party types, not just the calling and called devices, the parameter **ALLOW_ALL_PRIVATE_DATA** must be added and set to **true**.
- **special**: similar to the function of **normal** but instead provides possibility for the OpenScape ProCenter (and OpenScape Contact Center - special customer change request for Bundestag) to replace the "not known" with the given <special value>
PRESENTATION_RESTRICTED=special +
PRESENTATION_RESTRICTED_SPECIAL_VALUE=<special value>

NOTE: The application offers the choice when to switch-over to one of the **private data**. By default, the parameter **PRESENTATION_RESTRICTED** and **ALLOW_ALL_PRIVATE_DATA** are not included in the Connectivity Adapter configuration.

5.4.10.2 Delayed CSTA Response Features

CSTA Deflect Call Request is used to divert a call from a ringing device to another destination that may be inside or outside the switching sub-domain. If the destination device is external and a trunk could be seized, the request is always positively acknowledged by ACL and the application is not informed about any failure of the diversion.

There are options in OpenScape 4000 CSTA to configure it in a way that the positive response provided to report the successful seizure of the trunk is not sent to the application right away. Instead the CSTA response is based on the state event reporting the availability of the destination. Positive response is sent with the adequate state event if the destination is reachable or a relevant CSTA error is sent if not. These settings are the following:

- **CSTA3_DELAY_DEFLECT_CALL_RESP**

In order to get this behaviour for a deflect from an RCG and the target is the calling party the parameter must be set to **1**.
The option can be used from HiPath 4000 V5.

- **CSTA3_DELAY_DEVICE_DEFLECT_CALL_RESP**

Set this parameter to **1** if this behaviour is required for calls deflected from a digital or analog subscriber, trunks, and hunt group devices and the target party is the called party.
The option can be used from HiPath 4000 V6 R1 or higher.

CSTA Single Step Transfer Call Request is used by an application to transfer a party in an existing call to a new device. If the destination device is external and a trunk could be seized, the request was always positively acknowledged by ACL and the application is not informed about any failure of the transfer.

- **CSTA3_DELAY_SST_CALL_RESP**

must be set to **1** to get this behaviour. This option can be used from HiPath 4000 V6 R1 or higher.

To activate these configuration changes the restart of the corresponding Connectivity Adapter is necessary.

5.4.10.3 Support of the Offered mode of the Alerting state

The CSTA / ACL-C interface has been enhanced to support the Offered mode of the Alerting State as described in Standard ECMA-269. In Offered mode the handling of an incoming call is offered to a monitoring application before the call starts to ring on the device. It is supported on digital phones (i.e. HFA clients and digital TDM clients). Applications supporting the offer can either

- accept the call using Accept Call Service implemented in V6 R1

- deflect the call in the classical way but before it starts to ring on the originally dialled destination
- reject the call

To get CSTA Offered Event indicating the offer described above for all the devices monitored by any applications connected to this CA, the following AMO command must be executed to that ACL linkpair, used by the Connectivity Adapter, to which the monitoring CTI application is connected:

```
CHANGE-XAPPL:CTYPE=SUBAPPL,APPLNO=xx,SUBAPPL=yy,ADDEVT=ALL;  
CHANGE-XAPPL:CTYPE=SUBAPPL,APPLNO=xx,SUBAPPL=yy,ADDEVT=CALLOFM;
```

NOTE: **CALLOFM** is not part of **ALL** events.

Starting V6 R2 the offered mode can be changed also on the Connectivity Adapter's configuration page on the CSTA GUI, see [Figure 41 on Page 44](#) and

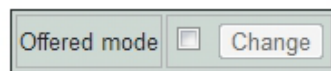


Figure 41 *Change the Offered Mode*

also [Figure 19 on Page 23](#). The **CALLOFM** in AMO-XAPPL can be added or deleted with it. The checkbox reflects the actual state checked and updated when the Connectivity Adapter window is loaded. Pressing **Change** is possible only when the checkbox's state is different from the result of the result of DISPLAY-XAPPL AMO command re-checked before modification. If the state of the Offered mode is not known, an info about it is shown under the checkbox. See an example for it on [Figure 22 on Page 25](#).

Offered mode can be activated or deactivated on a per Connectivity Adapter basis. The incoming calls will be offered to all monitoring applications having a monitor point at the called party by a CSTA Offered Event. If none of these applications accepts the offer (i.e. accepts, deflects or rejects the call by CSTA service) the call returns under the control of the switching function after a 2 seconds timeout and the device starts to ring.

5.4.10.4 Delivering deviceIDs in E.164 Format (SFR international)

This feature was introduced in HiPath 4000 V6 R2. The logic of the generation of the E.164 numbers is implemented in ACL. HiPath 4000 CSTA gets the information from the switching function in the ACL messages (see the ACL descriptions for details).

Sending out numbers in E.164 format can be switched on at the checkbox appearing on corresponding Connectivity Adapter's global settings (see e.g. [Figure 19 on Page 23](#)) or using the CA's Advanced Configuration page (see

Figure 37 on Page 39), adding the parameter **E164_NUMBER_FORMAT** and setting it to **1**. This configuration parameter is valid for a Connectivity Adapter, so if it is switched on, all the applications connected to it will have the numbers in E.164 format. If the feature is switched on, Monitor Start Request must contain the E.164 number. Monitor start requests with numbers in other format are rejected on HP4K CSTA level. This is true vice-versa: if the feature is switched off, the Monitor Start Request containing a dialling number beginning with '+' is rejected.

Other service requests are let through HP4K CSTA with either extension or E.164 number. ACL is able to determine the extension from it. CSTA responses contain the E.164 format if the request was sent with that format and the E.164 number is available in the ACL response.

E.164 number format is provided in every monitor events' DeviceID field that normally contains a dialed number.

Restrictions

- During a normal call setup the called party in the ORIGINATED event is not in E.164 format. At that state the party belonging to the dialed number can be anywhere, there is no information about the "rest" of the E.164 number so the called party will contain only the numbers dialed.
- The E.164 format will not appear in the dialing sequence if other sequence is dialed.

5.4.10.5 Enhancements for supporting OpenScape UC

The base of these enhancements was to provide an application controlled one number service (ONS) feature with preconfigured or dynamically handled preferred devices (ONDs)

Connectivity Adapter has to distinguish between "UC-like" and "not UC-like" applications. This property is configurable on a per Connectivity Adapter basis, so all applications connected to a Connectivity Adapter must await and accept the same monitoring style. Independent configuration parameters are available for the independent parts of the feature. "UC-like" application means that the above mentioned five CSTA configuration parameters are all set.

OS4K CSTA GUI has been modified in order to make it easier to reach the relevant configuration. A check box appears on the Connectivity Adapter's main configuration page where all "UC relevant" config parameters can be switched on/off "at one click" in the checkbox of "UC Functionality". The configuration parameters can also be changed one by one, either on this panel (see the figures below) or on the Advanced Configuration page of the Connectivity Adapter.

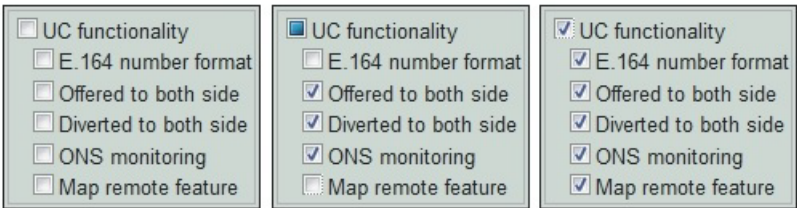


Figure 42 UC functionality on the GUI

OFFERED and DIVERTED events for the calling side

OpenScope 4000 has a device based monitoring This is communicated between the application and the switch using the capabilities exchange services when the connection has been built up. That information exchange is not modified as the global behaviour did not change with these user-specific monitoring changes.

Device base monitoring allows the system to provide DIVERTED event only to the diverting party. An additional event flow was implemented for OpenCsape UC in order to provide these events also on the calling side.The changes in the CSTA monitoring to provide the paired events are based on an unchanged ACL event flow.

IMPORTANT:

Restriction: The **Offered event** is generated in ACL only on the offered party (B) side. The CSTA Offered event can be generated to either A or B side when the party B is monitored. It can be considered in the Connectivity Adapter if A side is also monitored and the adequate offered event must be sent ALSO to party A. However, if B is not monitored neither ACL Offered nor CSTA offered event is provided.

IMPORTANT:

Restriction: in case of a multiple hop forward: CFNR+CFU if the hops are monitored, a **Divderted event** will be sent to each of them but only one Diverted will be sent to party A.

DIVERTED event to the calling party is mapped based on the state changes of the calling party itself. Special handling of the CallRedirectedEvent has been implemented to check if both A and B sides are monitored and map it to a DIVERTED also to A side. The implementation here is free from the restriction mentioned at the Offered event as in this case the CallRedirected Event has no event originator at all.

ONS based monitoring using the binding information

Connectivity Adapter awaits the binding information in the requests in the same format as in the DeviceList's Device Identifiers, and sends it out in the same way, i.e.

N<+15615551000>;ond=+15615551040

Requests:

If OND number is present in the request and ONS_MONITORING is on, Connectivity Adapter maps it to UsedDevice. The ONS number will always be mapped to a convenient element of ACL request's Cntl*Set, as it is a mandatory parameter. No checks of configuration. If the request contains binding, Connectivity Adapter maps it to ACL and fills the Used Device. If it is a version which does not accept it, ACL rejects the request.

Events, responses:

Connectivity Adapter maps the ONS and OND numbers from the following ACL IE-s: E.164 number and one of UsedDevice and UserExtension if ONS_MONITORING is on. If there is an inconsistency in the presence of the numbers (e.g. usedDevice is present but E.164 number not) the Connectivity Adapter maps the event in the old way (i.e. E.164 format is mapped if present and switched on). Mapping of the events where the originator is trunk remains unchanged.

