A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000

OpenScape 4000, CSTA and Phone Services

Service Documentation
07/2024

P31003-H31A0-S101-04-7620

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

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 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 V10 Maximum Values

Based on **OpenScape 4000 V10 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.

NOTICE: One Connectivity Adapter can support 4 application links simultaneously and maximum of 8 or 16 Connectivity Adapters supported.

2.2 CSTA application connection

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

1 CSTA link

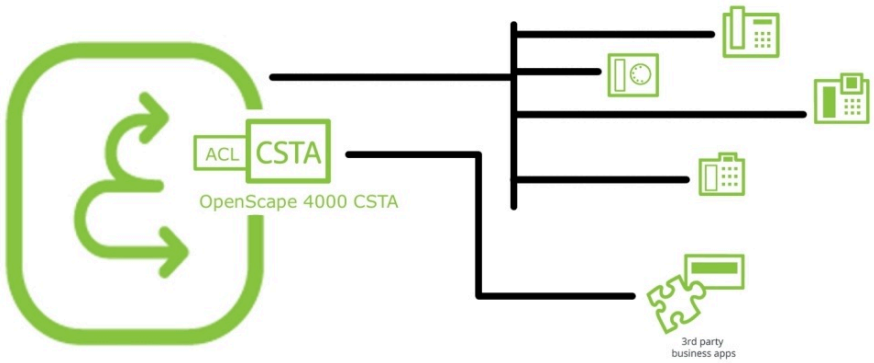


Figure 1: Scenarios - One CSTA link

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

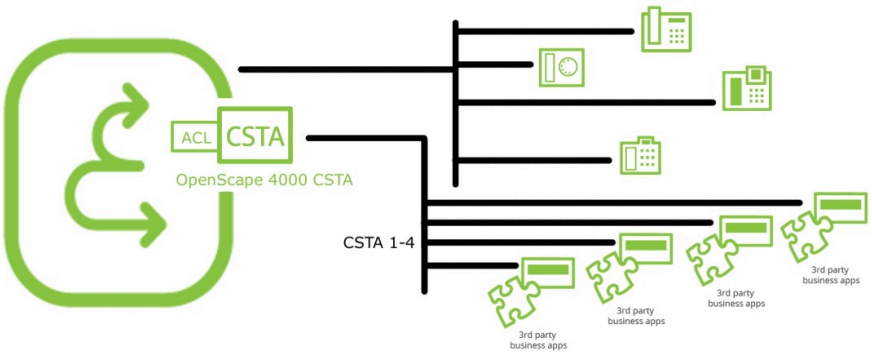


Figure 2: Scenarios - Four CSTA links per process

Maximum 4 applications can use the same Connectivity Adapter.

Maximum 8 (16) Connectivity Adapters on a system

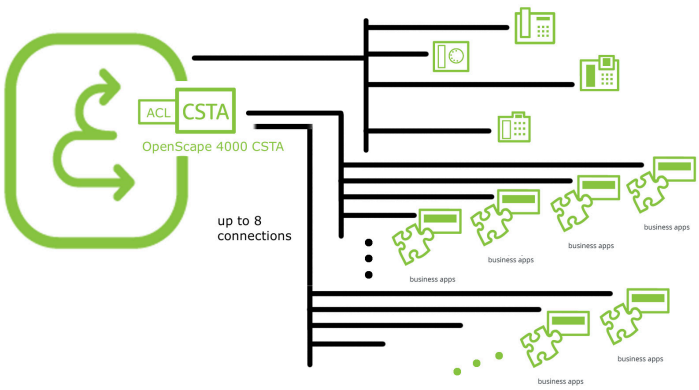


Figure 3: Maximum 8 Connectivity Adapters per system

In V8 R1, in case of enough physical memory on the hardware, the CSTA VM can have more memory than usual (e.g. 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 can be increased to 16. Please be aware that in care 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

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

3.2 Software Requirements

3.2.1 Operating System

The integrated OpenScape 4000 CSTA is a Linux container running on the OpenScape 4000 platform control host and sharing a SuSE Linux Enterprise Server (SLES) 15 SP3 as an operation system.

3.2.2 Supported Software

IBM Java 6 is used for the integrated OpenScape 4000 CSTA versions up till V7 R1 and IBM Java 7 in V7 R2 and V8 R1.

3.3 Configuration Batch Description

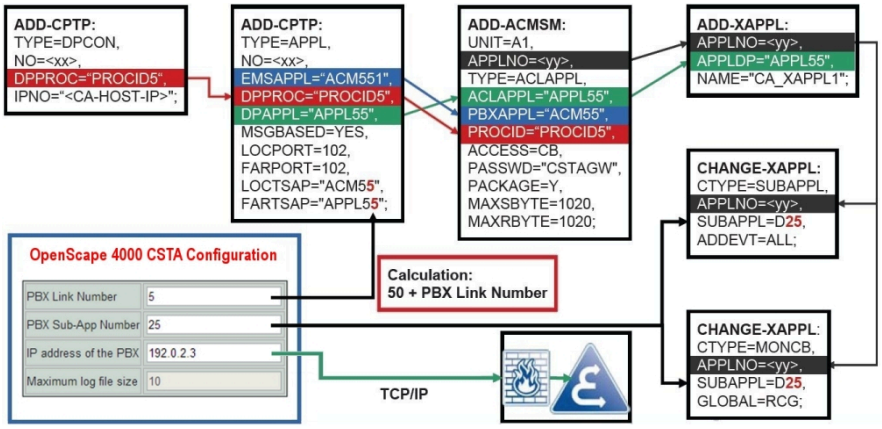


Figure 4: Configuration batch description

Figure 4 on Page 11 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:
2) AMO-DIMSU parameter: ECCS:
3) Maximum number of monitored devices is also set
4) 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.
5) Call processing timers must be set
6) AMO-CTIME, customer-specific CP1 timers, switching unit manages the call processing timers, which are evaluated by the MakeCall requests.
7) Initial communication ACL-C Link is configured
8) AMO-CPTP, communication parameters for tcp/ip connection (as ACL-C identifier only) TYPE:DPCON
9) Application interface parameters (transport address)
10) AMO-CPTP, communication parameters for tcp/ip connection TYPE:APPL
11) ACL Manager parameters
12) AMO-ACMSM, ACL manager communication parameter APPLTYP= ACLAPPL
13) XAPPL application
14) AMO-XAPPL, DVA -application ACL
15) XAPPL sub-application parameters
16) AMO-XAPPL, CTYPE: SUBAPPL.
17) XAPPL monitored elements
18) AMO-XAPPL, CTYPE: MONCB.

3.4 Configuration Requirements

From HiPath 4000 V6 all CSTA applications must use the CA4000 adaptor of the integrated OpenScape 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 HiPath 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, Genesys, CICA and several other applications)`
- `2205 (used as default in e.g. VAS-B, BLF)`
- `2209 (used as default in e.g. VAS-B, HiCALL, DTB)`
- `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 installation. The following facilities are available:

- CBAdmin 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 newer versions)`
  - `{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` for V7R0 or `tomcat6` for newer versions. A new process is responsible for this: `java`.

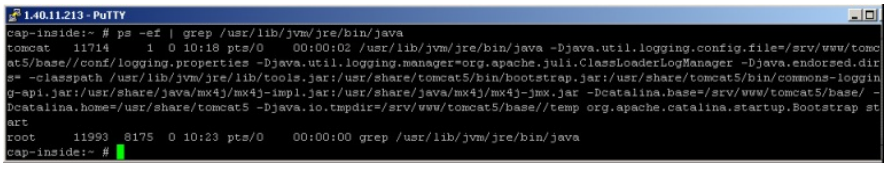


Figure 5: java process

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.

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.

Figure 7: cbdriver4000 process

> **NOTICE:** 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.

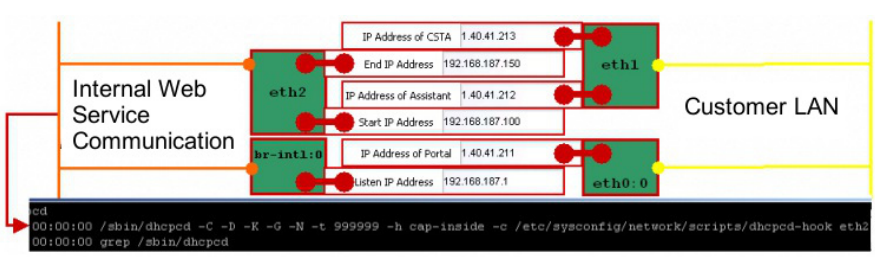


Figure 8: Internal WEB Service Communication

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.

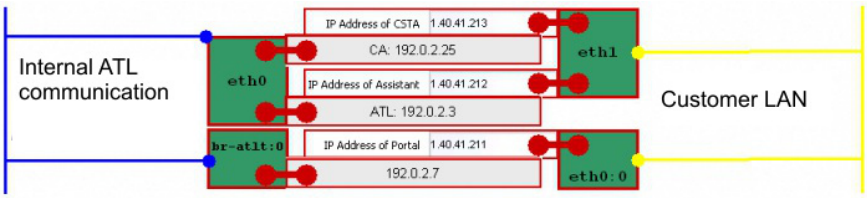


Figure 9: Internal Communication

5.2 Portal – IP Address Configuration

Log on to **OpenScape 4000 Assistant** and select:

Expert Mode > Platform Portal

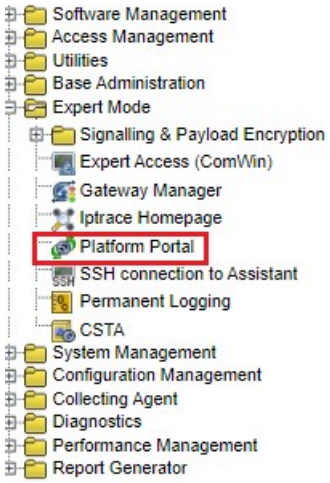


Figure 10: Connect to OpenScape 4000 Platform Administration (Portal)

Expand **System**, then LAN Configuration and select System to configure the OpenScape 4000 CSTA IP address.

Figure 11: System

Press **Next.**

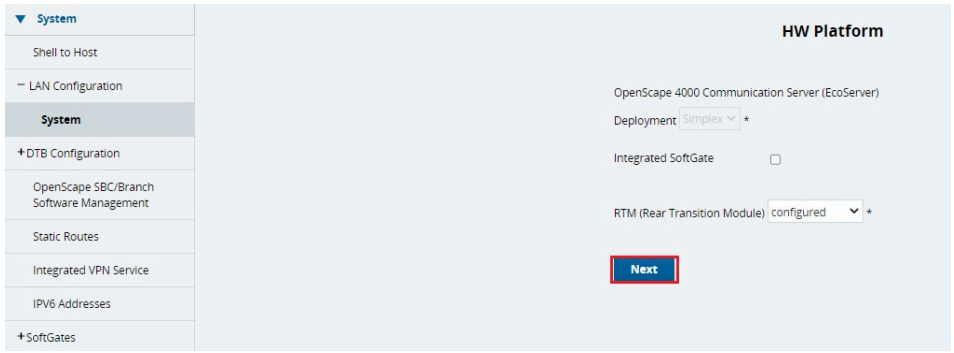


Figure 12: System - LAN Configuration - Step 1

Enter the OpenScape 4000 CSTA IP address and press **Next**.

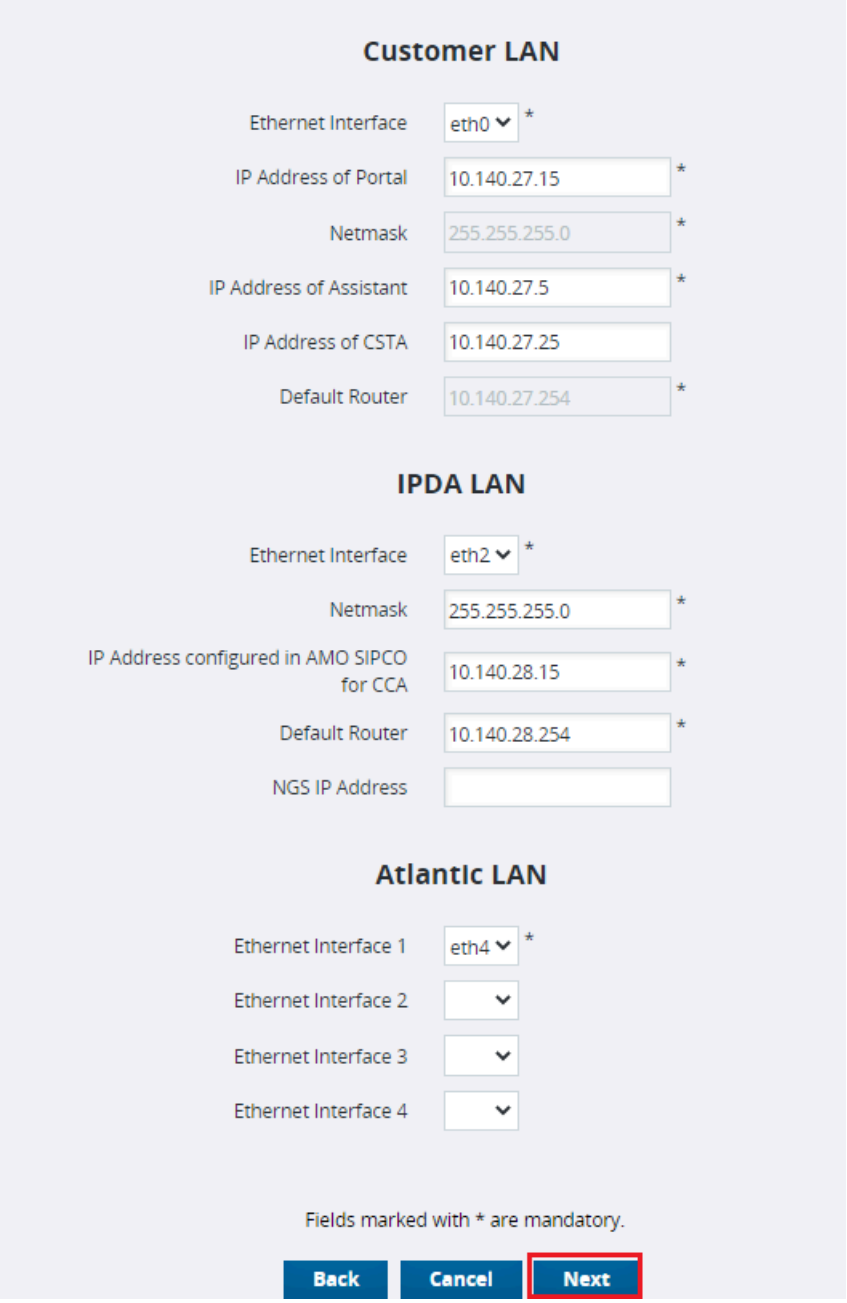


Figure 13: System - LAN Configuration - Step 2

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

Press **Next**.

Figure 14: System - LAN Configuration - Step 3

Press **Submit**.

5.3 Features

5.3.1 Important news in V10

5.3.1.1 General enhancements in V10

GUI

Starting with V10, the GUI for OpenScape 4000 CSTA was optimized to improve the user experience. In this way, the new CSTA design is also aligned with other OpenScape 4000 components.