Dynamic device list in the Accept Call request

OpenScape UC Application can send the list of preferred devices (OND-s) in the Accept Call request using a private element.

Interface to ACL has been enhanced with the following IE-s based on the ACL IS:

- ParRingGroup — list of devices alerting parallel
- RnaSeconds — ring no answer timer
- AlertingPattern — must contain the OND number, can contain the ring no answer timer and the parallel ringing group
- ListOfDevices — contains one or more alerting patterns
- CntlDestSet contains also the UsedDevice

ContinueCallRequest has been enhanced with the new optional field ListOfDevices

A list element containing binding information in the CSTA Accept Call Request's private data looks like

N<+15615551000>;ond=+15615551040;rna=20;grp=1

A list element can be sent also without binding:

<+15615551000>

ONS number supposed to be the accepting device. No checks are done on Connectivity Adapter level if it is valid. OND number if present, is mapped to the UsedDevice number (new) in the CntlDestSet of the actual element of ListOfDevices. If the list element contains no binding information, the number in it will be mapped to the UnknownAddress of the CntlDestSet. The value of the “r n a” will be mapped to the RnaSeconds and grp to the ParRingGroup.

Remote features

ACL Call Information event can optionally contain the new RemoteFeature IE. This indicates the change on the remote side that causes the change in the call linkage data. Connectivity Adapter will map the Call Information Event containing this Remote feature information element as if it had been a state transition event.

The following scenarios can be reported:

- Transfer (talking and ringing) on the remote switch
- Hold / Retrieve of the call on the remote switch
- Pick up on the remote switch
- Recall on the remote switch
- Call forwarding on the remote switch

Conference: As there is no possibility to get the remote conference list through the network interface, the remote conference will not be mapped from the Call Information Event.

Single Step Transfer for the consulting party

OpenScape 4000 supports the Single Step Transfer Call request to a party having an active and a held call for both calls.

Seamless Handover by Single Step Transfer

“Single step transfer” feature has been enhanced to provide a real Seamless Handover option where the conversation between the transferred party and the transferring ONS subscriber is maintained without interruption. This covers the enhancements to support the new Seamless Handover option for scenarios where the ONS subscriber is in “talk” state. CSTA interface is enhanced with new private elements in Single Step Transfer call service and in the monitor events in order to provide the requested information. Detailed CSTA flows are in the OpenScape 4000 CSTA Application Developer’s Guide.

Deflect of the second call

If second call waiting is activated on a subscriber and a second call is actually alerting on it, the state of that call in the OpenScape 4000 is Queued. The Deflect service is allowed for this special case of the Queued state. No new configuration: deflect is allowed from V7.0 for these cases.

Support the early release mechanism for Deflect, Call Forward No Answer and Single Step Transfer scenarios

OpenScape 4000 was enhanced to model early release for the UC application. Connectivity Adapter was changed to follow the new event flow and provide the CSTA event flow requested by UC.

Offered mode for Hunt Group members and ACD Agents

The Offered mode was enhanced to provide the offering mechanism also to these devices. The mapping of the Offered event was enhanced to handle the changed information. There is no special configuration for it.

Special CSTA flow for the Hunt Group calls

A call to a hunt group is modelled for the UC application on a way that a connection among the members should be reported. This connection will be sent using a new private element in the Connection Cleared event in case of Hunt Advance showing the next alerting HG member before the call is actually alerting on it. This model has no separate configuration possibility, "UC-like" monitors will have this event flow.

5.4.10.6 Special Settings to Application Connection

In case of a network problem (e.g. cable pulled out or network disabled, then the connection enabled again) there will be problems for the CTI application to build up the connection to the OpenScape 4000 CSTA again, since the corresponding application port of the OpenScape 4000 CSTA remains busy for a longer time.

A special settings has been introduced to overcome this difficulty, named **socket keepalive**.

Socket keepalive can be configured, to send "keepalive" (~0) messages to check for socket connection. If keepalive check fails, then the socket is closed.

Now keepalive is modified for sockets (both way: pbx and cti application), which can be configured in Connectivity Adapter configuration.

If not configured in Connectivity Adapter, then the default values are used:

- **keepalive: 1**
 - 1 - active
 - 0 - not active (makes no sense)
- **keepalive_time: 120 (sec)**
 - If nothing happened on socket then keepalive will be activated after this period of time.
- **keepalive_tries: 5**

Description: Before closing the socket, the application sends keepalive messages as many times as set here. If there is still no response after the last try then the socket will be closed.

IMPORTANT: Supported only on Linux, default values on Windows:
before Vista: 5,
Vista and after: 10.

- **keepalive_interval: 5 (sec)**

Time between tries of sending keep alive messages.

5.4.10.7 Special setting to deliver physical answering device information via OpenScape 4000 CSTA

Multiline appearance (keyset) monitoring is not supported in OpenScape 4000 CSTA V7.

There are some special changes introduced in order to make the recording of an incoming call possible also in the below described special case.

When a call arrives to a keyset device, which is monitored and the call is answered by its secondary line, the middleware delivered no information in the Established Event about the real answering device (secondary line), only the keyset number. Solution is implemented for this special case:

Physical device ID is sent out in the private data field of the CSTA_ESTABLISHED_EVENT. New private element named physicalAnsweringDeviceID is introduced, including the physical device number, which actually answers the call.

Additionally the CSTA_RETRIEVED_EVENT is also enhanced for that situation, when as a further action the secondary line holds the call then calls another device then ends that call, and then retrieves the held call. For the ASC, this physical device (secondary line) is delivered in the private data field of the CSTA Retrieved Event as physicalAnsweringDeviceID again.

This workaround solution can be activated with the following Connectivity Adapter entry:

ALLOW_PHYSICAL_APPEARANCE = 1

This feature is inactive by default.

5.4.10.8 Umlaut Characters

The CSTA ASN.1 does not support umlaut characters. Connectivity Adapter by default does not change the hexa values of the characters since they are usually from the basic ascii character set. If a name with umlauts is configured via AMO PERSI and OpenScape 4000 CSTA, ASN.1 interface is used, you must use a configuration parameter in Connectivity Adapter configuration (**Advanced Configuration**, see [Section 5.4.8, “Advanced Configuration”](#)) to "de-umlaut" them. This activates a conversion from CORNET TS characters to latin ascii.

USE_ACCENTED_CHARACTERS=0

With this config OoAaUu is should be shown instead of the accented version (ÖöÄäÜü).

From V7 R2 the special characters supported in CorNet-TS used for AMO-PERSI NAME are supported on CSTA XML and appear in UTF8 encoding. This case the mentioned config parameter mustn't be set or must be changed to 1.

5.4.10.9 Hunt Group Behavior

Hunt group behavior has been enhanced; now it is possible to set up parallel ringing for the devices.

For Example:

```
ADD-SA:TYPE=VCE,CD=3256,ITR=0,STNO=3258,STYPE=PRL,NAME="
",VARCQ=Y,BUSYCOND=ALL,FOLFWBSY=Y;
```

Also keep in mind that monitoring follows the above mentioned functionality. See ADG for further details.

5.4.10.10 UserToUser Info

The geographical location of the caller can be of great importance especially in case of emergency calls. The information (if available) is provided in a new private element. The element will occur in the first CSTA monitor event sent for the connection. It can be:

CALL_FAILED
CALL_FORWARDED
CALL_GROUP-QUEUED
CALL_OFFERED
CALL_QUEUED
HOLDING_STATE
ORIGINATED_STATE

RING_STATE

ROUTE_TABLE_SELECTED

Make call request will also support the private element.

5.4.10.11 Usage with OpenSape Contact Center (OSCC)

In case OpenScape 4000 CSTA is used with OSCC then the following parameters need to be set for the specific connectivity adapter:

```
ALLOW_RELATEDCLD=1  
CALLID_MAX_AGE=14400
```

5.5 Fault management

Starting V7 R2 OpenScape 4000 CSTA was enhanced to support and use the system's SNMP services. An SNMP syslogagent is installed on the CSTA VM. The logging of the CSTA processes was enhanced to use the syslog-ng when an SNMP trap generation is needed. SNMP daemon runs on the host. Traps about defects on the CSTA VM are generated from events that are not requested by GUI, i.e. probably not the effects of human interaction. This includes starting or stopping processes relevant for basic functionality (connectivity adapters and CICA), loss of monitor messages, loss of internal connections. See also the system's descriptions for more information.

6 Phone Services – Introduction

OpenScape 4000 CSTA V7 offers a number of small, user-friendly applications that are integrated and *free of charge*:

- EasySee
- EasyMail
- EasyLookup
- EasyShare (WebCollaboration integrated)
- EasyUC

OpenScape 4000 Phone Services is a package of XML Phone Services applications provided together with OpenScape 4000 CSTA and therefore also with OpenScape 4000 V7. It is aimed at optiPoint and OpenStage display phones' users, optiClient and CMI/Cordless phones' users and offers a set of innovative features to enhance productivity at the workplace.

6.1 Overview

6.1.1 EasyLookup

EasyLookup can be launched on the phone via a configured I/O button only. Searching multiple LDAP servers (using the same access parameters) can be performed irrespective of the current call state, i.e. the search function may also be used when no call is active.

Examples of use:

- Based on a name, you can get the contact details of a party to be called (as provided by the corporate LDAP directory)
- Based on the phone number of an active call, you can get the name and contact details of your partner (as provided by the corporate LDAP directory)
- Based on a phone number or name, you can search for colleagues in the same room as the person or for alternative numbers of that person
- Based on a phone number or name, you can get the e-mail address of that person



Figure 43

EasyLookup - Call the menu by pressing the application button on the device

- Call the menu by pressing the application button on the device.
- Select the desired function via the arrow buttons on the device.
- Enter the search parameters using the numeric keypad.
- Confirm your input and view the search results.
- View further information by pressing the arrow buttons.
- To dial the searched number during “idle” state, position to the requested result and you can either
 - press **OK** key (as illustrated)
 - lift the handset
 - or press the Speaker button

EasyLookUp for Consultation

It is possible to place an active call on hold, find a new user with EasyLookup feature and initiate a Consultation call to this user.

EasyLookUp searches multiple corporate directories

The Phone Services allow the usage of more than one directory services that are based on the LDAP protocol. The configuration possibilities include querying both at the same time and merging the results as one, or creating different user groups for different directory services.

6.1.2 EasySee

On a call, caller data for all connected parties is retrieved from an LDAP server and presented as a **vCard** in the PC's Web browser (if information about the caller is available!).

EasySee can be started on the phone via a configured I/O button and runs on the associated PC.

Example of use:

- Identification of unknown called / calling parties

NOTE: **EasySee** requires a locally installed program **OpenScape 4000 Phone Services Client Application (prev. XCI Tray)**. The **EasySee** function can also be invoked from the OpenScape 4000 Phone Services (prev. XCI Tray) context menu.

Remark: if the default browser is Firefox and a remote connection also uses this, then the EasySee will not pop-up the information in a new Firefox in the user's session.



Figure 44 EasySee

- Call the **EasySee** function by pressing the application button on the device.
- Display the results as a PhoneCard on the PC.

6.1.3 EasyMail

On a call, caller data are retrieved from an LDAP server and used to prepare a new e-mail on the PC to all parties involved in the call or conference.

EasyMail can be started on the phone via a configured I/O button and runs on the associated PC.

Example of use:

- Send mail “Please confirm the agreed course of action by e-mail!”
- Send mail “Please send us the slide set you are talking about!!”

NOTE: **EasyMail** requires a locally installed program **OpenScape 4000 Phone Services Client Application (prev. XCI Tray)**. The EasyMail function can also be invoked from the OpenScape 4000 Phone Services (prev. XCI Tray) context menu.



Figure 45 EasyMail

- Call the EasyMail function by pressing the application button on the device.
- Open an e-mail window on the PC with the e-mail addresses of all conversation partners.

6.1.4 EasyShare

On a call, caller data is retrieved from the UC server and used to start an e-mail with a FastViewer[®] (WebCollaboration) session invitation and with the FastViewer Client also started.

WebCollaboration integration requires that the FastViewer server be set appropriately on the XCI graphical user interface (information on the PhoneServices configuration is provided later on).

NOTE: WebCollaboration integration - EasyShare of Phone Services requires a locally installed program **OpenScape 4000 Phone Services Client Application (prev. XCI Tray)**.

(No FastViewer client installation is required, the OpenScape 4000 Phone Services (prev. XCI Tray) already includes FastCOM.)



Figure 46 WebCollaboration integration

- Call the WebCollaboration integration function by pressing the application button on the device.
- FastViewer client is started and invitation e-mail is created.

6.1.5 EasyUC

Simple access is possible from the phone menu to the UC server to control some of the UC functions.

The UC user account must be entered the first time the UC menu is used on the physical device. However, the account can also be entered in the OpenScape 4000 Phone Services (prev. XCI Tray) graphical user interface (to avoid mistyping problems with the phone keypad).

Examples of use:

- Change the preferred device of the UC user **UC Device**

Phone Services – Introduction

Overview

- Change the availability of the user **UC Status**
- Search in the UC database or in the user's UC contact list (UC Lookup)

NOTE: In the case of the connected call status, the contact data are shown based on the phone number of the active call. If OpenScope 4000 Phone Services Client Application (prev. XCI Tray) is also used, an e-mail is generated by selecting the e-mail address of the contact, as with EasyMail.



Figure 47 EasyUC

Example:

Calling the UC Status function sets the availability to unavailable. This is also shown on the user's Web graphical user interface (from any browser).

6.2 Structure

Overview – Single connected OpenScape 4000 CSTA in case of OpenScape 4000 V7

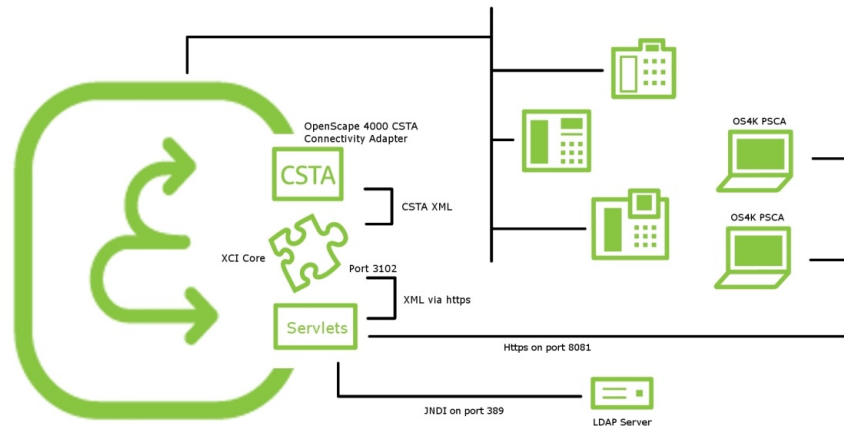


Figure 48

Single connected OpenScape 4000 CSTA (OpenScape 4000 V7)

Administration URLs – in case of OpenScape 4000 V7 integrated variant

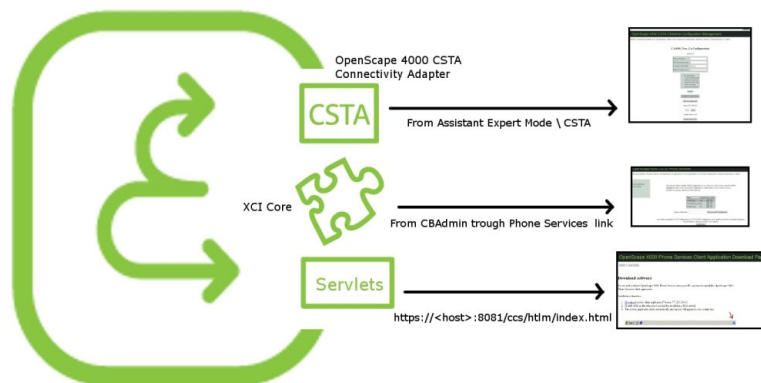


Figure 49

Administration URLs – in case of OpenScape 4000 V7 integrated variant

- **OpenScape 4000 CSTA:** From OpenScape 4000 Assistant > ExpertMode/ CSTA
- **XCI core:** From CBAAdmin with Phone Services UI link
- **OpenScape 4000 Phone Services:** `https://<CLAN IP of CSTA VM>:8081/ccs/html/index.html`

Phone Service URLs

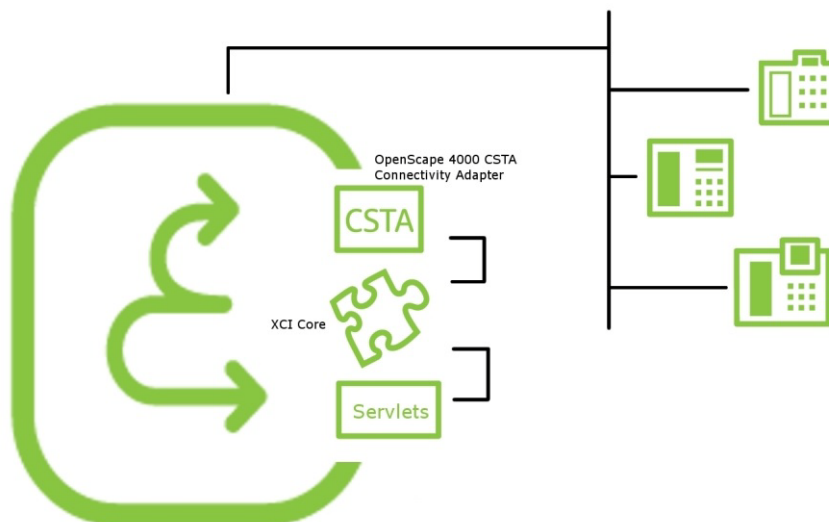


Figure 50 Phone Service URLs

- **AllAppsMenu:** <https://<CLAN IP of CSTA VM>:8081/ccs/menu>
- **EasySee:** <https://<CLAN IP of CSTA VM>:8081/ccs/pc?PHONE=%phone%>
- **EasyMail:** <https://<CLAN IP of CSTA VM>:8081/ccs/mailme?PHONE=%phone%>
- **EasyLookup:** <https://<CLAN IP of CSTA VM>:8081/ccs/ccs?PHONE=%phone%>
- **EasyShare:** <https://<CLAN IP of CSTA VM>:8081/ccs/WCServlet?PHONE=%phone%>
- **EasyUC:** <http<s>://<CLAN IP of CSTA VM>:8081/ccs/UCMenu?PHONE=%phone%>

It is important in this case that the CTI application must send an IORegister with only its own applicationID and not with all applicationIDs to the Connectivity Adapter!

6.4 Configuration

6.4.1 Configuration Steps

- Complete the OpenScape 4000 ACL-C AMO configuration and assign the phone's I/O service function button via AMO-ZIEL (and if that is needed then with AMO-TAPRO). Don't forget to change the **REPDIAL pause timer**.
- Add an XMLPS service in **XCI_GUI** (including **domain** information). Add devices, set user passwords and assign keys for OpenScape 4000 Phone Services Application URLs.
- Set up the CCS and LDAP configurations.