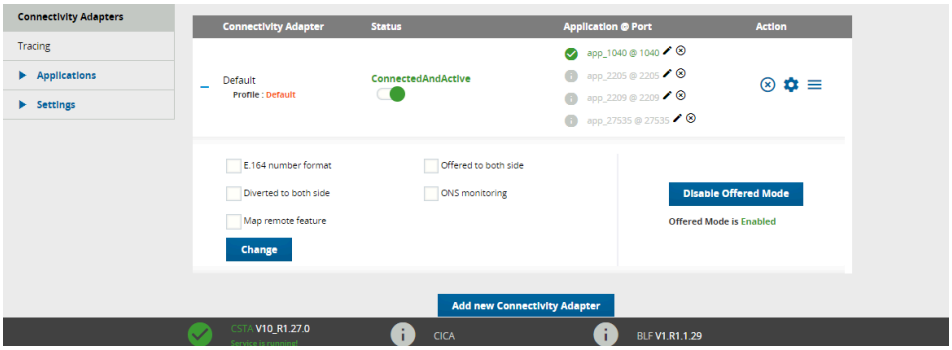


Figure 15: OpenScape 4000 V10 CSTA Dashboard

Most of the existing pages were combined or enhanced to offer more control over the whole CSTA.

Before V10, the landing page contained all configured Connectivity Adapters and each adapter had to be selected individually to have access to the configuration. The landing page was changed into a dashboard that offers at a glance a quick overview of the CSTA.

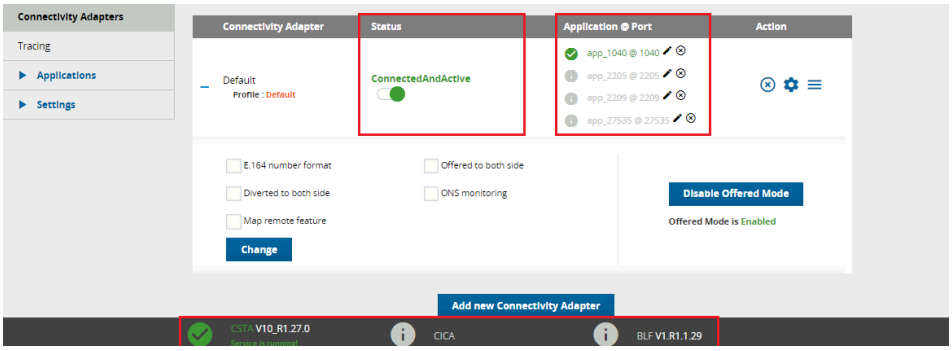


Figure 16: Dashboard Overview

You can now see the status of your Connectivity Adapters and corresponding applications without leaving the main/landing page.

At the bottom of the page, the status bar was introduced. This new component offers:

- an overview of the CSTA version that is currently running
- the status of the CSTA service
- the status of the CICA application that is running inside the CSTA environment
- the status and the version of the integrated BLF server

Private cbdriver versions are also displayed here.

The GUI redesign of the OpenScape 4000 CSTA comes with new design elements like:

- a new menu design

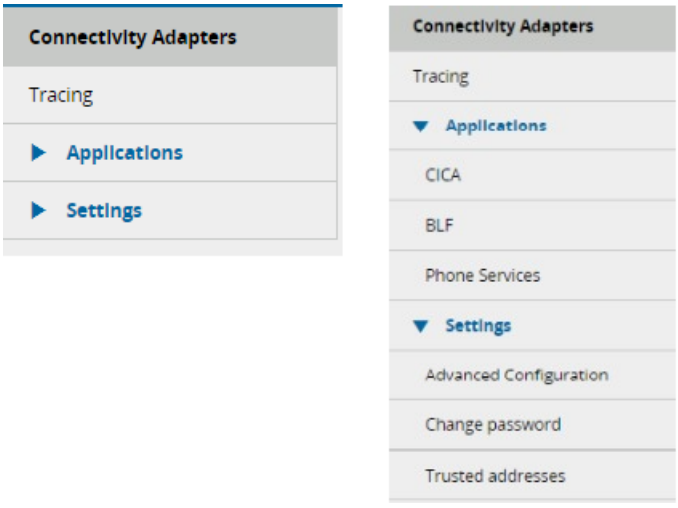


Figure 17: CSTA menu (collapsed and expanded)

- expandable tables

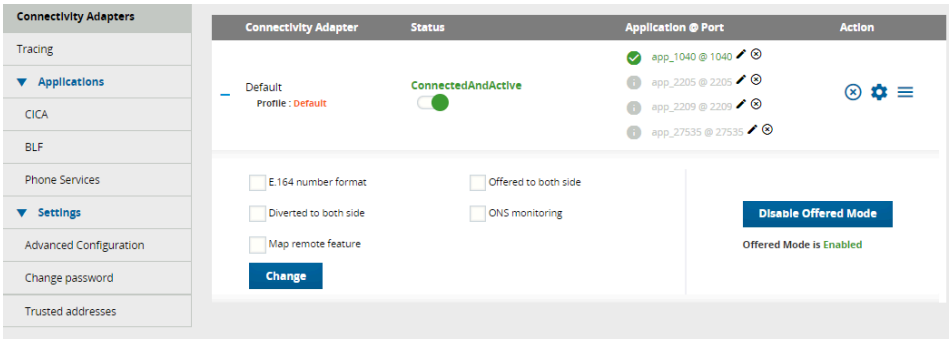


Figure 18: Connectivity Adapter List

- floating windows

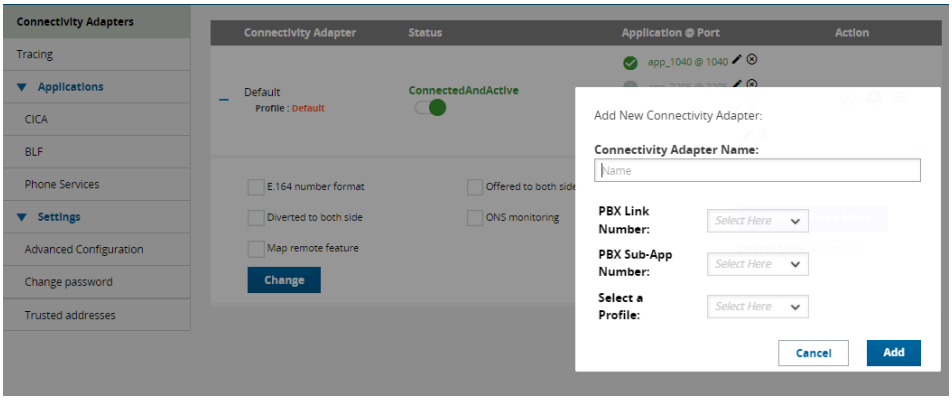


Figure 19: Floating window for adding a new Connectivity Adapter

- floating menus

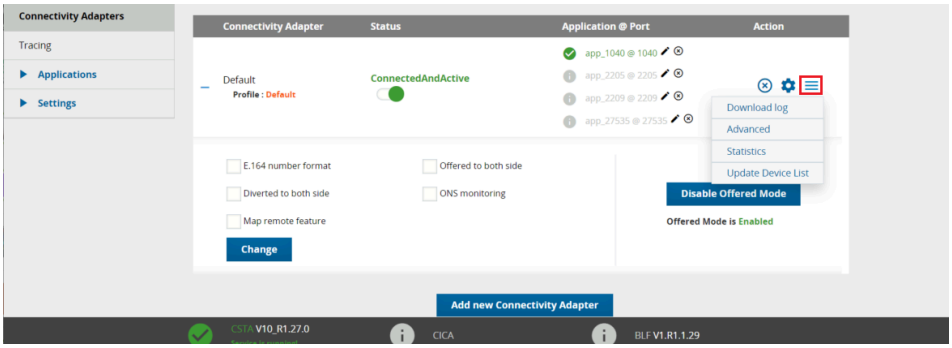


Figure 20: Floating menu available for each Connectivity Adapter

Application profiles

The OpenScape 4000 CSTA offers support for multiple applications connected to its ports, but up until V10 all the custom configurations were done manually (using Advanced Configuration) to ensure compatibility.

Starting with V10, the CSTA GUI offers the possibility to select the desired profile and all the custom configurations will be done automatically in the background. This way manual intervention is minimal, and an application can be used as soon as a port is configured for it.

Application profiles affects all the applications configured for a Connectivity Adapter.

Available profiles:

- Default
- ASC
- Circuit
- Concierge/PSSF
- OSCC
- OSMO
- UC

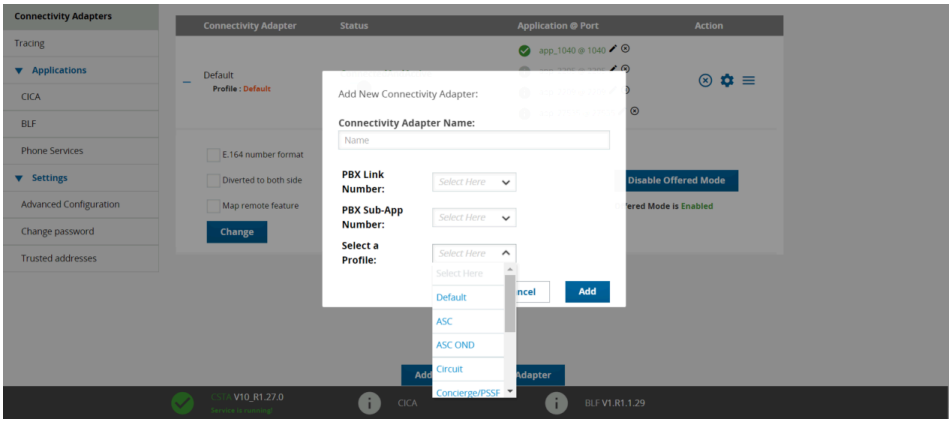


Figure 21: Selecting a profile

Available profile actions:

- set (when adding a new Connectivity Adapter)
- change (from the Modify Connectivity Adapter window)
- reset (from the Modify Connectivity Adapter window)

Some profiles require **Offered Mode** to be active. The application profile will also take care of this action. If the current PBX configuration does not allow **Offered Mode** to be configured, then you can retry this action manually or adjust the PBX values.

All the existing Connectivity Adapters are set to the Default profile after upgrading from a version lower than V10.

The Default profile does not track changes done in the Advanced Configuation, but all the other profiles are monitored after every change and signaled on the main page if the configuration was altered.

Certificate handling

In previous versions, OpenScape 4000 CSTA provided a standalone feature to change the default certificate and private key that were used for communication through the https protocol. Starting with V10, the certificate handling has moved to Assistant.

To activate a new certificate, log in to OpenScape 4000 Assistant and go to:

Access Management > Manage Web Server Certificates > Certificates for this Web Server > Activate

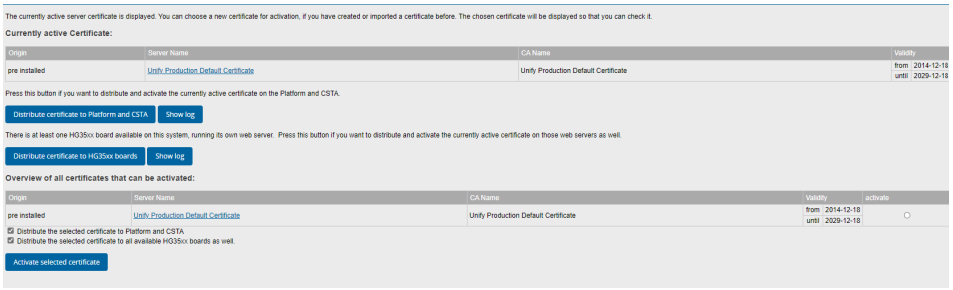


Figure 22: How to distribute new certificates to CSTA

IMPORTANT: In case a 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.

NOTICE: In case of OpenScape 4000 V8 integrated OpenScape 4000 CSTA, the CBAdmin 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 (previously XCI Tray) is now done using the OpenScape 4000 distributed certificate that should be the same as the one used by the Assistant.

5.3.1.2 Security

Support of TLS 1.3 and TLS 1.2 is enabled by default.

In OpenScape 4000 V10, TLS 1.0 is not offered anymore. The only option available in OpenScape 4000 Assistant is TLS 1.3 with fallback to TLS 1.2.

TLS configurable from Assistant

Starting with V8R2, the TLS version can be configured for OpenScape 4000 CSTA from OpenScape 4000 Assistant (**Access Management > Security Mode Confuration > TLS protocol section)**.

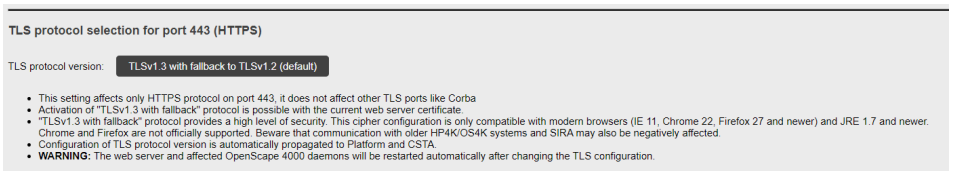


Figure 23: OpenScape 4000 Assistant TLS protocol

Possible values for the TLS protocol version:

- TLS 1.3 with fallback to TLS 1.2 (default)

Default CSTA certificate

To increase CSTA security, the default web certificate was replaced starting with V8R2. The previous default CSTA certificate was replaced by the certificate

used by Assistant that has a 2048-bit public key and sha256WithRSAEncryption signature algorithm.

5.3.2 Other features

5.3.2.1 Discontinuation of the CSTA Licensing

License control for CSTA has been removed since V7. However the CSTA functionality will be continued in V8 license check for CSTA connectivity has been cut off. The CSTA license has been removed in the ordering tools, CLS and OpenScape 4000 V8 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.

5.3.2.2 Further enhancements for the OpenScape 4000 - OpenScape UC interaction

General behavior

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 model 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:

Table 1: Configuration parameters in Connectivity Adapter

Name	Description	Default value in Connec-tivity 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_SIDES	Send the Offered event to the calling party.	0 (off)	

Name	Description	Default value in Connec-tivity Adapter	Comments
DIVERTED_TO_BOTH_SIDES	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)	

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

- Offer the incoming call's controll to monitoring applications: see Section 5.4.9.3, "Support of the Offered mode of the Alerting state"
- Enhance the supported number formats: see Section 5.4.9.4, "Delivering deviceIDs in E.164 Format (SFR international)"
- Provide DIVERTED event also for the calling side Section 5.4.9.5, "OFFERED and DIVERTED events for the calling side" (developped 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 5.4.9.5, "ONS based monitoring using the binding information"
- Device search based on a user defined list: see Section 5.4.9.5, "Dynamic device list in the Accept Call request"
- Provide state transitions of the remote side: see Section 5.4.9.5, "Remote features"
- Enhance Single Step Transfer service: see Section 5.4.9.5, "Single Step Transfer for the consulting party" and Section 5.4.9.5, "Seamless Handover by Single Step Transfer"
- Send Offered events also to the calling side: see Section 5.4.9.5, "OFFERED and DIVERTED events for the calling side"
- Enhance Deflect call service: see Section 5.4.9.5, "Deflect of the second call"
- Emulate an early release mechanism for Deflect, Call Forward No Reply and Single Step Transfer scenarios: see Section 5.4.9.5, "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 5.4.9.5, "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 5.4.9.5, “Special CSTA flow for the Hunt Group calls”

The features listed below are implemented for the V8 R1.

- Static OND is a feature used by OSCC, but all applications can receive these parameters as private data. see Section 5.4.9.12, “Static OND”

5.3.2.3 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 Developper’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 5.4.8, “Circuit Interface Connectivity Application”.

5.3.2.4 General enhancements

The logging of all “CSTA processes” was enhanced to use syslog when it is necessary to send a 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.

In V8 R1 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 10.

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.

Tracing

Enhancements were made in OpenScape 4000 CSTA V8R2 to ensure a better tracing and logging mechanism. The new tracing feature allows tracing to be enabled simultaneously for maximum 4 Connectivity Adapters.