6.4.2 AMO Configuration OpenScape 4000 V7

Repdial pause timer

```
CHANGE-CTIME: TYPESWU=CP2, REPAUSE=1;
```

Key layout change if that is not default:

```
CHANGE-TAPRO: STNO=<stno>, DIGTYP=<digtyp>, KY<xx>=NAME;
```

For digital phones

```
ADD-
```

```
ZIEL: TYP=NAME, SRCNO=<stno>KYNO=<xx>, DESTNON=C13999<xx>, DEV=<device>, [PROTECT=YES];
```

For cordless phones/CMI key 9 only:

ADD-
ZIEL:TYP=NAME, SRCNO=<stno>, KYNO=09, DESTNON=C15C1399909, DEV=<device>, [PROTECT=YES];

NOTE: In case of keymodule the led-id starts from 21 - so please take care to configure it accordingly on XCI and in the AMOs as well.

NOTE: CMI specialities: please observe the DeviceType on the Phone Services UI > Devices. It must be **CMI**. Also note that the application can be reached through the **DTB** button.

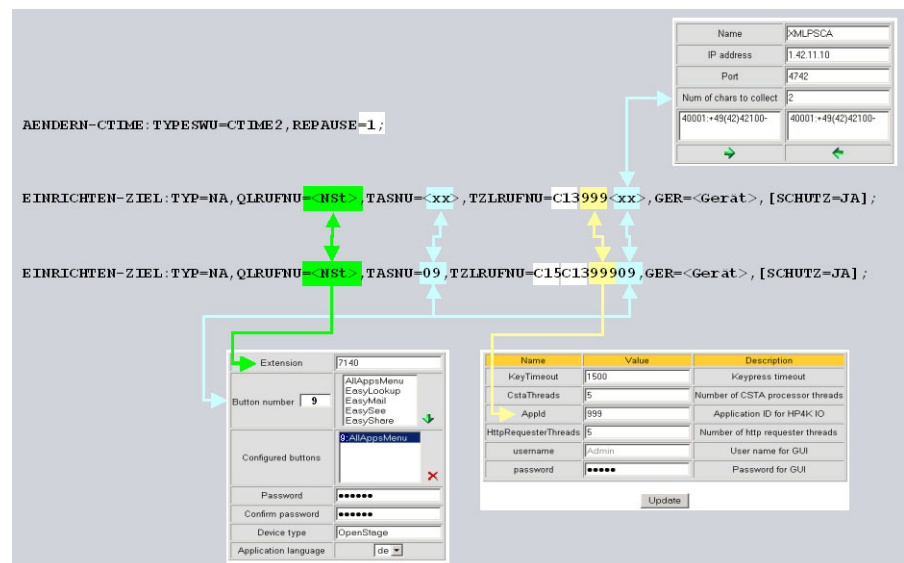


Figure 52 AMO Configuration

6.4.3 OpenScape 4000 CSTA

- As described in the previous sections, a **Connectivity Adapter instance** is up and running.
- The ACL link to OpenScape 4000 has to be established.
- A CSTA link has been configured and is to listen on one connection port.

Phone Services – Introduction
Configuration

Settings | Connectivity Adapter List | **Configuration** | Status | Log | Advanced Configuration | Statistics | Version | CICA | Phone Services UI | Log

Application

Application name	New_App
TCP Port (1025-30000)	1041
Automatic Global Routing Trigger	NO
Monitor Filter	CSTA Standard
Private Data Version Number	4.1.0
Use External DNIS	No
Add application Cancel	

Figure 53 Application

Available from CBAAdmin with Phone Services UI link without authentication window (with SSO).

Enter the XMLPS administration graphical user interface URL in a browser window and log in.

XMLPS for OpenScape4000 CSTA

Login:

Password:

Login

Figure 54 Login

[Settings](#) | [Connectivity Adapter List](#) | [Configuration](#) | [Status](#) | [Log](#) | [Advanced Configuration](#) | [Statistics](#) | [Version](#) | [CICA](#) | **Phone Services UI** | [Logout](#)

CA4000_New_CA Configuration

advanced

PBX Link Number	9
PBX Sub-App Number	20
Maximum log file size	10

☐ UC functionality

☐ E.164 number format

☐ Offered to both side

☐ Diverted to both side

☐ ONS monitoring

☐ Map remote feature

Modify

Offered mode

☐

Change

Configured applications

Add new application

Status: RUNNING

Start Stop

Update Device List

Figure 55 Phone Services UI

First switch to the **Domain** configuration Web page and **Add** at least 1 **domain**. Multiple domains are supported for one PBX.

[Connectivity Adapter](#) | **Domain** | [Device](#) | [XMLApplication](#) | [Configuration](#) | [CCS Configuration](#) | [CCS LDAP Configuration](#) | [Manage Suspensions](#) | [Logout](#)

Show

Add

List of domains

Name	Country code	Area code	Main number	Virtual node code
------	--------------	-----------	-------------	-------------------

Figure 56 Domain - Add

This configuration is required whenever an LDAP server address book call number is used for destination dialing, to convert canonical numbers into a dialing format.

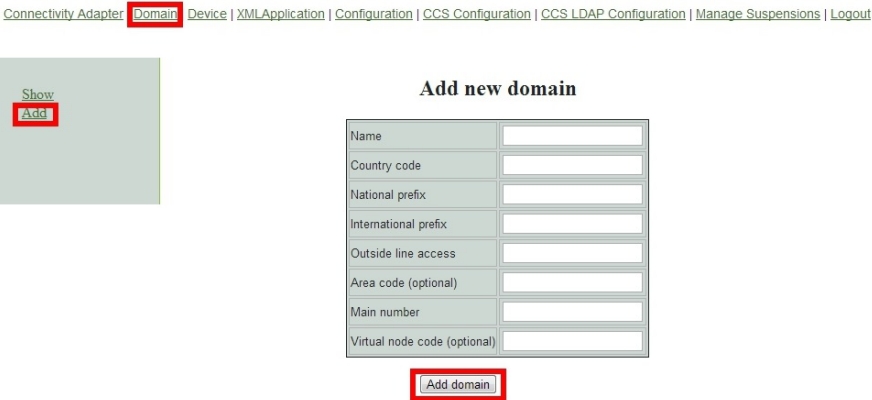


Figure 57 Add new domain

The domain configuration is required whenever EasyLookup uses the LDAP address book to dial a number. Dialing numbers must be converted from a canonical format into a dialing format.

Enter at least the mandatory values and press **Add domain**.

Switch to the **Connectivity Adapter** configuration Web page.

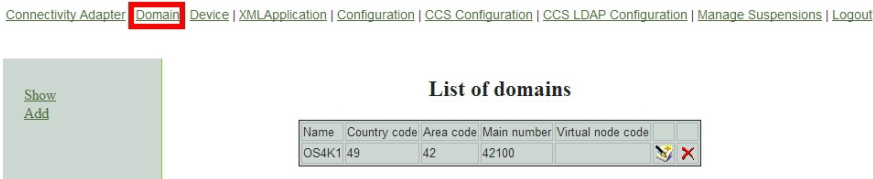


Figure 58 List of domains

Add a Connectivity Adapter, i.e. the connection parameters from the XMLPS to the CSTA link. This is the configuration of an **XMLPS**.



Figure 59 List of Connectivity Adapters

This process converts CSTA messages into **XML over http** or vice versa. A Multiple Connectivity Adapter (multiple OpenScape 4000 Vx) can be connected.



Figure 60 XMLPS

Enter a process **Name**, the CA **IP address** and the CA application **Port**.

The **Num of chars to collect** parameter must match the AMO-ZIEL configuration (C13999xx).

Press the ➡ button to assign at least one previously configured **Domain**.

The screenshot shows a web interface with a breadcrumb trail: **Connectivity Adapter** | Domain | Device | XMLApplication | Configuration | CCS Configuration | CCS LDAP Configuration | Manage Suspensions | Logout. The 'Connectivity Adapter' tab is active. On the left, there is a 'Show' button and a red 'Add' button. The main area is titled 'Add new Connectivity Adapter' and contains a form with the following fields: 'Name', 'IP address', 'Port', and 'Num of chars to collect' (which has a dropdown menu showing 'OS4K1-49(42)2100-'). At the bottom of the form is a red button with a right-pointing arrow and a green button with a left-pointing arrow. Below the form is a button labeled 'Add Connectivity Adapter'.

Figure 61 Add ConnectivityAdapter



Figure 62 XMLPS - Add new domain

Press **Add ConnectivityAdapter** to save this configuration.

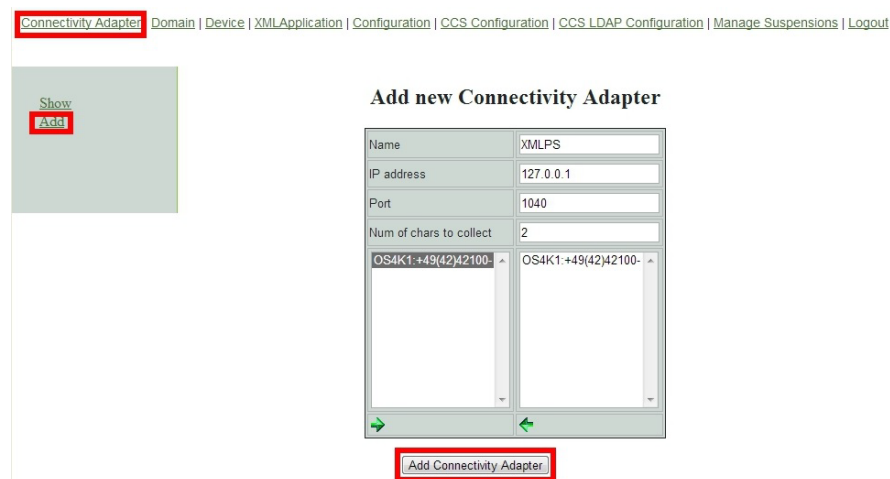


Figure 63 Add new Connectivity Adapter

Switch to the **Device** configuration Web page to add phones, assign users and passwords and define the key assigned application URLs.