OpenScape 4000 CSTA was enhanced to:

- provide all the tracing and logging options in one page
- by default, allow tracing to start automatically as soon as an application connects to a Connectivity Adapter (if the limit wasn't reached)
- offer the possibility to switch between different tracing states: AUTO, STOP or BIND (depending on the use case)
- allow downloading the logs, traces and CSTA configuration for a certain connectivity adapter or for all the connectivity adapters
- automatically use all the options from V8R1 under Trace Control (to trace CSTA messages, ACL messages, messages in ASCII, messages in HEX and disable loopback messages)

See a general description in Section 5.4.3.2, "Tracing".

Advanced Configuration

Starting with V8R2, Advanced Configuration page offers an autocomplete mechanism when selecting a connectivity adapter.

The autocomplete feature was designed to:

- ensure that all the known parameters are used according to predefined specifications
- help user choose between the possible values for a parameter, rather than typing the value
- avoid duplicates, unwanted blank spaces, misconfigured parameters and incorrect values
- speed up the process of adding or modifying a parameter

See a general description in Section 5.4.8.2, "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 Start Automatically is checked, at this case it will be started automatically at next CSTA service startup.".

CSTA Login GUI

Harmonizing the OpenScape 4000 CSTA Login GUI is also part of V8R2 enhancements. The Login was customized so it would look like OpenScape 4000 Portal Login. For login credentials see Section 5.4.6.1, "Advanced Configuration".

Figure 24: OpenScape 4000 CSTA Login GUI (V8R2)

The suspension page was also adapted to the V8R2 login.

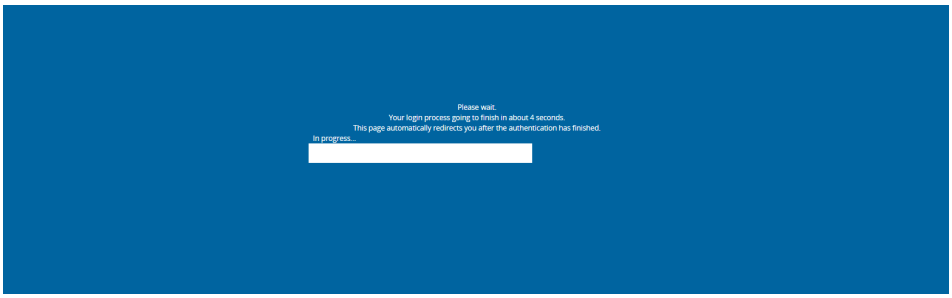


Figure 25: OpenScape 4000 CSTA Suspension page (V8R2)

5.4 CBAdmin – Configuration and Management

5.4.1 Connectivity Adapter Instance

Log on to **OpenScape 4000 V10 Assistant** and select **Expert Mode > CSTA**

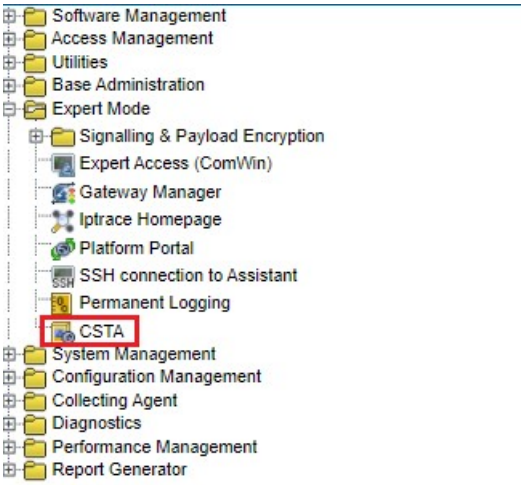


Figure 26: Connect to OpenScape 4000 CSTA

The **Connectivity Adapter** instance **Default** is created and configured automatically during the installation.

Starting with V10, the Connectivity Adapter name is displayed without the **CA4000_** prefix. The database and the logging still use the prefix.

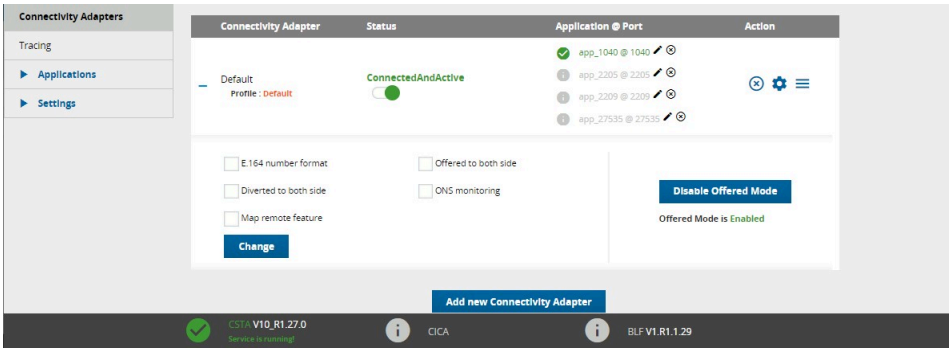


Figure 27: OpenScape 4000 - CSTA main page

To display the default connection parameters, press the  icon found under the **Action** column.

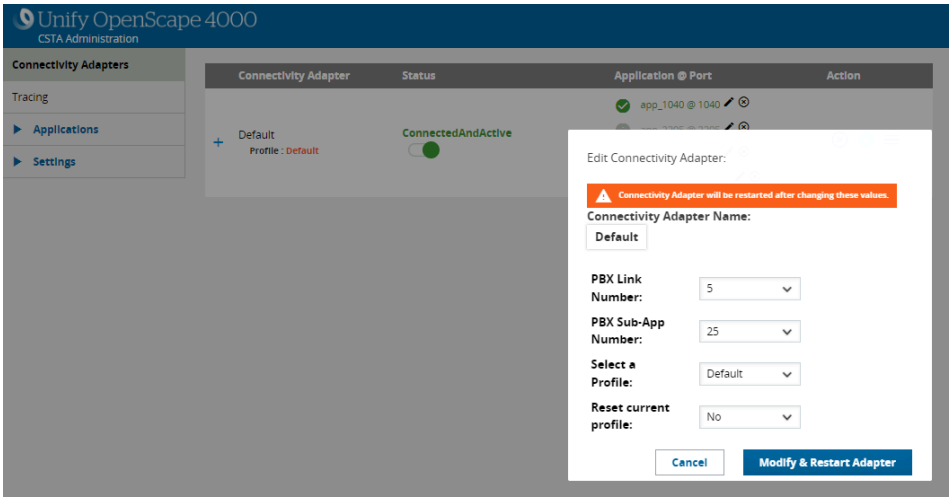


Figure 28: Edit Connectivity Adapter

To view the extended parameters, press the + icon next to the **Connectivity Adapter**.

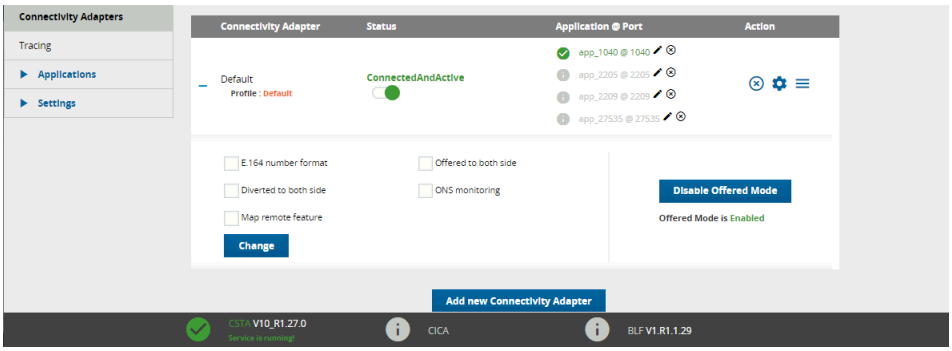


Figure 29: Connectivity Adapter extended functionality parameters

The default connection parameters are:

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

Configured applications:

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

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

A new **Connectivity Adapter** instance can be connected only to the same OpenScape 4000 V10.

To add a new **Connectivity Adapter**:

1) Enter the name of the new **Connectivity Adapter** instance. Note that starting with V10, the Connectivity Adapter's name must not exceed 20 characters. Existing adapters are not affected.

2) Select an available **PBX Link Number** and **PBX Sub-App Number** to configure the ACL Link.
3) Select the **Default** profile or the profile that matches the application to be configured to this Connectivity Adapter.
4) Click **ADD**.

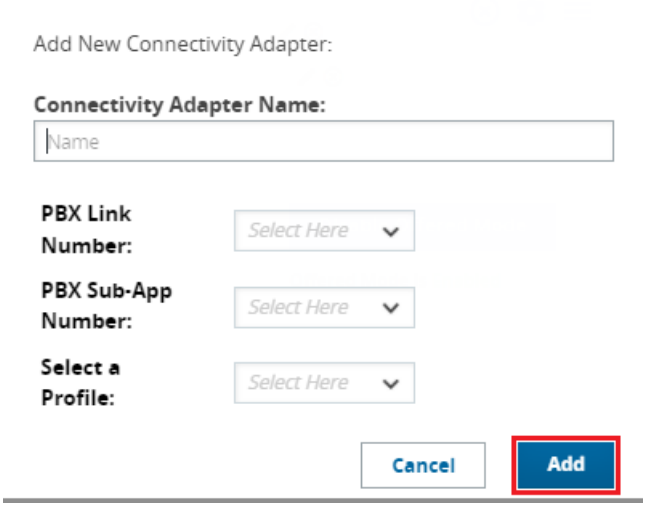


Figure 30: New Connectivity Adapter example

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

To add a new OpenScape 4000 CSTA **Application** link:

1) Click on **Add new application**.
2) Enter the new **Application Name**.
3) Enter a new and not yet existing (not used) TCP-Port in the **Application Port** field.

   The new **Connectivity Adapter** instance listens on the given port and only one OpenScape 4000 CSTA application can establish a link to this port.
4) Click **ADD**.

The new application link is displayed in the **Connectivity Adapter** main page on the column described as **Application @ Port**.

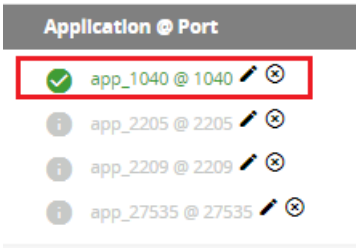


Figure 31: Configuration - New application added

5.4.2 Status – Connection Check

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

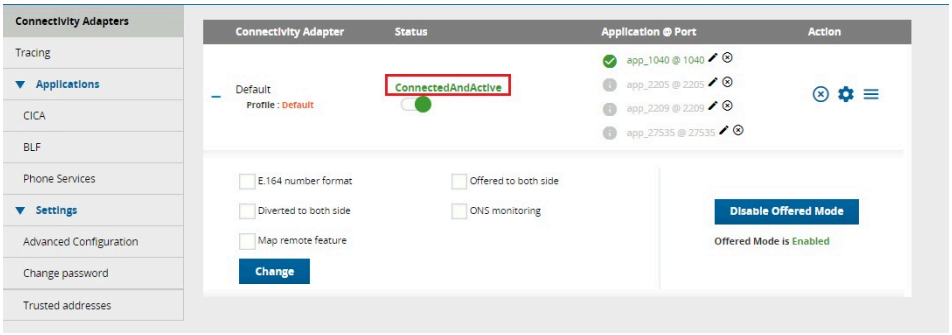
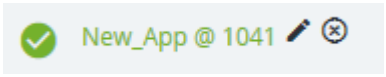


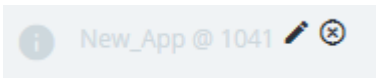
Figure 32: Status - PBX Link

Also, the link status of the application connection is displayed using a specific color:

- Active (green)



- Inactive (grey)



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 its own subfolder named after itself in the Logs/Connections directory (note that in this case the "CA4000_ prefix" is used).

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 since 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 Connectivity Adapter logs

Logging has been changed since V7R2. The former Debug, System and Error logfiles 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.

5.4.3.2 Tracing

Starting with V8R2, and now in V10, all the V8R1 pages located under the Log page are migrated to a new page called **Tracing**.

The **Tracing** page is always visible and offers the possibility to configure the **Advanced Log Properties** directly.

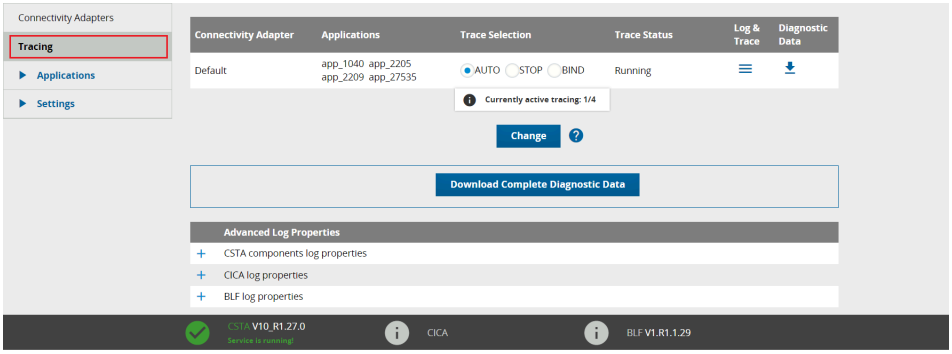


Figure 33: OpenScape 4000 CSTA Tracing

If in V8R1, tracing had to be configured and started for each Connectivity Adapter separately, and it could run only for a limited amount of time, starting with V8R2, tracing configuration is preconfigured and can run continuously.

Tracing can be set simultaneously for maximum 4 Connectivity Adapters.

The Tracing Control table offers an overview of the tracing status and it allows access to logs, traces and diagnostic data.

The **Trace Selection** column offers the following options for tracing:

AUTO

- Default option for every new connectivity adapter
- Tracing starts automatically when the first application connects to the corresponding Connectivity Adapter and stops when the last application disconnects
- It is not persistent after a system reboot (tracing starts after reboot only if an application connects to this connectivity adapter)
- Has less priority than the BIND option when multiple changes are executed on the Tracing page

STOP

- Stops the trace
- Applications can connect to their corresponding ports for this Connectivity Adapter, but the tracing will not start
- If an application is connected to a Connectivity Adapter and the tracing is stopped and then the Trace Selection is switched to AUTO or BIND tracing will automatically start if the limit is not reached

BIND

- Persistent after reboot
- Tracing runs continuously
- Counts as running even if the Connectivity Adapter is stopped

The **Trace Status** column is displaying the actual state of the tracing for the corresponding Connectivity Adapter:

for AUTO

- Waiting for connection (No external application is connected to this Connectivity Adapter)
- Running (External application connected, tracing is running)

- Limit reached, connected but not tracing (If this status is displayed, it means that the trace limit was exceeded and it's already running for other 4 Connectivity Adapters)

for STOP

- Permanently stopped (Tracing is not running)

for BIND

- Running, waiting for connection (Tracing is running, but no external application is connected to this connectivity adapter)
- Running (Tracing is running, applications are connected to this adapter)

For an overview of the available tracing spots (there are maximum 4 available) an indicator is visible below the Change button (Currently running: <Number of running traces>/4).

If by any reasons a Connectivity Adapter is stopped, then the tracing option will be kept. Taking this into consideration, if the trace selection was BIND when the connectivity adapter was stopped then the trace must be manually switched to STOP or AUTO to free this tracing spot.

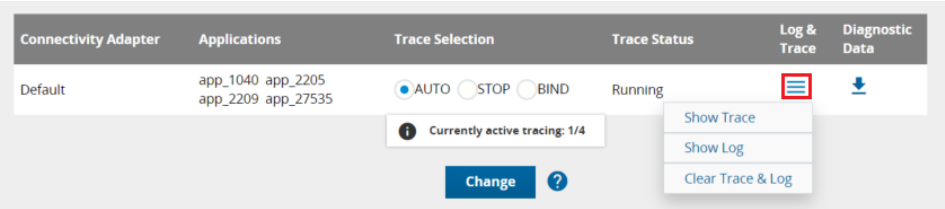


Figure 34: Log & Trace

By placing the mouse over the  icon, the **Log & Trace** menu is displayed. This has the following options:

- **Show trace** - display the current trace in a pop-up window.
- **Show Log** - display the current log in a pop-up menu
- **Clear Trace & Log** - clears the content of the log and the trace.

Enabling auto refresh is still possible.

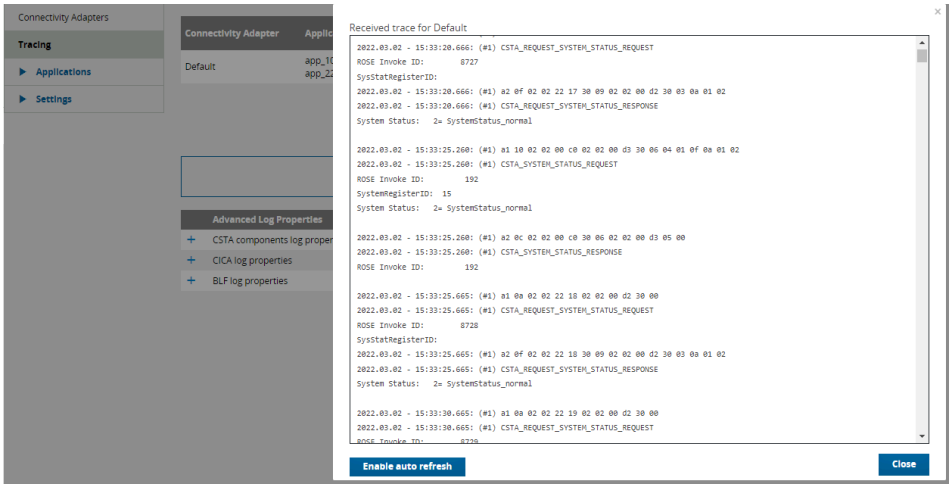


Figure 35: Displaying the log

The **Download Complete Diagnostic Data** button is downloading both configuration and logs for all connectivity adapters. A custom download button  is also available for each connectivity adapter. In this case, the content of the archive is comprising of the corresponding logs and traces for that connectivity adapter and the configuration of the CSTA.

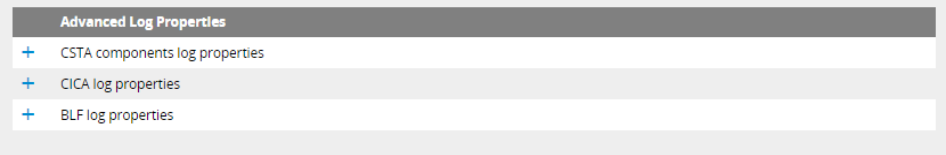


Figure 36: Advanced Log Properties

All the other logging properties corresponding to CSTA and its components (CICA and BLF) are now part of the **Advanced Log Properties**table and can be extended individually depending on the requirement, by pressing the + sign next to them.

File size must be specified in MB.

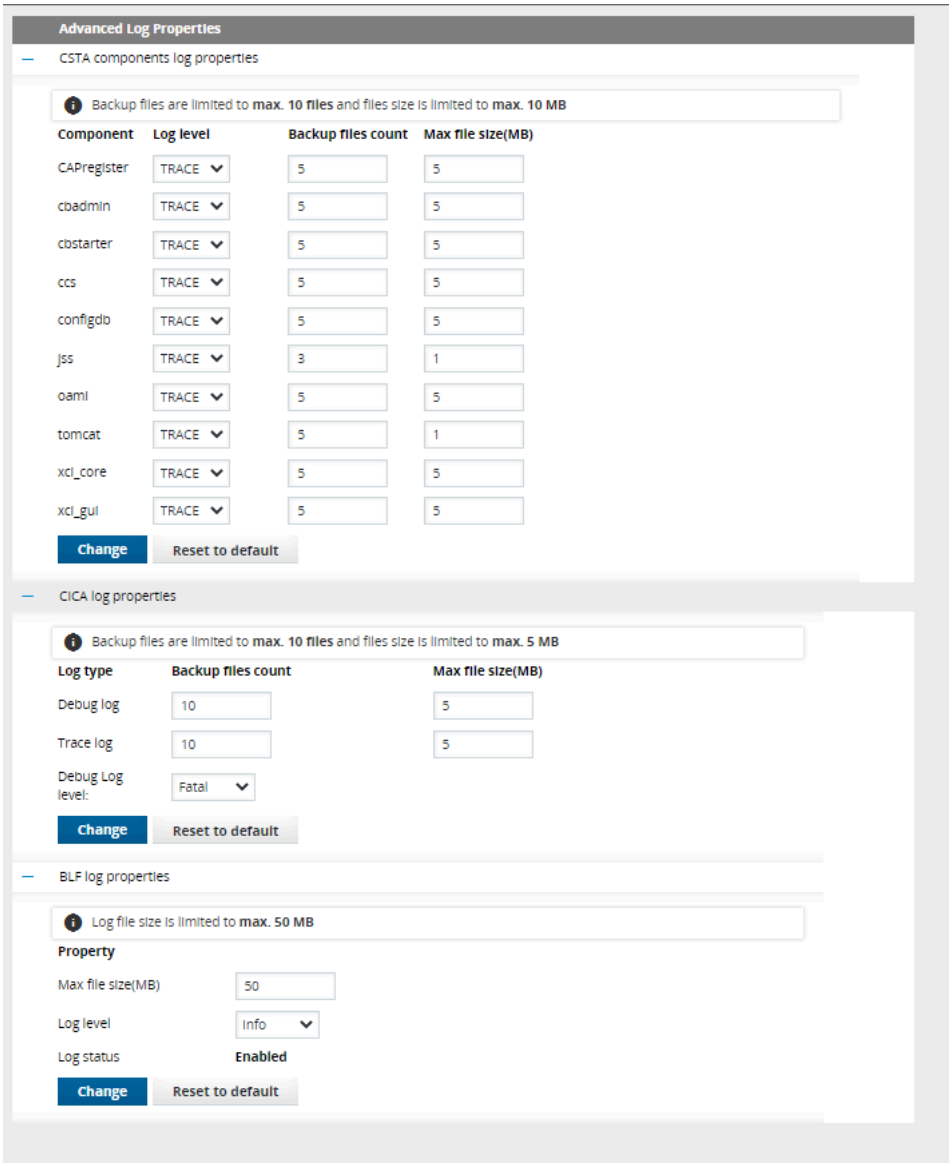


Figure 37: Tracing - Advanced Log Properties

5.4.4 Statistics

Detailed information about ACL/CSTA is shown in the **Statistics** pop-up window, which can be reached from the Connectivity Adapters page using the menu next to each Connectivity Adapter.

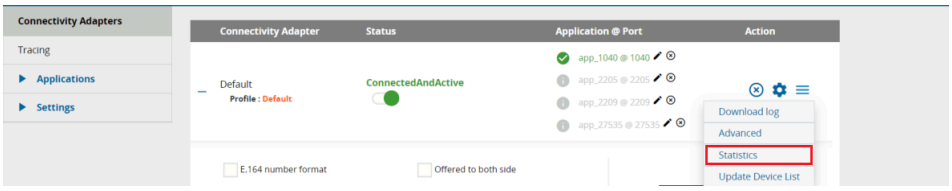


Figure 38: Actions available for a Connectivity Adapter

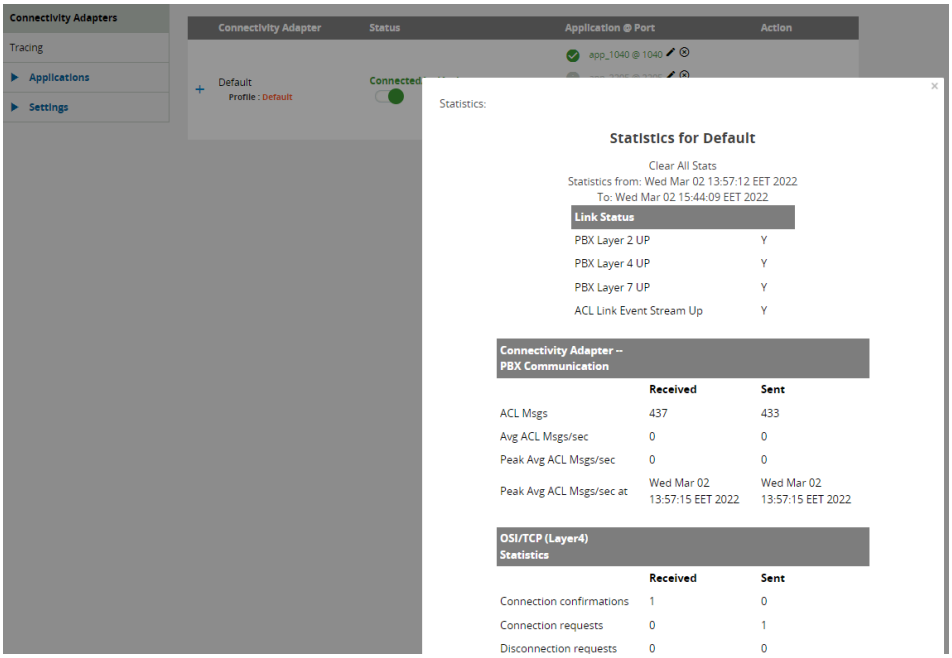


Figure 39: Statistics

- **Link Status**

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

  Definition of the fields:

  Statistics - Link Status” section

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.

Field	Explanation
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.

- **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:

  Statistics - “PBX Communication” section

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.

- **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:

Statistics - “Application” section

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.
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.

Field	Explanation
Peak Avg CSTA Msgs at	The date and time peak when CSTA message traffic occurred.

- **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.

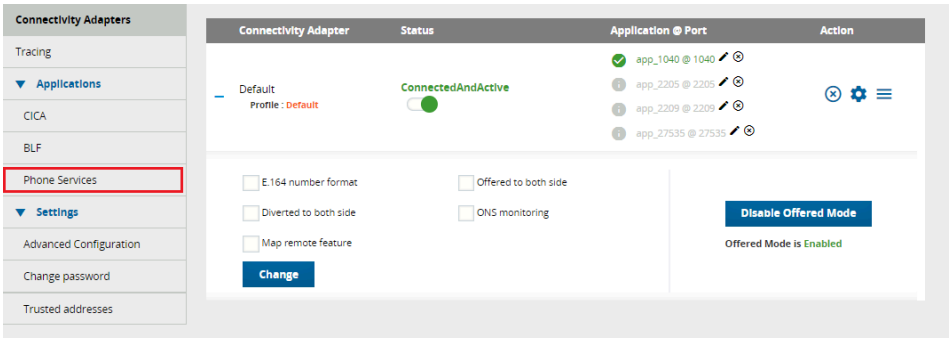


Figure 40: Phone Services UI

NOTICE: This will be explained in Chapter 6, Section6.5, “Configuration”

5.4.6 Settings

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

5.4.6.1 User/Password

At the initial installation, the default credentials are Admin/Admin. You can change the default user and password, as seen below.

NOTICE: 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 Assistant’s page again.

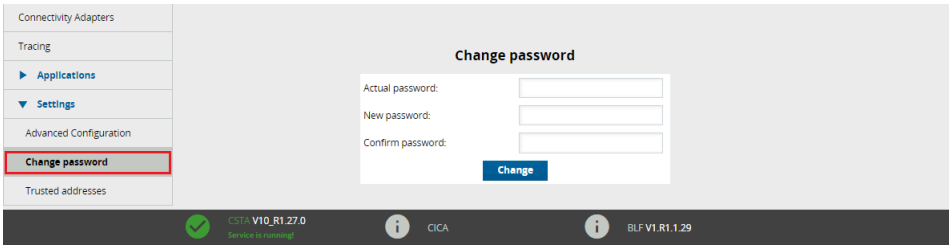


Figure 41: Change default user and password

5.4.6.2 CBAdmin – Trusted IP Addresses

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

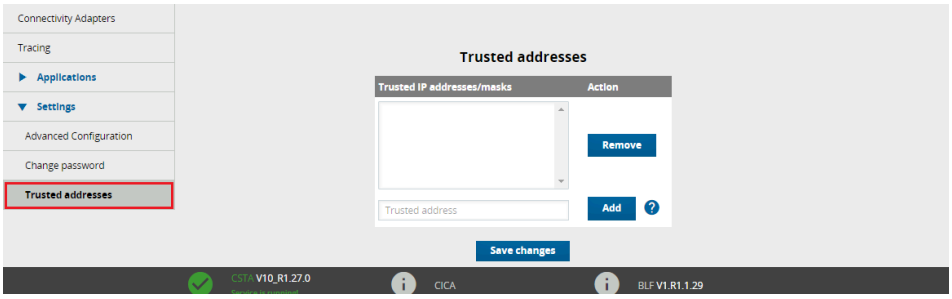


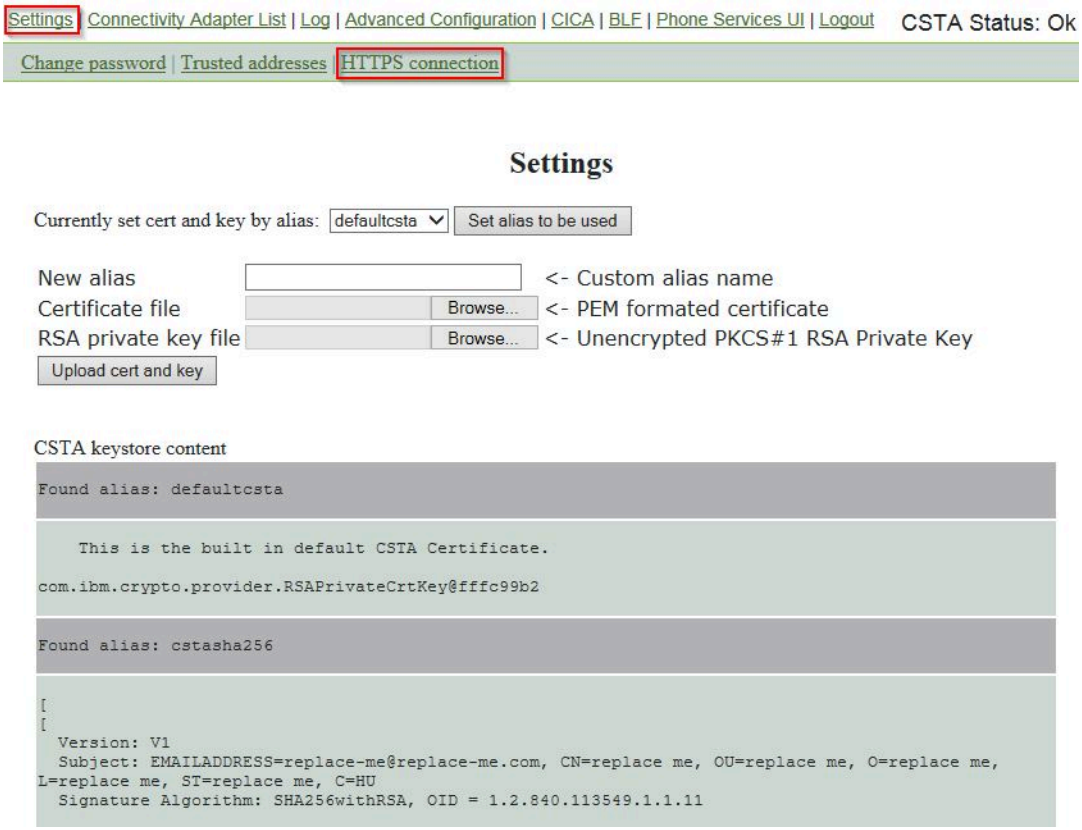
Figure 42: Trusted IP addresses

The IP addresses and/or ranges in this list are able to communicate with the RMX platform through the OpenScape 4000 CSTA. 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.