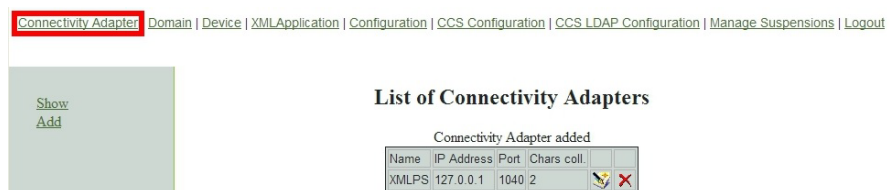


Figure 64 Device

Select the **Connectivity Adapter**, pick a **Domain** and enter the **Extension** number.

The **Button number** has to have the **AMO-ZIEL** configuration on this phone.

Assign one configuration to that button. When a user presses this button, the assigned application (URL) will be called.

A logon **Password** needs to be set for **OpenScape 4000 PSCA**.

The **Application language** is used by EasyLookup (on the phone) only.

Press the **Add device** button to save the device configuration.

Connectivity Adapter | Domain | **Device** | XMLApplication | Configuration | CCS Configuration | CCS LDAP Configuration | Manage Suspensions |

Search
Add
Export
Import

Add new device

Connectivity Adapter	XMLPS ▾
Domain	+49(42)42100- ▾
Extension	<input type="text"/>
Button number	<div> <input type="text"/> <div> AllAppsMenu EasyLookup EasyMail EasySee EasyShare </div> </div>
Configured buttons	<input type="text"/> <input type="button" value="X"/>
Password	<input type="password"/>
Confirm password	<input type="password"/>
Device type (optional)	<input type="text"/>
Application language	en ▾
User group	Not assigned ▾

Add device

Figure 65 Add new device

A new OpenScope 4000 Phone Service device has been added. Further devices can be added in the same way.

NOTE: An additional “user group” parameter can be seen on the **Device** details page. This is important only if the Phone Services are being used with multiple LDAP servers (check LDAP settings for details), otherwise leave it on **Not Assigned**.

It is possible to **export** the existing device database, and **import** a previously exported database. The export result is a .csv file. In case of import a Connectivity Adapter must be configured using the ID and domain listed in the CSV's device entries. The import will take effect after the restart of the CSTA service.

For information, switch to the **XML Application** configuration Web page.

[Device](#) [XMLApplication](#) | [Configuration](#) | [CCS Configuration](#) | [CCS LDAP Configuration](#) | [Manage Suspensic](#)

Add new device

Device added

Connectivity Adapter	XMLPS
Domain	+49(42)42100-
Extension	
Button number	<div>AllAppsMenu EasyLookup EasyMail EasySee EasyShare</div>
Configured buttons	
Password	
Confirm password	
Device type (optional)	
Application language	en
User group	Not assigned

Add device

Figure 66 Device added

Do not change anything in this configuration!!

Switch to the Configuration Web page.

[Connectivity Adapter](#) | [Domain](#) | [Device](#) [XMLApplication](#) | [Configuration](#) | [CCS Configuration](#) | [CCS LDAP Configuration](#) | [Manage Suspensions](#) | [Logout](#)

List of XML applications
Adding a new application is not a supported feature!

Name	Description	URL	
AllAppsMenu	Menu for Applications: EasyLookup, EasySee, EasyMail, EasyShare, Web Collaboration and Easy UC	%CONFIG_TOMCAT_BASE_URL%/ccs/menu	
EasyLookup	Display additional information for connected person(s)	%CONFIG_TOMCAT_BASE_URL%/ccs/ccs?PHONE=%phone%	
EasyMail	Opens blank email-form with filled-out email addresses for connected persons	%CONFIG_TOMCAT_BASE_URL%/ccs/mailme?PHONE=%phone%	
EasySee	Display of Directory Information	%CONFIG_TOMCAT_BASE_URL%/ccs/pc?PHONE=%phone%	
EasyShare	Starts a collaboration session with the participant of a phone call	%CONFIG_TOMCAT_BASE_URL%/ccs/WCServlet?PHONE=%phone%	
Easy UC	Menu for UC applications: UCStatus, UCDevice, UCLookup	%CONFIG_TOMCAT_BASE_URL%/ccs/UCMenu?PHONE=%phone%	

Figure 67 List of XML applications

It is recommended to change the Admin user password. If possible use only the SSO login from the OpenScape 4000 Assistant.

Configuration

Name	Value	Description
KeyTimeout	1500	Keypress timeout
CstaThreads	5	Number of CSTA processor threads
AppId	999	Application ID for HP4K IO
HttpRequesterThreads	5	Number of http requester threads
username	Admin	User name for GUI
password	****	Password for GUI
MaxScheduledThreadCount	30	Max number of scheduled task executor threads
PingTime	60	Time between two ping requests (to tray)
UCProtocolName	https	UC connection protocol
UCProtocolPort	4709	UC connection port
UCServerName	fe-automatix	UC server name
UCDefaultURL	http://localhost:4708/	UC default URL
UCSearchMaxResults	35	Maximum number of results for UC searches.
RepeatedSendDataDelay	0	Remove repeated SendData requests within the given time (ms, 0: turned off)
FvServerList	10000-99999;openscapewebc	OpenScape Web Collaboration server list. Format: [FirstId1]-[LastId1]:[serverA1],[serverA2],...
FvMailSubject	OpenScape Web Collaboratic	Subject of the invitation emails.
FvMailBody	Ladies and Gentlemen, You h	Body of the invitation emails. %SESSION_ID% is replaced with the actual session id. " " is the new line marker.

Update

Figure 68 Configuration

The **AppId** parameter has to match one part of the destination number in the AMO-ZIEL configuration.

This application ID can only be used by one application in a OpenScape 4000.

In case of **EasyUC** and **WebCollaboration integration**, please make sure to set the relevant information (like server address and port) to the corresponding field.

NOTE: Leave the other parameters as they are! Performance enhancements may only be carried out together with the development department.

In order to translate the UC host names (backend and fronted) to IP addresses platform linux DNS must be set or CSTA linux must be configured via /etc/hosts.

UC Simplex it is only one address, in case UC Large Deployment the user must add the UC Backend and Fronted IP addresses in /etc/hosts file from CSTA virtual machine.

Log out to exit the XMLPS configuration.

6.5 LDAP Connection Configuration for EasyLookup

6.5.1 CCS Configuration

First we need to set up some basic parameters for the Phone Services. Open up the **CCS Configuration** menu on the Phone Services graphical user interface.

Domain | Device | XMLApplication | **Configuration** | CCS Configuration | CCS LDAP Configuration | Manage Suspensions | Logout

CCS configuration

EasySee URL:	http://192.168.0.205:8080/ccs/phoneCard?PHONE=
EasySee Card URL:	http://192.168.0.205:8080/ccs/d4w?scdid=
LDAP Config File:	SCDV2.cfg <small>(see the Advanced configuration page in CBAdmin for template configurations (Component type: LDAPConfigFile, component: template.cfg))</small>
Default Country Code:	49
Default Area Code:	89
Default Main Number:	722
Outside Line Access:	0
National Prefix:	0
International Prefix:	00
Menu order:	Search by phone, name
SAT activated:	SAT deactivated
<div>ChangeReset</div>	

Figure 69 CCS Configuration - CCS LDAP Configuration

EasySee URL:	http://192.168.0.205:8080/ccs/phoneCard?PHONE=
EasySee Card URL:	http://192.168.0.205:8080/ccs/d4w?scdid=
LDAP Config File:	SCDV2.cfg <small>(see the Advanced configuration page in CBAdmin for template configurations (Component type: LDAPConfigFile, component: template.cfg))</small>
Default Country Code:	49
Default Area Code:	89
Default Main Number:	722
Outside Line Access:	0
National Prefix:	0
International Prefix:	00
Menu order:	Search by phone, name
SAT activated:	SAT deactivated
<div>ChangeReset</div>	

Figure 70 CCS Configuration

- LDAP Config File**
This is the default LDAP configuration that will be used. If there is more than one configured, then the one required can be selected from a drop down list.
- Domain attributes**

These are the parameters which have to match the OpenScape 4000 office code and outside line access code configuration.

- **Menu order**

On the device, the possible search options will be presented in this order.

- **SAT activated**

- **SAT deactivated**

If deactivated then the found numbers based on the given domain attributes will get transformed to dialable by the PBX.

- **SAT activated**

If activated then the transformation needs to be done in the Phone Services application.

6.5.2 CCS LDAP Configuration

LDAP specific settings can be configured on the **CCS LDAP Configuration** page. Multiple LDAP server can be used with Phone Services, however it requires a more detailed setup. First let's go over a scenario when only one LDAP server is used.

Connectivity Adapter | Domain | Device | XML Application | Configuration | CCS Configuration | **CCS LDAP Configuration** | Manage Suspensions | Logout

[CCS LDAP List](#)
[User Groups](#)

This is the list of the available LDAP configurations to use. If none is set for a device then the default (highlighted) will be used. If an LDAP configuration is enabled then it can be used by a device through a user group, otherwise it will be ignored.

Name	Enabled	Edit	Delete
SCDV2.cfg	No		
ActiveDirectory.cfg	No		
template.cfg	No		

Unique config name:

Any change regarding to CCS Configuration or to CCS LDAP Configuration can be applied on the fly by manually triggering a Synchronization. This process takes a few minutes.

Figure 71 *List of LDAP configurations*

On this page the currently available LDAP configurations can be seen. The one which has been chosen on the **CCS Configuration** page is marked with dark grey. That's the one that will be used for searching.

- **New LDAP configuration**

Adding a new LDAP configuration is possible, by giving an unique name and clicking on the **Add new LDAP Configuration** button. After this the added configuration will be shown in this list.

- **Delete configurations**

Click on the cross in the column **Delete** to delete an unused configuration.