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.

NOTICE: In case of OpenScape 4000 V8 integrated OpenScape 4000 CSTA, the CBAdmin 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 V8 R1 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.

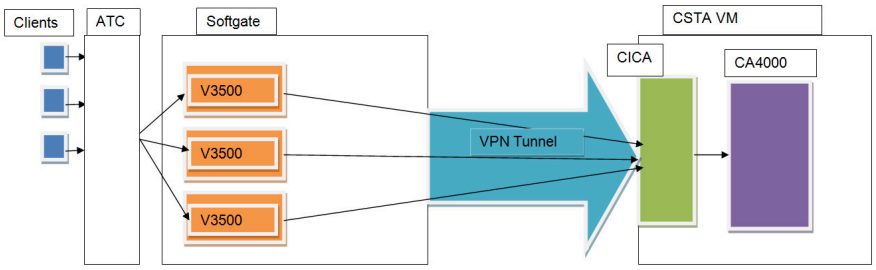


Figure 43: General architecture of the circuit connection

5.4.7.2 Configuration

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

Starting the CICA application implies that CICA starts automatically at CSTA service start. This is the normal functionality of the application, in case of Circuit connectivity it needs to be set.

The status of the CICA application can be seen in the status bar at the bottom of the page. A possibility of manual starting and stopping is added. The process can be stopped manually, but in this case it will not start automatically at the next CSTA service backup.

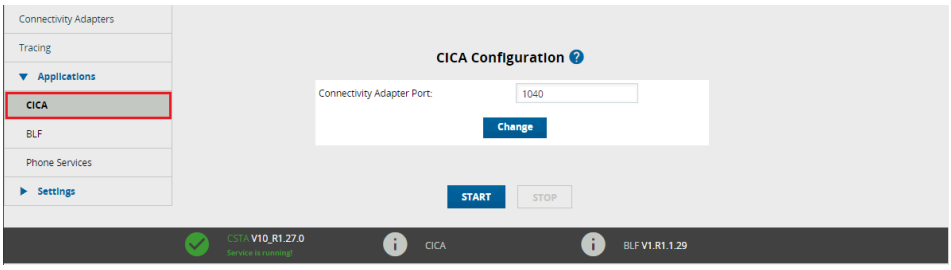


Figure 44: CICA configuration page

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.

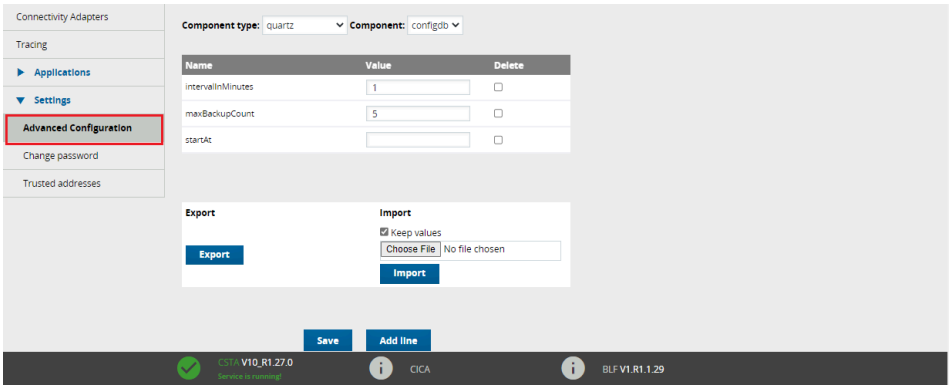


Figure 45: Advanced Configuration - Component selection

Structure of the page:

Two list boxes are on the top of the page, which can be used to select the configuration type (**Component type**) and the configuration (**Component**) to be edited. After the selection, the page will reload and it will show in a table only the available configuration parameters and values. You can modify, delete or add entries.

You can also apply all 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**

  Click on the **Add line button** to add a new setting, which will appear in the configuration. Fill in the name and the value. The modification will be

maintained after **Save**. If the new line was added my mistake, then you can delete it (before saving it) using the **Delete** button in the last column.

Starting with V8R2, an autocomplete functionality is available when using Advanced Configuration to edit a Connectivity Adapter.

The Autocomplete mechanism was implemented for all the optional parameters. If one of the known optional parameter is missing it means it was already configured.

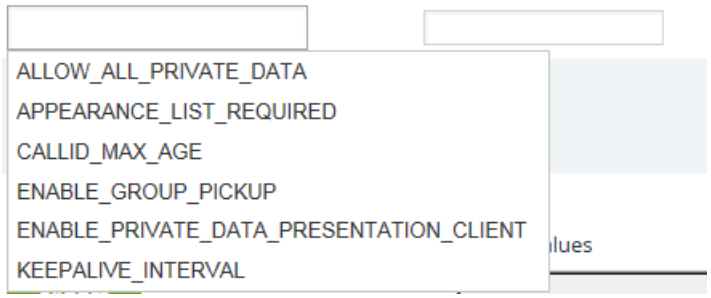


Figure 46: Advanced Configuration - New parameter

Modifying an existing parameter is also possible with the help of the autocomplete functionality:

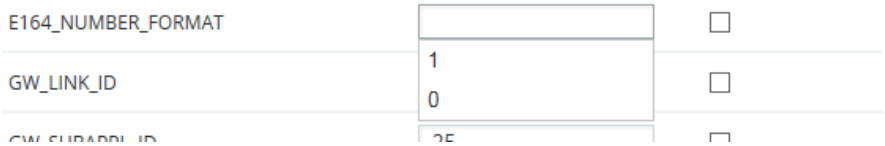


Figure 47: Advanced Configuration - Modify parameter

Save

After pressing **Save**, the values of the configuration parameter are saved/ deleted in the configuration database. The processes will identify 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. Note that duplicates are not allowed, extra white spaces are also forbidden and known parameters are restricted to a certain predefined format. If all the conditions are met then saving is allowed.

Export/Import

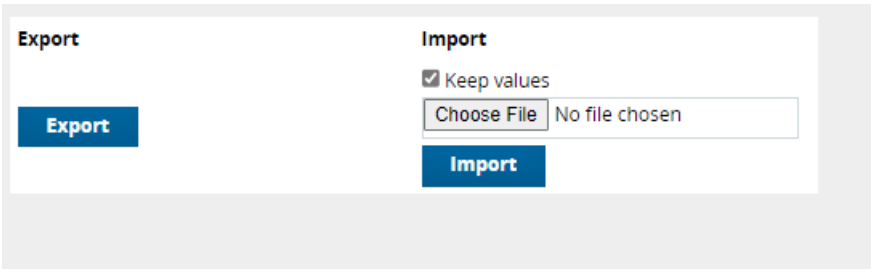


Figure 48: Advanced Configuration - Export/Import

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. The files that correspond to the related component are located in these main directories.
- **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 you need to restart the OpenScape 4000 CSTA service and the tomcat service. If the configuration type is **ca4000** it is enough to restart the **Connectivity Adapter**. The application offers the possibility to restart it (or you can do it later manually).

5.4.9 Integrated BLF Server (iBLF)

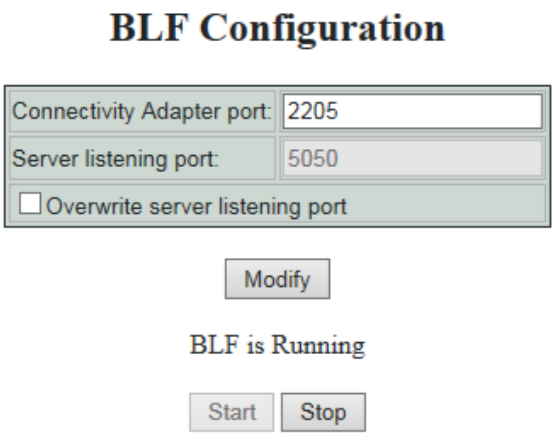
5.4.9.1 Accessing the iBLF Menu

The configuration can be done from the CSTA web based management by logging on to the OpenScape 4000 Assistant and selecting: **Expert Mode > CSTA**.

The CSTA menu contains a new link, BLF, located next to CICA and it is available with or without selecting a Connectivity Adapter:

The following submenu will be available after accessing the BLF web page.

5.4.9.2 BLF Configuration



Connectivity Adapter port

This field allows users to change the Connectivity Adapter port used by the integrated BLF Server to connect to the cbdriver. This application port and the corresponding Connectivity Adapter must be configured and available.

Server listening port

The server listening port value must be unique. CA applications should not use this port. The port is required by the BLF Client for communication with the integrated BLF Server.

There is an option to overwrite the server listening port by checking the checkbox next to this option, but it must be used with caution because the port must be available.

Modify action

Button "Modify" will submit the values for the "Connectivity Adapter port" and the "Server listening port".

NOTICE: If at least one of the values is new, then a restart will be triggered for the BLF Server.

BLF Status and actions

There are 2 possible values for this field:

1) BLF is Running (only Stop action is possible)

2) • BLF is not Running (only Start action is possible)

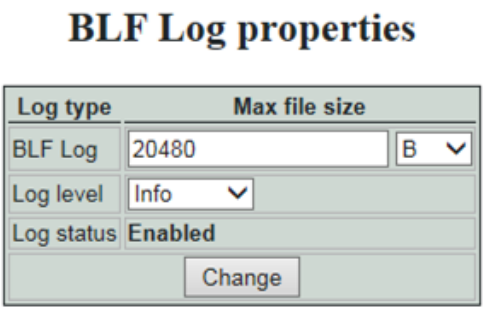
All the actions are followed by a response below the "BLF Configuration" title:

Modify	
"BLF configuration already present"	The user submitted the same existing values
"BLF configuration updated"	A valid change was made in the configuration

Start/Stop	
"BLF successfully started!"	BLF Server was started
"BLF successfully stopped!"	BLF Server was stopped

5.4.9.3 BLF Log Properties

BLF Log



Value must be smaller or equal to 10 MB. If the unit is changed, then the value must be manually adjusted. Possible units are B, KB and MB.

Log level

Possible log levels are:

- Info
- Debug
- Warning
- Error
- Fatal
- OFF - will disable logging

Log status

Possible values:

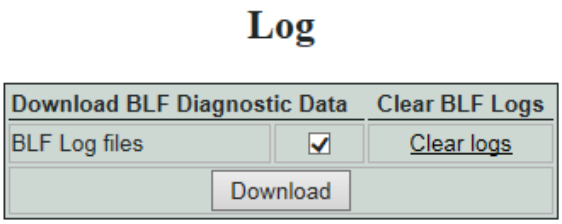
- Enabled - any other log level, except OFF, will enable the logging
- Disabled - set Log level to OFF

All the actions are followed by a response below the "BLF Log properties" title

Change	
"BLF logging was disabled!"	Log level was set to OFF => Logging was disabled.
"BLF log properties updated successfully!"	Change action was successfully, no errors occurred.

5.4.9.4 Download

Download action



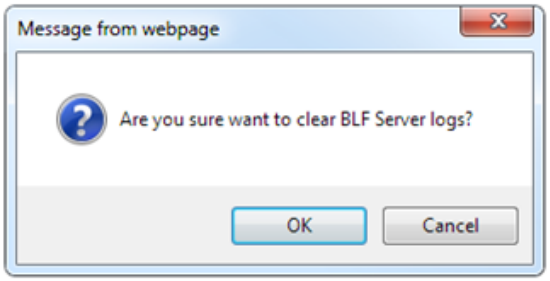
By clicking the Download button, the BLF logs will be downloaded as a zip file.

The zip filename starts with BLFSysdiag and it's followed by the IP and current date of the CSTA.

The checkbox must be kept checked.

Clear logs action

After clicking the Clear logs link a message box will appear requesting confirmation for deleting the logs. Log files will be deleted if the question in the message box is confirmed.



Confirmation message will be displayed below the Log title: "BLF Logs were cleared successfully!"

5.4.9.5 Version

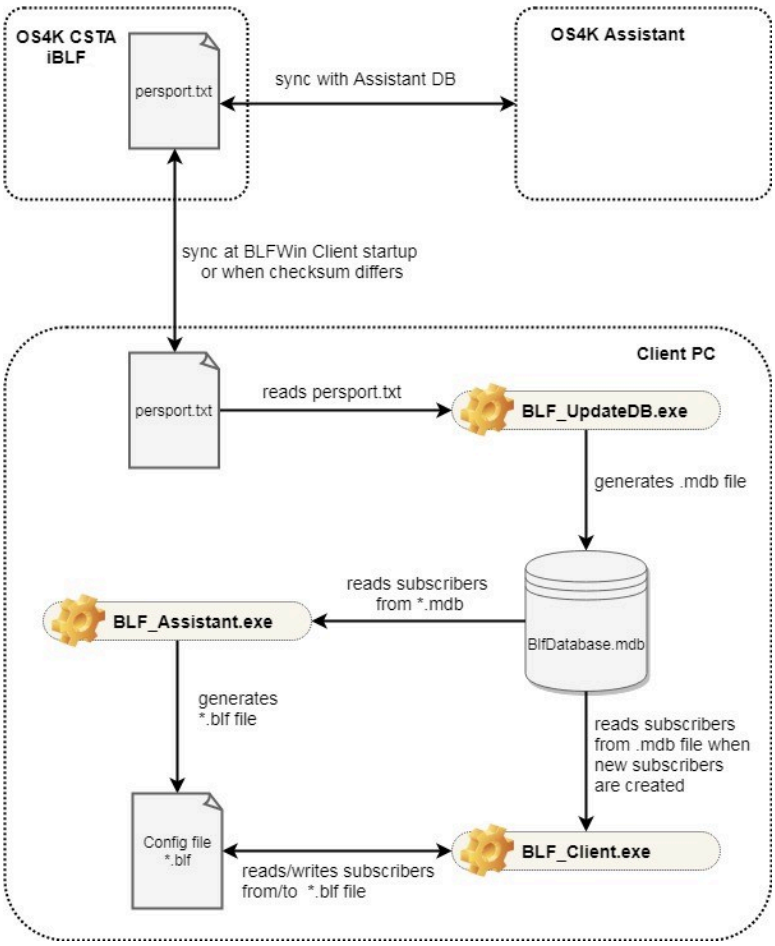
BLF Version

The current BLF server version is displayed.

If the version can't be identified, it is possible that the version file is missing and a BLF Server restart is required.

5.4.9.6 iBLF synchronization

Integrated BLF can synchronize with OS4K Assistant database regarding subscribers' information. An initial synchronization is performed at each iBLF startup, and then periodically, every day, at a configurable time. In case of a successful sync, the output is stored in a local file, i.e. persport.txt, which contains the following fields: displayname, isdn_cc, isdn_ac, isdn_lc ,vnac, extension. These fields are extracted from the PERSPORT table within OS4K Assistant using a built-in user, i.e. xpr450, to connect to the XIE interface using api2hipath module. A checksum is performed for each database after a successful sync.



iBLF synchronization with Assistant database

NOTEs:

- Synchronization parameters, e.g. time of sync, are stored in blf_config file at the following path on the CSTA machine: /opt/blf/ .
- File persport.txt is stored at the same location as well.
- Currently, vnac field is not handled in this configuration. It is however saved for future use.

5.4.9.7 Handling on BLF-Win client's side

At startup, immediately after establishing the connection to iBLF, each BLF-Win client will receive the persport.txt file in < Database Path >, i.e. C:\ProgramData\BLF\Database. Based on the file's checksum, it will be updated by iBLF if there are any changes in Assistant's database. An application, i.e. BLF_UpdateDB.exe, that runs as background process on client's PC will take persport.txt as input and create BlfDatabase.mdb in < Database Path >.