IMPORTANT: LDAP configuration chosen on the **CSS Configuration** page cannot be deleted.

- **Editing and viewing configurations**

To edit or view a configuration click on the icon in the column **Edit**.

- **General settings**

On the upper section the general settings can be seen.

This is the quick edit view of this LDAP configuration.
Check the Advanced Configuration in CBAAdmin for further editing options

Setting for ActiveDirectory.cfg

LDAP Configuration Enabled	<input type="checkbox"/>
LDAP Server Address:	:0
LDAP User (empty if anonymous):	
LDAP Password:	
Search Base	
Telephone number match:	1
MaxLengthCIWildcardNumber:	4
Search method in queryName field:	surname firstname ▼
Number Format in LDAP:	canonical ▼

Figure 72 General LDAP settings

- **LDAP Configuration Enabled**

If this is checked then this LDAP server configuration can be added to a user group. For single LDAP usage it doesn't make any difference.

- **LDAP Server Address**

Address on which the LDAP server can be reached in host:port format.

- **LDAP User**

User to authenticate with. Can either be a direct user or a full path to the user entry, whichever one is supported by the LDAP provider.

- **LDAP Password**

Password for the user mentioned above.

- **Search base**

Full path of the search base which must be used for queries.

- **Telephone number match**

1 - if the server is doing automatic matches and conversion based on schema or on matching rule

0 - if Phone Services has to do this manually.

- **MaxLengthCIWildcardNumber**

If the previous is set to 0 then the query will be launched with the last X number of digits (X is what we define here). This must be the same length as the extension numbers.

- **Search Method in queryName field**

How should the Phone Services handle names: Surname before given name or vice versa.

- **Number format in LDAP**

Phone Services need to know which format is being used in the LDAP for storing phone numbers.

Possible values: **canonical** or **extension**

IMPORTANT: Phone Services requires the LDAP database to be consistent regarding the format of the phone numbers. At the moment only **canonical or extensions** are supported. If **extensions** is set then canonical won't be found and vice versa.

LDAP Attributes

LDAP Attributes		
Surname:	sn	
First name	givenName	
Display name	displayName	
Query name	cn	
Department:	department	
Locality:	l	
Mail:	mail	
Fax:	facsimileTelephoneNumber	
Room number:	physicalDeliveryOfficeName	
Building:	building	
Search number:	telephonenumber	
Telephone number:	telephonenumber	Telephone number searchable: <input type="text" value="yes"/>
Mobile phone number:	mobile	Mobile phone number searchable: <input type="text" value="yes"/>
Alternate phone number 1:	otherTelephoneNumber	Alternate phone number 1 searchable: <input type="text" value="yes"/>
Alternate phone number 2:		Alternate phone number 2 searchable: <input type="text" value="no"/>
Organisation:	o	
Country:	c	
SCDID (only used for SCD):	scdid	
PO Box:	postOfficeBox	
Description:	description	

Figure 73 *LDAP attribute specification*

Most of these settings are self-explanatory. If **telephone number searchable** is set to **yes** then the Phone Services will try to query that attribute as well. If it is set to **no**, then it will be ignored.

Click **Save** to set all the changes made on this page. By clicking on the **CCS LDAP List** on the left menu, or by clicking the **CCS LDAP Configuration** in the top menu, we can get back to the list of **LDAP configurations**.

IMPORTANT: At this time, the new settings are not applied on the fly. For any change to take effect either a synchronization must be started, or the tomcat service needs to be restated.

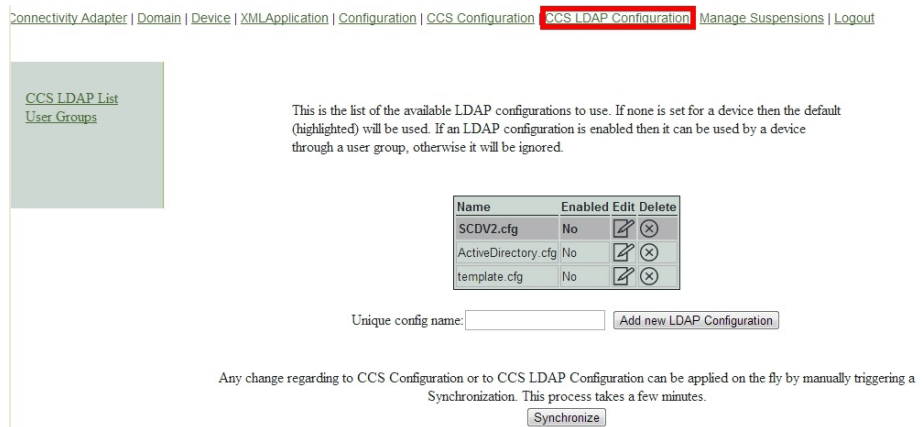


Figure 74 CCS LDAP Configuration

Synchronization can be started from the **CCS LDAP Configuration** page by clicking on the **Synchronize** button. This process puts a high load on the Phone Service and takes some time (one or two minutes usually).

6.5.3 Phone Services with Multiple LDAP Servers

As mentioned before Phone Services supports the usage of more than one LDAP server at the same time. In this case, LDAP configurations will be assigned to user groups, and user groups that will be assigned to devices.

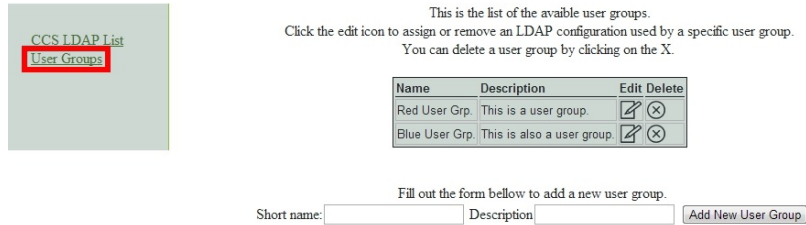
First of all, a LDAP configuration needs to be created for every single LDAP server, just as if they were used separately from each other.

If this is done, then the configurations representing a server need to be added to a user group. For this click on the **User Groups** menu on the left side of **CCS LDAP Configuration** page.

Phone Services – Introduction

LDAP Connection Configuration for EasyLookup

[Connectivity Adapter](#) | [Domain](#) | [Device](#) | [XMLApplication](#) | [Configuration](#) | [CCS Configuration](#) | **CCS LDAP Configuration** | [Manage Suspensions](#) | [Logout](#)



This is the list of the available user groups.
Click the edit icon to assign or remove an LDAP configuration used by a specific user group.
You can delete a user group by clicking on the X.

Name	Description	Edit	Delete
Red User Grp.	This is a user group.		
Blue User Grp.	This is also a user group.		

Fill out the form below to add a new user group.

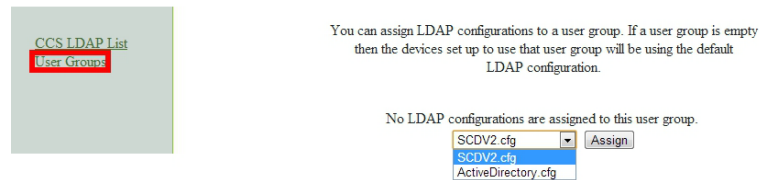
Short name: Description:

Figure 75 User groups

Creating a user group is possible by filling out the form, and deleting is possible by clicking on the cross.

After a user group is created, one or more LDAP configurations can be assigned to it by clicking on the **Edit** button.

[Connectivity Adapter](#) | [Domain](#) | [Device](#) | [XMLApplication](#) | [Configuration](#) | [CCS Configuration](#) | **CCS LDAP Configuration** | [Manage Susp](#)



You can assign LDAP configurations to a user group. If a user group is empty then the devices set up to use that user group will be using the default LDAP configuration.

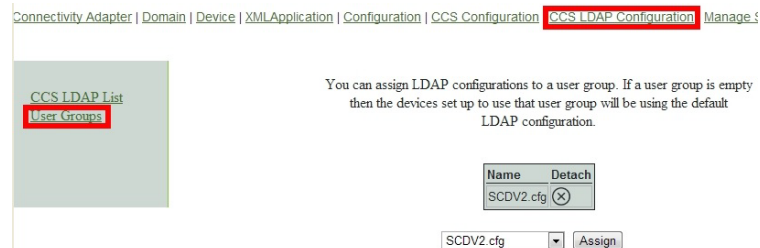
No LDAP configurations are assigned to this user group.

SCDV2.cfg

Figure 76 User group - assign LDAP Configuration

As mentioned before the first option in an LDAP configuration is an enabled/disabled flag. An LDAP configuration will be shown here in order to be assigned, only if that flag was checked previously.

Removing from a user group is done by clicking the cross here as well.



You can assign LDAP configurations to a user group. If a user group is empty then the devices set up to use that user group will be using the default LDAP configuration.

Name	Detach
SCDV2.cfg	

SCDV2.cfg

Figure 77 User group - detaching a configuration

After the user groups have their desired LDAP configuration assigned, the devices must be set to these user groups.

This can be done on the device modify page (**Device** menu > search for a device > **Modify**).

Connectivity Adapter | Domain | **Device** | XML Application | Configuration | CCS Configuration | CCS LDAP Configuration

Search
Add

Modify existing device

Connectivity Adapter

XMLPS

Extension

1660

Button number

AllAppsMenu
EasyLookup
EasyMail
EasySee
EasyShare

✓

Configured buttons

12 AllAppsMenu

Password

...

Confirm password

...

Device type

Application language

en

User group

Not assigned
Not assigned
Red User Grp.
Blue User Grp.

Modify device

Figure 78 Device modify - assigning a user group

Click **Modify** to save this setting. When this is done, this device will use the LDAP servers that are assigned to the set user group. From a technical point of view the parallel search and the result will be merged. With this solution the user won't be able to see any difference in Phone Services usage.

6.5.4 Configuration Example: Web Page Design

custom5

queryname

firstname

surname

custom2

custom1

department

locality

custom6

roomnumber

mail

Details for: Senior Service Trainer

personal information

Name

Friedhelm Grunert

Given name

Friedhelm

Surname

Grunert

Grad. title

Initials

Function

Catchword

Country

Deutschland

Organization

APT

Location

Paderborn

Room

DEF1/03

gID

SCD-ID

Common Name

E-Mail

a42u7140@labor9521.de

URL

Remark

Communication

Telephone

+49 (42) 42100 - 7140

Telephone 2

+49(151)10835128

Telefax

+49(89)7007-18108

pers. Telefax

Mobile

+49(175)1826746

Pager

Video 1

Video 2

Post box

33094

NetMeeting

Organization

Org-chart

Assistant

Representation

Cost location

Cost location unit

Certificates

Other

number1

number3

number2

fax

custom5

Figure 79 Configuration parameter EasySee Web page

Configuration Example: Web Page Design

The EasySee Web page is based on the attributes available in every LDAP Configuration.

Customization of this Web page is possible but not covered in the training!

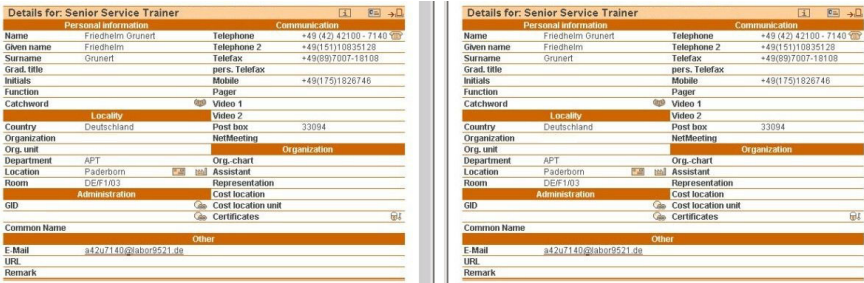


Figure 80 Web page design

6.6 Suspension

NOTE: This feature is related to the Phone Services graphical user interface and to CBAAdmin graphical user interface as well.

Temporary login lock

Both CBAAdmin and the Phone Services graphical user interface (XCI_GUI) have a login page that needs to be defended from attackers. While most of the defense mechanism is not noticeable for the administrator, there is vivid one, and that is the delayed login.

As a general rule, after every single login attempt a short suspension will be given (single sign on is not affected). These few seconds are enough to give significant defense against brute force attacks. After the login a progress bar can be seen, that will give a rough estimation when the suspension will end (the animation is browser and load dependent, but the suspension length always matches with the displayed information). If a login fails then this delay time increases exponentially.

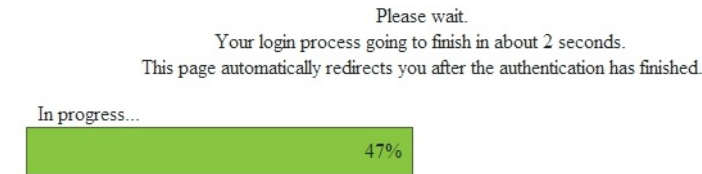


Figure 81 CBAAdmin - delayed login progress

A similar bar can be seen if the Phone Services graphical user interface is accessed directly and not from CBAAdmin.

Suspension List

In the **Suspension List** the IP addresses are listed in a table from where the last failing attempts came. This list can be displayed in the Phone Services **Manage Suspensions** menu.

Manage Suspensions > Show List

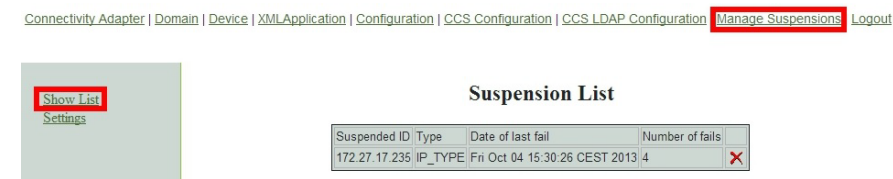


Figure 82 Manage Suspension - suspended addresses

If an IP address needs to be removed from the suspensions then this can be done by clicking the cross.

Settings

There are two settings for this feature which can be reached via the link **Settings** from the left side of the **Manage Suspension** page.

Manage Suspensions > Settings



Figure 83 Manage Suspension - settings

- Enable/disable suspension list
With **Enables and Disables the suspension list** the feature can be turned on or off in the column **Current Value** with **Enable** or **Disable**.

IMPORTANT: It is not recommended to turn this feature off, since then the administrator graphical user interface can be successfully penetrated by brute force attacks.

- **Allow authentication from host server without suspension checking**
If this option is enabled the check is skipped, if the login request comes from the same machine, where OpenScape 4000 CSTA is installed.

6.7 OpenScape 4000 Phone Services Client Application or OpenScape 4000 PSCA (prev. XCI Tray)

NOTE: You can download **OpenScape 4000 Phone Services (prev. XCI Tray)** from the OpenScape 4000 Phone Service Web page. OpenScape 4000 V7 integrated variant: <https://<CLAN IP fo CSTA VM>:8081/ccs/html/index.html>

[Home](#) | [Download](#)

Download software

To use and/or initiate OpenScape 4000 Phone Services from your PC you have to install the OpenScape 4000 Phone Services client application.

Installation instructions

1. [Download](#) systray client application (Version V7_R0.204.0)
2. Double click on the setup.exe icon and the installation will be started
3. The systray application starts automatically and an icon will appear in your system tray



Figure 84 Download OpenScape 4000 Phone Services

Select **Download** to download the program.

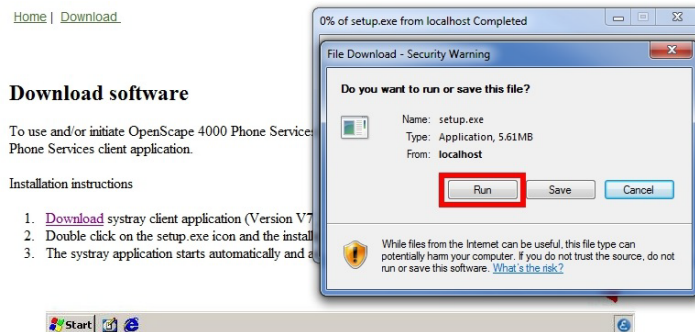


Figure 85 Run or Save

Press **Run** to execute and install or **Save** to save the program.

Phone Services – Introduction

OpenScape 4000 Phone Services Client Application or OpenScape 4000 PSCA (prev. XCI Tray)

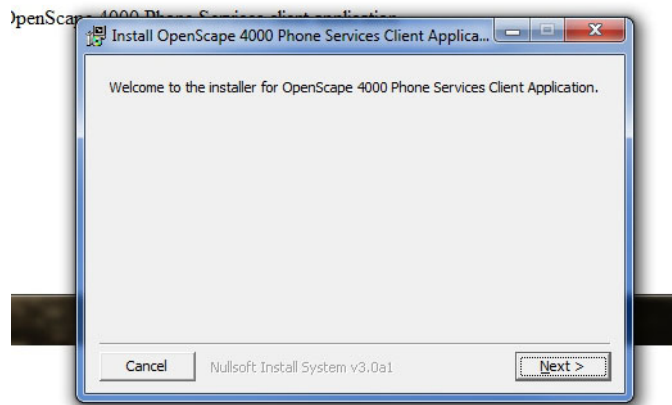


Figure 86 *OpenScape 4000 Phone Services (prev. XCI Tray) installation*

After starting setup.exe, first a confirmation window will appear, then the option to change the installation directory. At the end of the installation click **Close** to finish.

You then need to start the OpenScape 4000 Phone Services (prev. XCI Tray) via the Start menu:

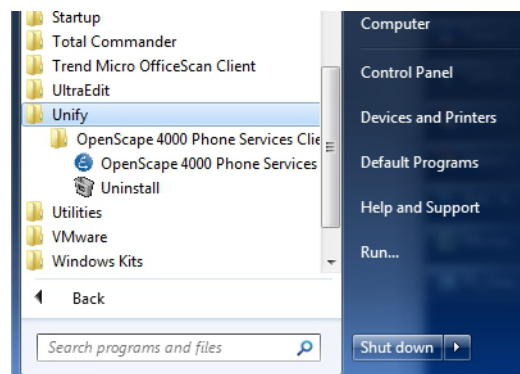


Figure 87 *OpenScape 4000 Phone Services in Start menu*

Please note that OpenScape 4000 Phone Services can run only in one instance even on a multisession computer. Meaning if a user is already started OpenScape 4000 Phone Services, then another user in another session won't be able to use it also.

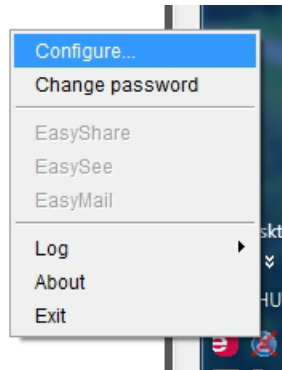


Figure 88 OpenScape 4000 Phone Services - Configuration menu

Because there is no valid configuration as yet, you need to add a configuration by selecting the Configure.. menu from the OpenScape 4000 Phone Services (prev. XCI Tray):

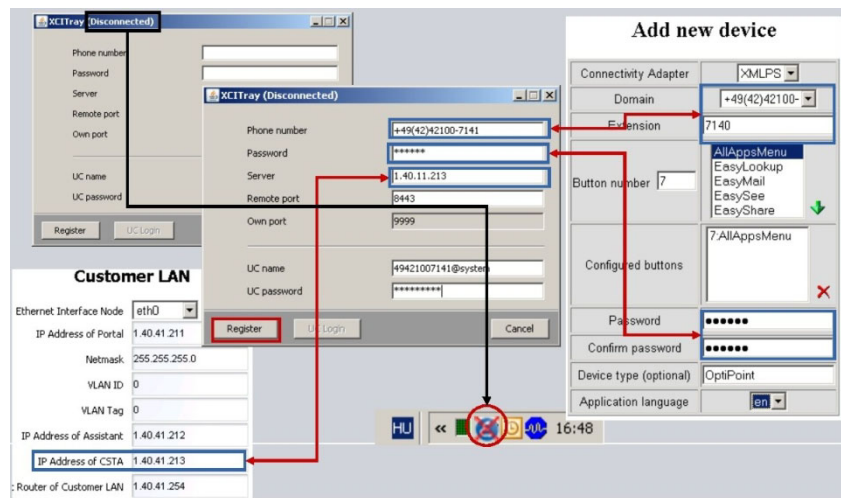


Figure 89 OpenScape 4000 Phone Services (prev. XCI Tray) configuration

In case of problems, open the Logs menu from the popup menu by clicking the OpenScape 4000 Phone Services (prev. XCI Tray) icon.