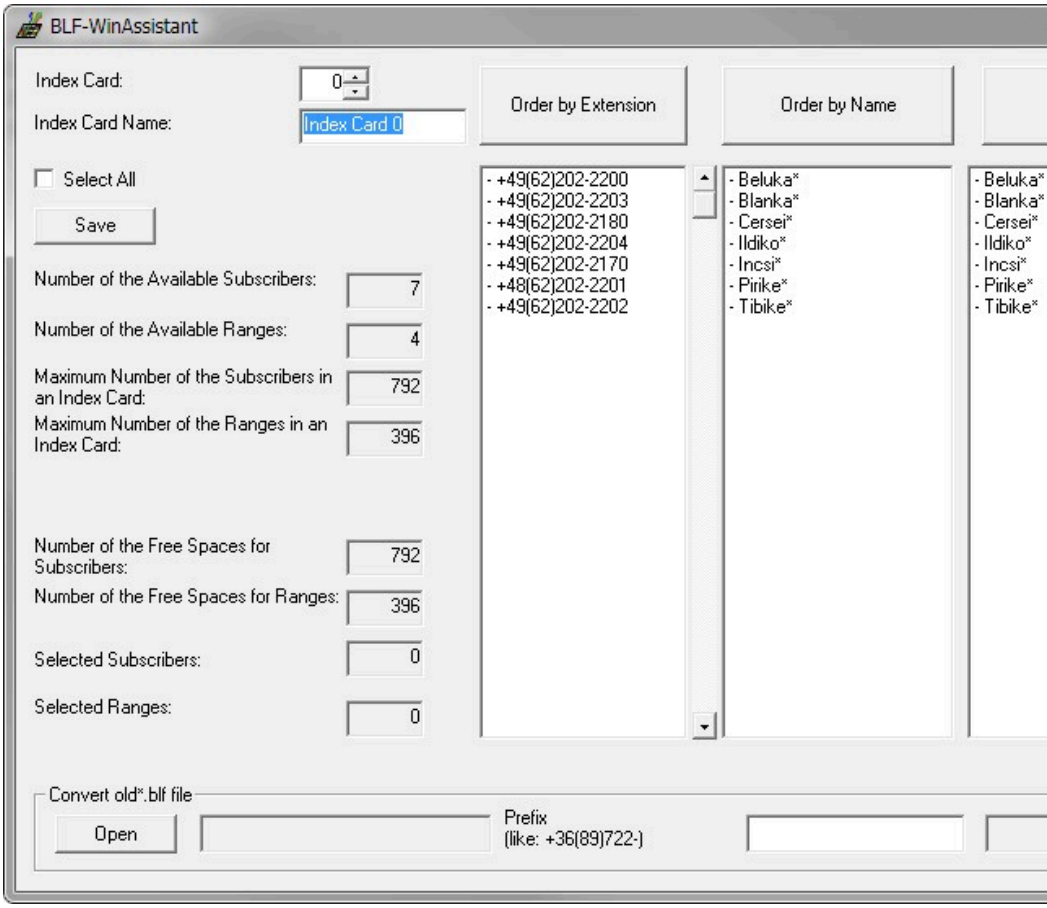
Using BLFWinAssistant.exe, the user can create an initial BLF-Win config file (i.e. *.blf) based on the BlfDatabase.mdb database. BLFWinAssistant.exe will automatically load the existing BlfDatabase.mdb file present at < Database Path >. User can define how many index cards will be created and which extensions (or extension ranges) will be monitored by BLF.

Once the *.blf file created at the previous step will be loaded, BLF-Win client will use both config file and BlfDatabase.mdb for subscribers' handling.

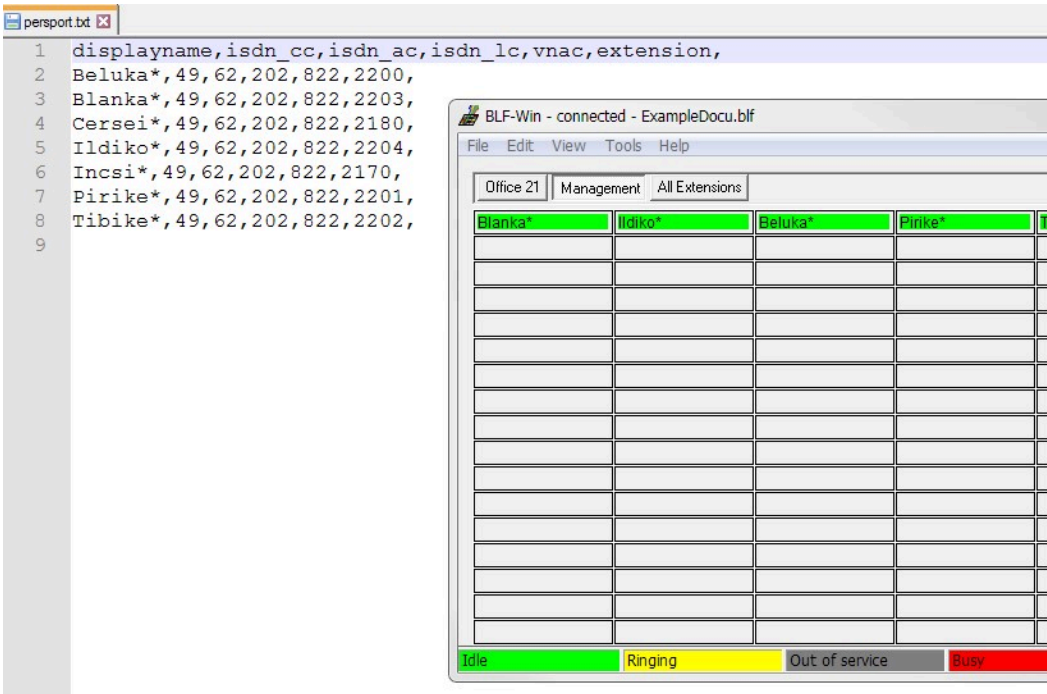
5.4.9.8 Using BLF-Win Assistant

BLF-Win Assistant loads BlfDatabase.mdb and fills the list boxes with information provided by the database (Figure 77). For example, to create a *.blf file (Figure 78) with 3 index cards, the following steps are necessary:

- Select Index Card 0 and define a name for it, e.g. Office 21;
- Select which subscribers you want to add for this Index Card;
- Increase Index Card to 1 and define its name, e.g. Management;
- Select subscribers you want to add in this Index Card;
- For 3rd Index Card define a name, e.g. All Extensions and select all ranges from the last column;
- Click Save button to save a new *.blf file;



BLF-Win Assistant

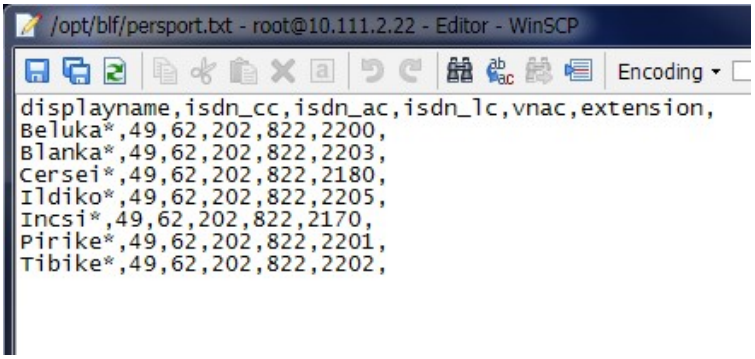


Resulted *.blf configuration file based on persport.txt

5.4.9.9 Example of synchronization

Let's assume the initial content of persport.txt file is as shown in Figure 79. Using BLFWin Assistant, user will generate Init2.blf config file by selecting all subscribers and click on Save (Figure 80). This new generated configuration file will be eventually opened in BLF-Win Client (see Figure 81) and all subscribers will show their status.

If a new subscriber is added in Assistant database, after a successful synchronization between iBLF and Assistant, all changes will reflect in persport.txt (see Figure 82). In BLF-Win client, when adding the new subscriber's number, it will automatically sync with the database (Figure 83).



Initial content of persport.txt

5.4.10 Additional Supported Services via OpenScape 4000 Assistant

After log in on to **OpenScape 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**

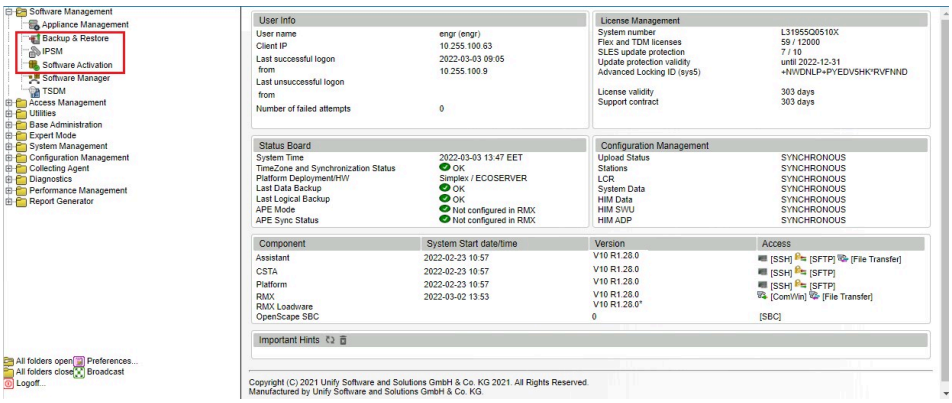


Figure 49: Connection to Backup & Restore, Software Activation/Transfer

Backup & Restore

The configuration parameters related to CSTA can be stored selectingBEER_CSTA (CSTA configuration) on the Backup/Restore GUI, menu item Backup, see Figure 51 on Page 53. The selected one of the stored

backups can be restored using menu item Restore. Compatibility related topics should be checked in the Release Notes.

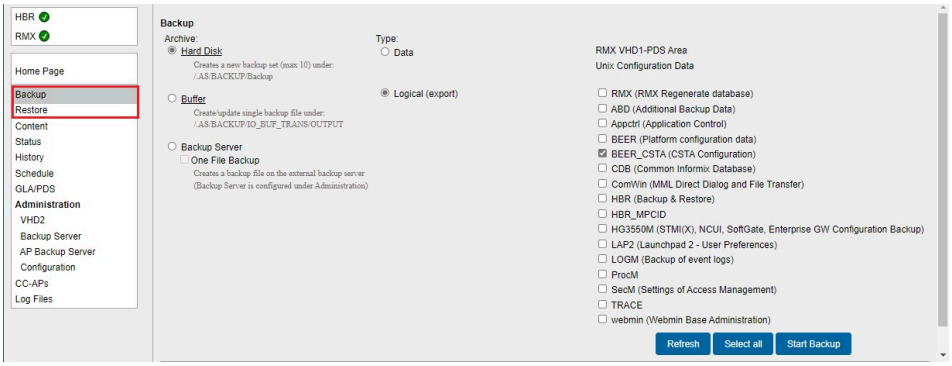


Figure 50: Backup & Restore - BEER_CSTA (configuration)

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 5.4.8.2,"A status field is also added, it checks the process's status whenthe page is reloaded. A possibility of manual starting and stopping isadded. The process can be stopped even if Start Automatically is checked,at this case it will be started automatically at next CSTA service startup.". We summarize these settings here.

5.4.11 Special Settings

5.4.11.1 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.
- **special**: similar to the function of **normal** but instead provides possibility for the OpenScape ProCenter (and OpenSape 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>

NOTICE: 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.

5.4.11.2 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.

5.4.11.3 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;

NOTICE: 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.

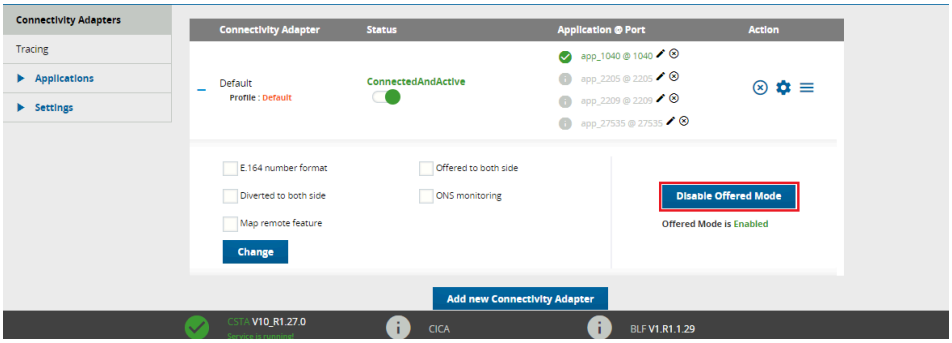


Figure 51: Change the Offered Mode

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 examle for it on Figure 32 on Page 35.

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 controll of the switching function after a 2 seconds timeout and the device starts to ring.

5.4.11.4 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 29 on Page 33) or using the CA's Advanced Configuration page (see Figure 44 on Page 48), 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 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.

5.4.11.5 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.

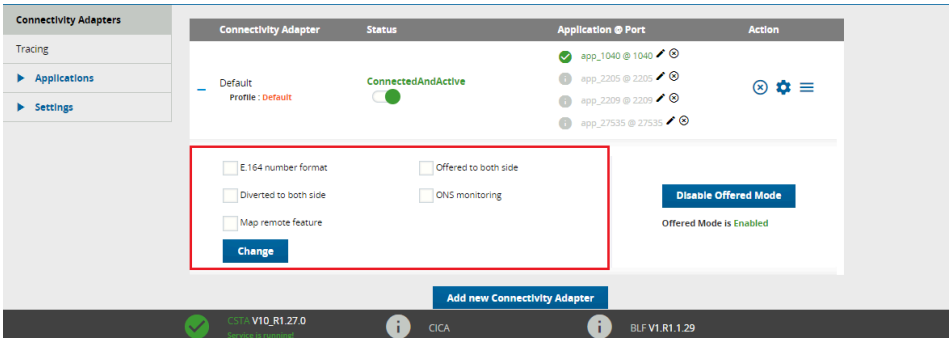


Figure 52: Extended functionality on the GUI

OFFERED and DIVERTED events for the calling side

OpenScape 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 Diverted 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 elemet 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

TheOffered 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.

5.4.11.6 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.

The **throttle** mechanism is used to prevent flooding.

This mechanism is activated by default and can be configured by setting the **THROTTLE** parameter in **Advanced Configuration**.

Behavior:

- Default: 30 requests are allowed within an interval of 1 second (e.g. THROTTLE has value 30)
- Configurable: via the THROTTLE parameter in Advanced Configuration
  - if THROTTLE = 0, then the mechanism is disabled (not recommended)
  - if THROTTLE > 100, then the maximum value of the parameter is 100.

    Therefore, if the value of the parameter is higher that 100, it will be set 100.

When the throttle mechanism is activated, a log entry is generated and the following message is displayed: "Too many requests sent, throttle mechanism activated thread:xxxxxxx".

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

Multiline appearance (keyset) monitoring is not supported in OpenScape 4000 CSTA V8 R1.

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:

1) ALLOW_PHYSICAL_APPEARANCE = 1

This feature is inactive by default.

5.4.11.8 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 5.4.8.2, “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 Start Automatically is checked, at this case it will be started automatically at next CSTA service startup.”) to "de-umlaut" them. This activates a conversion from CORNET TS characters to latin ascii.

1) 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.

5.4.11.9 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 furhter details.

5.4.11.10 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:

1) 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.

5.4.11.11 Usage with OpenScape 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

5.4.11.12 Static OND

Static OND is a feature used by OpenScape Contact Center. In case static OND is set for a station all applications which are monitoring that station will receive by default staticOND value as private data in CSTA FORWARDING EVENT and CSTA GET FORWARDING RESPONSE.