Phone Services – Introduction

OpenScope 4000 Phone Services Client Application or OpenScope 4000 PSCA (prev. XCI Tray)

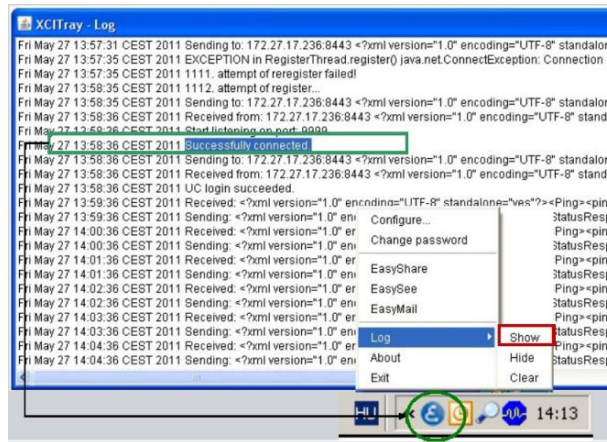


Figure 90 OpenScope 4000 Phone Services logs

This log message provides helpful information about the connection.

Following successfully registration via the OpenScope 4000 Phone Services (prev. XCI Tray) menu, EasySee, EasyMail and EasyShare can be started easily (not only from the phone menu).

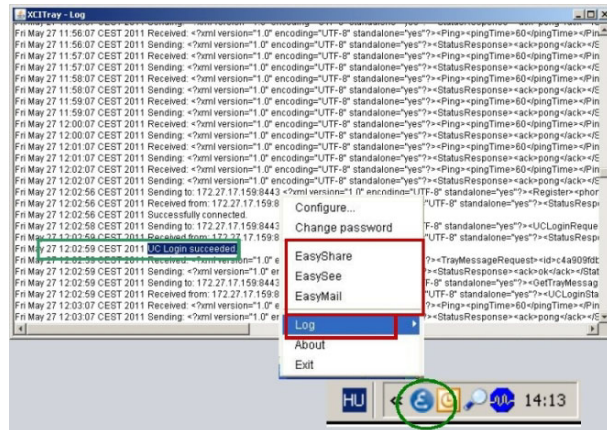


Figure 91 OpenScope 4000 Phone Services Menu - functions

If the OpenScope 4000 Phone Services (prev. XCI Tray) is then also entered automatically by the UC account, log in to the UC server to use the EasyUC functionality.

NOTE: For EasyUC functionality you can enter the UC server account into the OpenScope 4000 PhoneServices (XCI Tray) Window, it should be <username>@system. The @system is automatically added to the username if it is missing.

List of Figures

Figure 1	Scenarios - One CSTA link.	7
Figure 2	Scenarios - Four CSTA links per process	8
Figure 3	Maximum 8 Connectivity Adapters per system	8
Figure 4	Configuration batch description	9
Figure 5	java process	14
Figure 6	bash process	14
Figure 7	cbdriver4000 process	14
Figure 8	Internal WEB Service Communication	15
Figure 9	Internal Communication	15
Figure 10	Connect to OpenScape 4000 Platform Administration (Portal)	15
Figure 11	System	16
Figure 12	System - LAN Wizard - Step 1	16
Figure 13	System - LAN Wizard - Step 2	17
Figure 14	System - LAN Wizard - Step 3	17
Figure 15	System - LAN Wizard - Step 4	18
Figure 16	Wizard complete.	18
Figure 17	Connect to OpenScape 4000 CSTA.	22
Figure 18	Connectivity Adapter List - Select Connectivity Adapter	22
Figure 19	Configuration - CA4000_Default Configuration	23
Figure 20	Connectivity Adapter List - Add New Connectivity Adapter	24
Figure 21	Add CA	24
Figure 22	Configuration - Modify	25
Figure 23	Configuration - Add new application.	26
Figure 24	Configuration - Add application	26
Figure 25	Configuration - New application added.	27
Figure 26	Status - PBX Link	27
Figure 27	Log - Show/Clear up till version V7 R1.	28
Figure 28	Log - Show / Clear in V7 R2.	29
Figure 29	Log - Data download	30
Figure 30	Component log properties	30
Figure 31	Statistics	31
Figure 32	Phone Services UI	33
Figure 33	Change default user and password	34
Figure 34	Trusted IP addresses	35
Figure 35	HTTPS Connections.	35
Figure 36	General architecture of the circuit connection	38
Figure 37	Advanced Configuration - Component selection	39
Figure 38	Advanced Configuration - Export/Import	40
Figure 39	Connection to Backup & Restore, Software Activation/Transfer	41
Figure 40	Backup & Restore - BEER_CSTA (configuration)	41
Figure 41	Change the Offered Mode	44
Figure 42	UC functionality on the GUI	46
Figure 43	EasyLookup - Call the menu by pressing the application button on the device	54
Figure 44	EasySee	55
Figure 45	EasyMail	56
Figure 46	WebCollaboration integration	57

List of Figures

Figure 47	EasyUC	58
Figure 48	Single connected OpenScape 4000 CSTA (OpenScape 4000 V7)	59
Figure 49	Administration URLs – in case of OpenScape 4000 V7 integrated variant	59
Figure 50	Phone Service URLs	60
Figure 51	Phone Service XML Service Tray Port in case of OpenScape 4000 V7 integration 8081	61
Figure 52	AMO Configuration	63
Figure 53	Application	64
Figure 54	Login	64
Figure 55	Phone Services UI	65
Figure 56	Domain - Add	65
Figure 57	Add new domain	66
Figure 58	List of domains	66
Figure 59	List of Connectivity Adapters	66
Figure 60	XMLPS	67
Figure 61	Add ConnectivityAdapter	67
Figure 62	XMLPS - Add new domain	67
Figure 63	Add new Connectivity Adapter	68
Figure 64	Device	68
Figure 65	Add new device	69
Figure 66	Device added	70
Figure 67	List of XML applications	70
Figure 68	Configuration	71
Figure 69	CCS Configuration - CCS LDAP Configuration	72
Figure 70	CCS Configuration	72
Figure 71	List of LDAP configurations	73
Figure 72	General LDAP settings	74
Figure 73	LDAP attribute specification	75
Figure 74	CCS LDAP Configuration	76
Figure 75	User groups	77
Figure 76	User group - assign LDAP Configuration	77
Figure 77	User group - detaching a configuration	77
Figure 78	Device modify - assigning a user group	78
Figure 79	Configuration parameter EasySee Web page	78
Figure 80	Web page design	79
Figure 81	CBAdmin - delayed login progress	79
Figure 82	Manage Suspension - suspended addresses	80
Figure 83	Manage Suspension - settings	80
Figure 84	Download OpenScape 4000 Phone Services	81
Figure 85	Run or Save	81
Figure 86	OpenScape 4000 Phone Services (prev. XCI Tray) installation	82
Figure 87	OpenScape 4000 Phone Services in Start menu	82
Figure 88	OpenScape 4000 Phone Services - Configuration menu	83
Figure 89	OpenScape 4000 Phone Services (prev. XCI Tray) configuration	83
Figure 90	OpenScape 4000 Phone Services logs	84
Figure 91	OpenScape 4000 Phone Services Menu - functions	84

List of Tables

Tabelle 1	Configuration parameters in Connectivity Adapter	19
Table 2	Statistics - Link Status" section.	31
Table 3	Statistics - "PBX Communication" section	32
Table 4	Statistics - "Application" section	32

Index

A

Additional Supported Services 41
Application Environment 13

C

CBAAdmin - CA Instance Configuration 22
CBAAdmin – CA Instanz Konfiguration 42
CBAAdmin Configuration Management
 Phone Service UI 33
Configuration Batch Description 9
Configuration Example
 Web Page Design 78
Configuration Requirements 10
CSTA Switch Integrated – Introduction 13

E

EasyLookup 53
EasyMail 55
EasySee 55
EasyShare 56
EasyUC 57

H

Hardware Requirements 9
HiPath 4000 CSTA 5
HiPath 4000 Phone Services
 Download 81
HiPath 4000 Phone Services XCI Tray 81
HiPath 4000 V6 Maximal Values 7

I

Internal Integration 7
Introduction 5

P

Phone Service UI 33
Phone Services
 Configuration
 AMO Configuration HiPath 4000 V4, V5, V6 62
 Configuration Steps 62
 HiPath 4000 CSTA 63
 EasyMail 55
 EasySee 55
 EasyShare 56
 EasyUC 57
 LDAP Connection
 Configuration for EasyLookup 72
 Overview 53

Requirements 61

Structure 59

Phone Services – Introduction 53

Port List 11

Portal – IP Address Configuration 15

R

Requirements 9

S

Scenarios 7

Software Requirements 9

 Operation System 9

X

XCI Tray

 Configuration 83

 Install 81

 Logs 84