In order to be able to deactivate Private data from CSTA FORWARDING EVENT and CSTA GET FORWARDING RESPONSE a new flag DISABLE_STATIC_OND was introduced in CSTA.

Possible values:

- DISABLE_STATIC_OND=0 (default)
- Static OND is reported as private data in CSTA FORWARDING EVENT and CSTA GET FORWARDING RESPONSE
- DISABLE_STATIC_OND=1
- Static OND is not reported as private data in CSTA FORWARDING EVENT and CSTA GET FORWARDING RESPONSE

5.4.11.13 Shared-Bridged Appearance

Shared-Bridged Appearance feature refers to OpenScape 4000 keyset (multiple appearance) feature

In order to activate support of OpenScape 4000 CSTA Shared-Bridged Appearance, set APPEARANCE_LIST_REQUIRED flag to YES in Connectivity Adaptor Advanced Configuration.

5.5 Fault management

In V8 R1 OpenScape 4000 CSTA was enhanced to support and use the system's SNMP services. A SNMP syslogagent is installed on the CSTA. 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 are generated from events that are not requested by GUI, i.e. probably not the effects of human interaction. This incluides starting or stoopping 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 Sesvices applications provided together with OpenScape 4000 CSTA and therefore also with OpenScape 4000 V8. 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 53: 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 a 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

> **NOTICE: 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 54: 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!!”

NOTICE: 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 55: 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).

NOTICE: 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 56: 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**
- Change the availability of the user **UC Status**
- Search in the UC database or in the user's UC contact list (UC Lookup)

NOTICE: In the case of the connected call status, the contact data are shown based on the phone number of the active call. If OpenScape 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 57: 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 V8

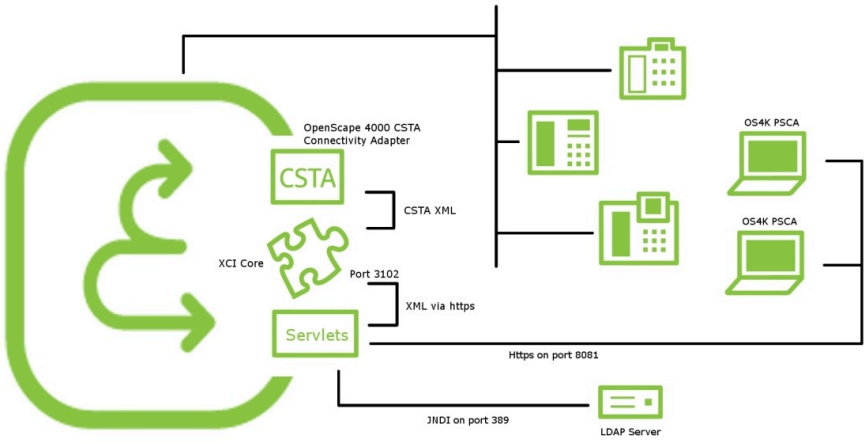


Figure 58: Single connected OpenScape 4000 CSTA (OpenScape 4000 V8)

Administration URLs – in case of OpenScape 4000 V8 integrated variant

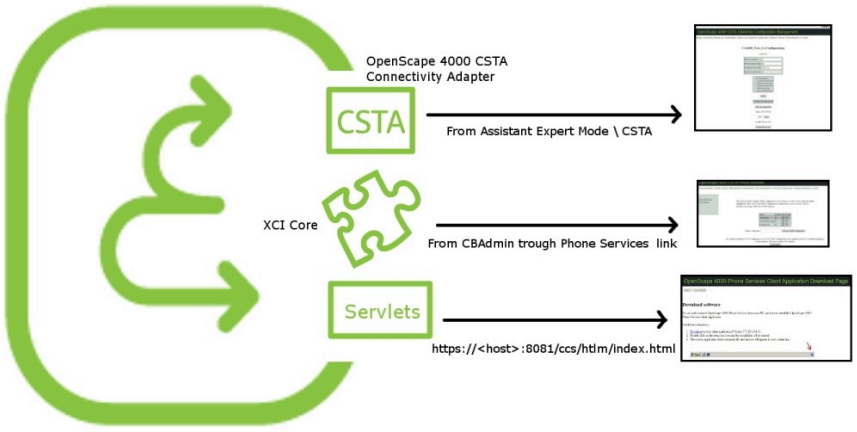


Figure 59: Administration URLs – in case of OpenScape 4000 V8 integrated variant

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

Phone Service URLs

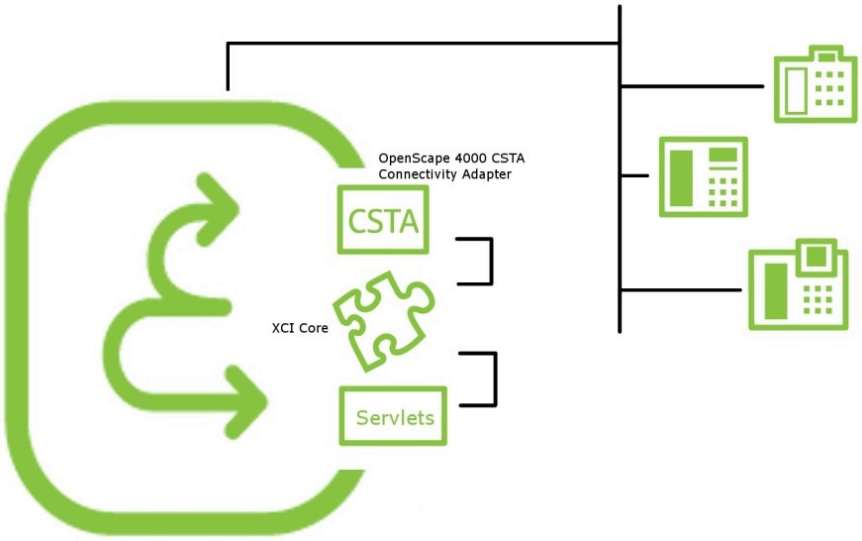


Figure 60: Phone Service URLs

- **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%`

Phone Service XML Service Tray Port - In case of OpenScape 4000 V7 integration 8081

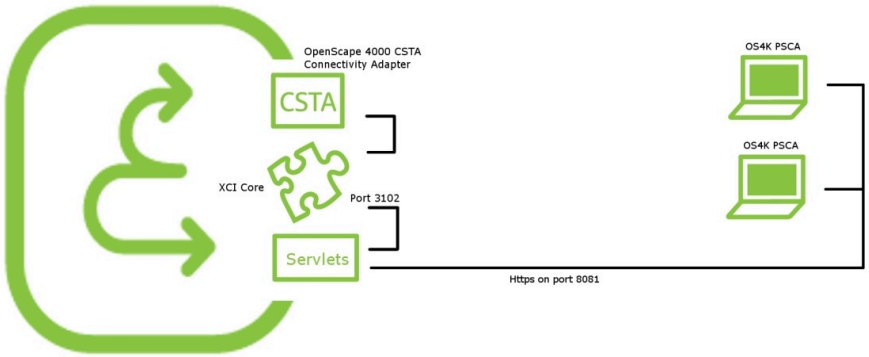


Figure 61: Phone Service XML Service Tray Port in case of OpenScape 4000 V8 integration 8081

6.3 Requirements

Hardware and Software Requirements

- OpenScape 4000 Phone Services is installed automatically together with OpenScape 4000 CSTA
- OpenScape 4000 digital phones with display and cordless phones
- PC (with Windows OS) with the OpenScape 4000 Phone Service Client Application, here after OpenScape 4000 PSCA (previously known as XCITray) application installed; PSCA can be downloaded from the OpenScape 4000 Phone Service Administration Web page.

NOTICE: OpenScape 4000 PSCA is not required for either EasyLookup or EasyUC, however with OpenScape 4000 PSCA the EasyUC functionality provides more enhanced possibilities (e.g.: sending e-mails to the person connected via phone, as with EasyMail).

IMPORTANT: If more than one IOServices are planned to be used on the same OpenScape 4000 system via the same Connectivity Adapter of OpenScape 4000 CSTA (e.g. Phone Services of the OpenScape 4000 CSTA is used, and to the same Connectivity Adapter there is another CTI application connected, which uses IOServices of the switch via CSTA, like COBS of HiPath CAP V3.0), then please consider using different application IDs for each application (e.g: Phone Services with 999 and CTI application with 998). 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 Restrictions

- Performance measurement test proof that in case 2000 Phone Services users configured in the database of OpenScape 4000 CSTA V8 and from those 100 devices.users using simultaneously the Easylookup (open data pathes) then the menu display reaction time is in an acceptable interval (3-4 seconds). This means that 100 data paths can be used at the same time.
- Metadirectory interconnectivity not supported.

6.5 Configuration

6.5.1 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.

LDAPS configuration

Enable LDAPS (LDAP over SSLL) support with following configuration steps:

- Activate "LDAP is SSL" checkbox on Phone Service UI (XCI GUI) under "CCS LDAP Configuration".

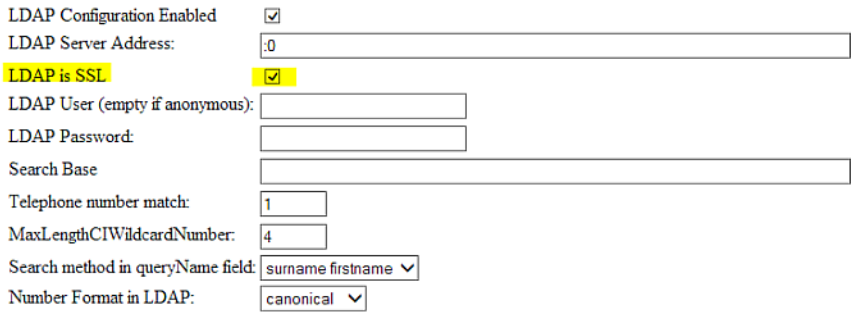


Figure 62: LDAPS Configuration

- CSTA CA Adapter used for XML Phone Services must be extended by parameter “IgnoreLDAPSCertificate” under Advanced Configuration:
  - Choose component type **->ccs_config and component ->ccs_config**
  - Click Add line and add “IgnoreLdapsCertificate” and set the value to “true”
  - Click Save

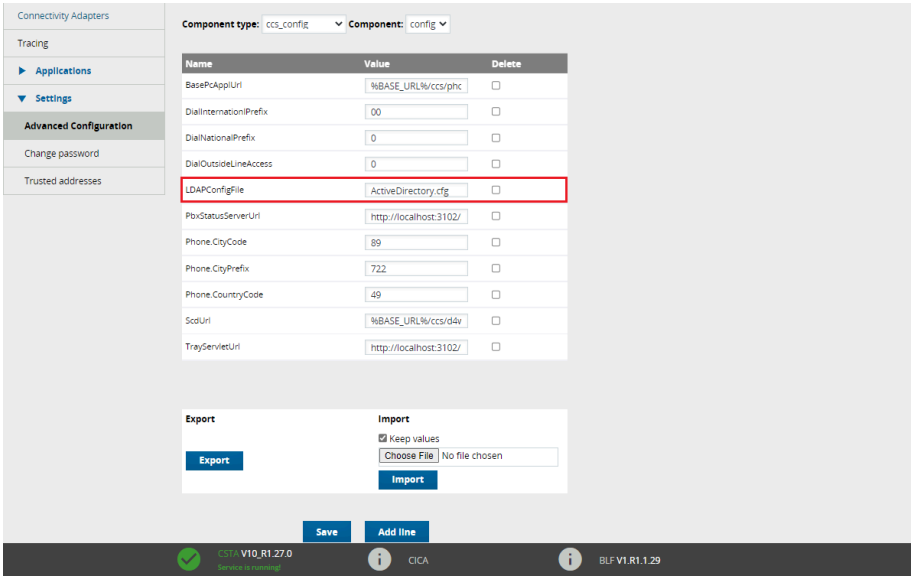


Figure 63: Advanced Configuration

NOTICE: XML Phone Services will accept all SSL certificates (regardless of the issuer) to activate secure connections using SSL.

6.5.2 AMO Configuration OpenScape 4000 V10

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=<devic
[PROTECT=YES];
```

For cordless phones/CMI only the key 13 must be used:

```
ADD-
ZIEL:TYP=NAME,SRCNO=<stno>,KYNO=13,DESTNON=C15C1399913,DEV=<devic
[PROTECT=YES];
```

Usually for the DECT devices is reserved the TAPRO standard 15 and it has the Type of voice terminal = OPTIT12. This standard usually has as first line the below one:

```
CHANGE-
TAPRO:,15,OPTIT12,CH,CBK,CONS,SPKR,RLS,PU,MB,NAME,NAME,CL,NAME,NAME;
```

To use the 13th key, the standard must be changed, and the 13th key must be set as NAME with the below AMO commands:

```
CHANGE-
TAPRO:STD=15,DIGTYP=OPTIT19,KY01=CH,KY02=CBK,KY03=CONS,KY04=SPKR,KY05=
TAPRO:STNO=<stno>,DIGTYP=STDDEV,KY13=NAME;
```

Then add the corresponding ZIEL command for the key 13:

```
ADD-
ZIEL:TYPE=NAME,SRCNO=<stno>,KYNO=13,DESTNON="C15C139913",DEV=BD, ,
[PROTECT=YES];
```

Additional note: if a DECT user needs to use DTB or other applications, then it must use the keys 9 and 11.

NOTICE: 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.

NOTICE: CMI special case: please observe the DeviceType on the Phone Services **UI > Devices.** It must be **CMI**. Also note that the application can be reached using the **INT** button from the DECT device then scroll and select application **Easy Services**.

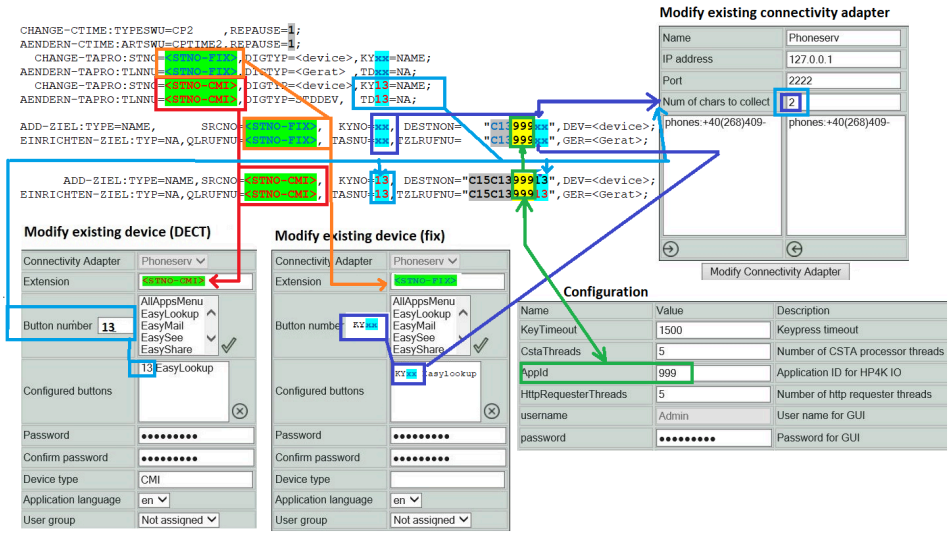


Figure 64: AMO Configuration

6.5.3 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.

NOTICE: Do not configure Easylookup on CA4000 with E164.

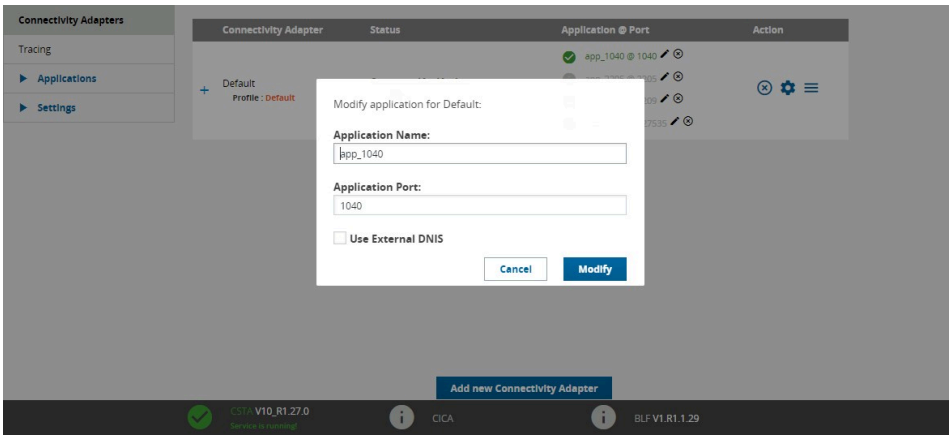


Figure 65: Application

After adding a new port for Connectivity Adapter you can switch to XMLPS via admin section.

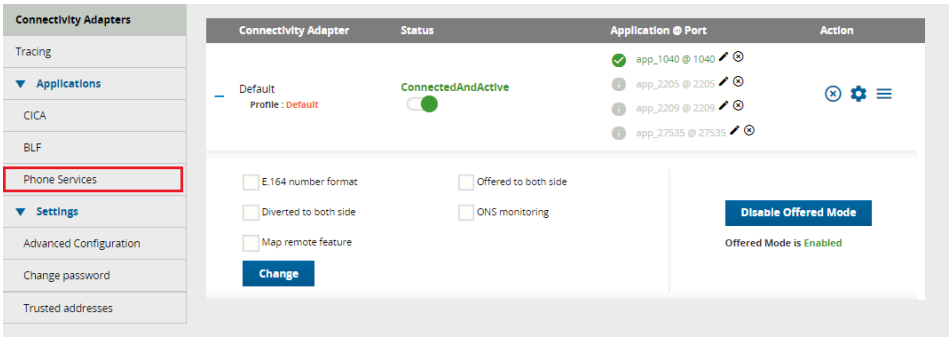


Figure 66: Phone Services UI

First switch to the **Domain** configuration Web page and **Add** at least 1 **domain**.

Multiple domains are supported for one PBX.

Figure 67: 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.

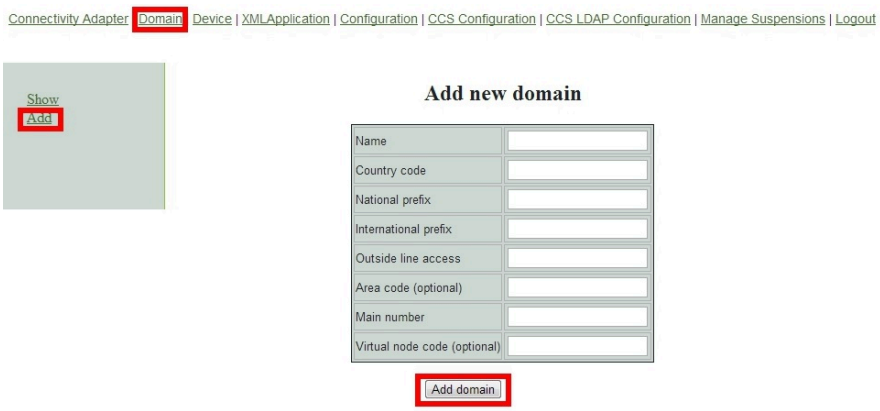


Figure 68: Add new domain

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.**

NOTICE: Virtual node code field is used in case of VNR and digit prefix (ZIVO) where additional digits like VNR code have to be used to convert the canonical format into dialing format. If VNR code was entered in the field Virtual Node Code, then in menu Devices the device number (Figure) must be without the VNR code.

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

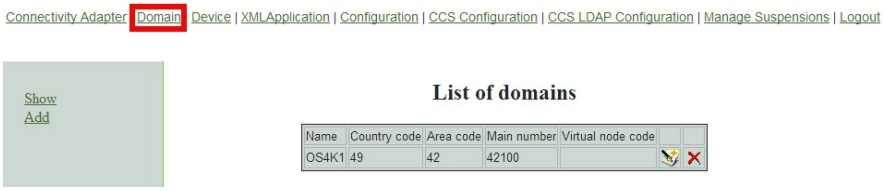


Figure 69: List of domains

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

Figure 70: 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 71: 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 (`C13999`**xx**).

Press the

button to assign at least one previously configured.**Domain**

Figure 72: Add Connectivity Adapter

Figure 73: XMLPS - Add new domain

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

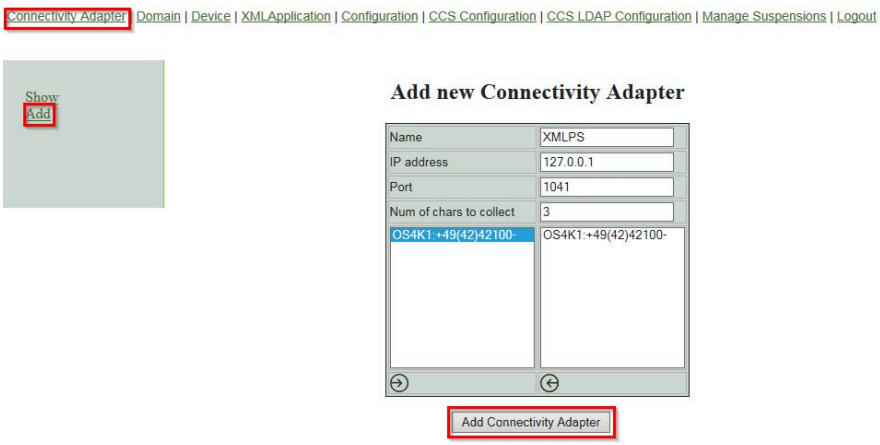


Figure 74: Add new Connectivity Adapter

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

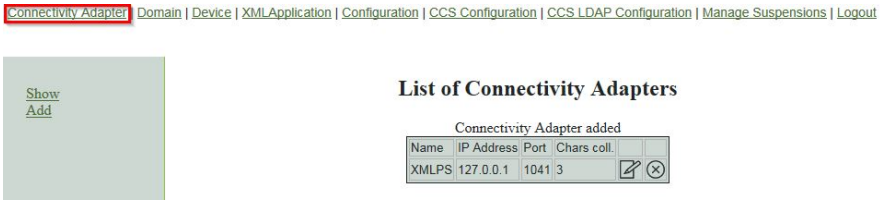


Figure 75: Device

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.

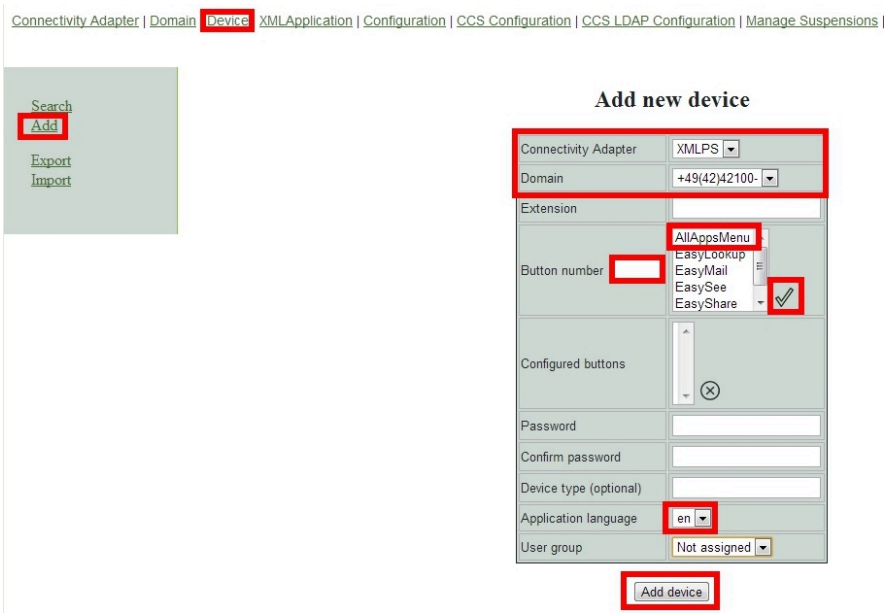


Figure 76: Add new device

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

NOTICE: 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.

In case of import we have two modes:

- Create - used to create or replace an existing DB
- Update - used to add new users to an existing DB

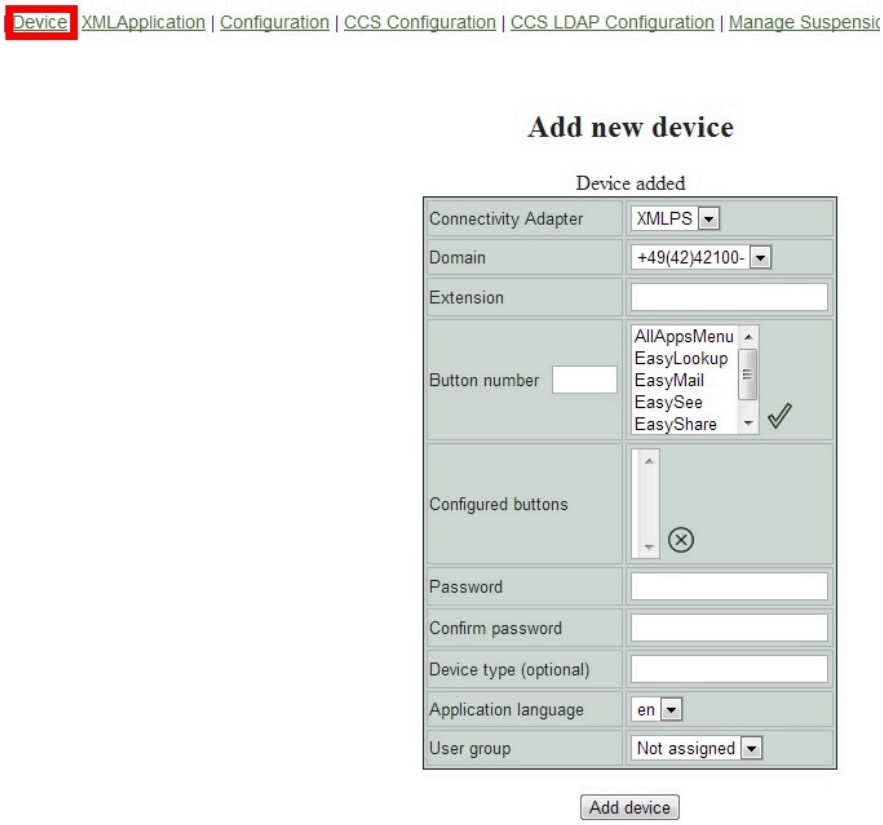


Figure 77: Device added

Do not change anything in this configuration!!

Switch to the **Configuration** Web page.

Figure 78: 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.

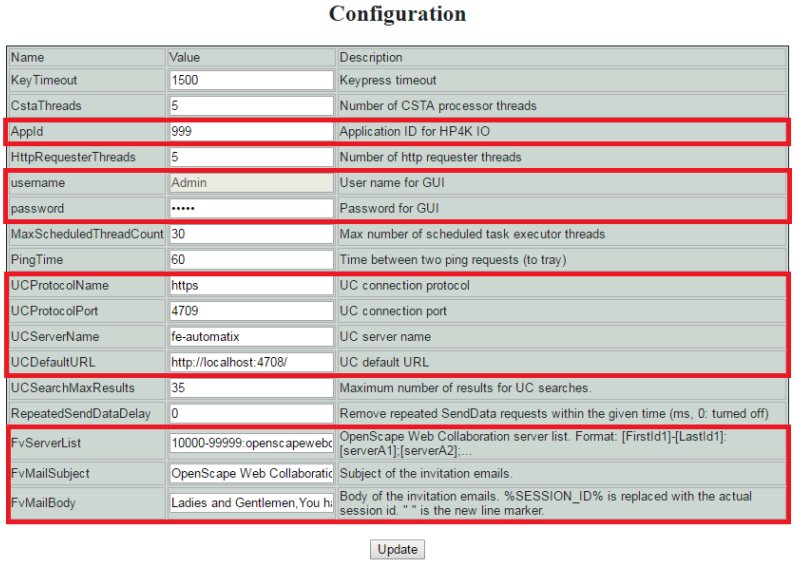


Figure 79: Configuration

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.

NOTICE: 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.

6.6 LDAP Connection Configuration for EasyLookup

6.6.1 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.

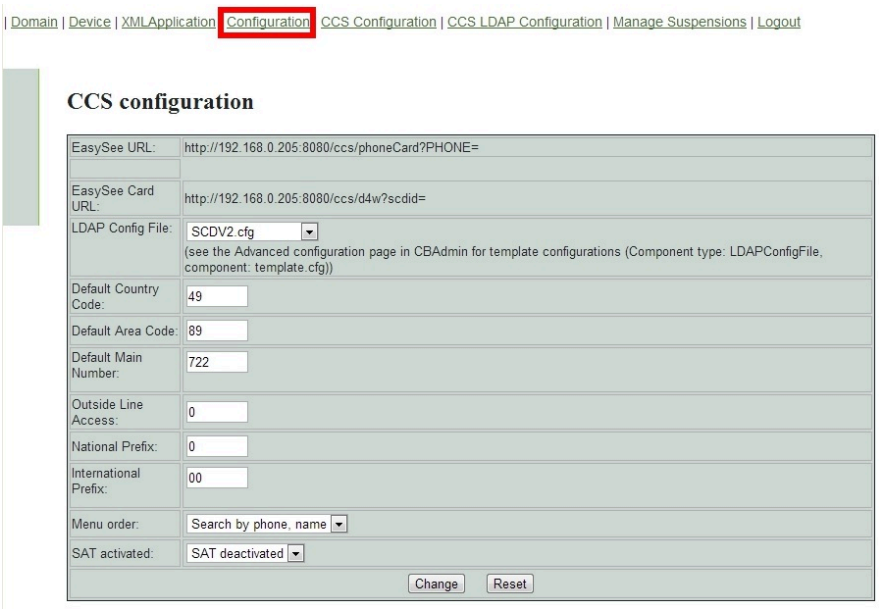


Figure 80: CCS Configuration - CCS LDAP Configuration

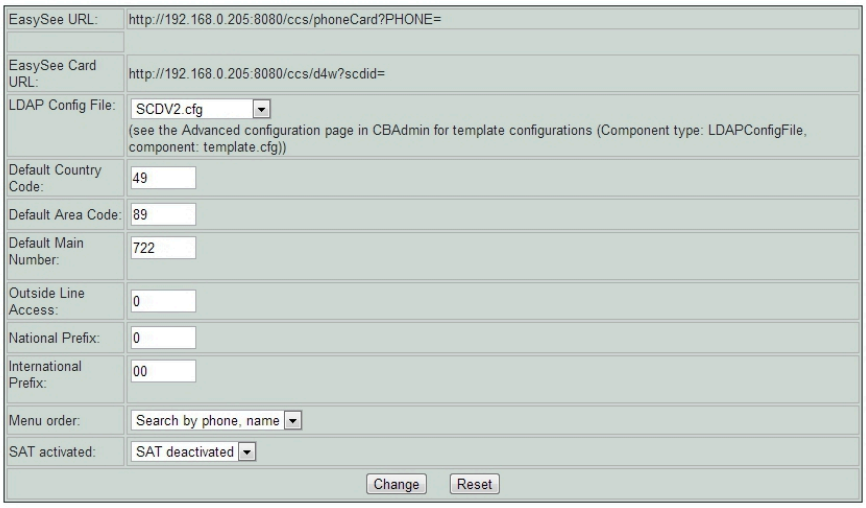


Figure 81: CCS Configuration

- **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.

6.6.2 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.

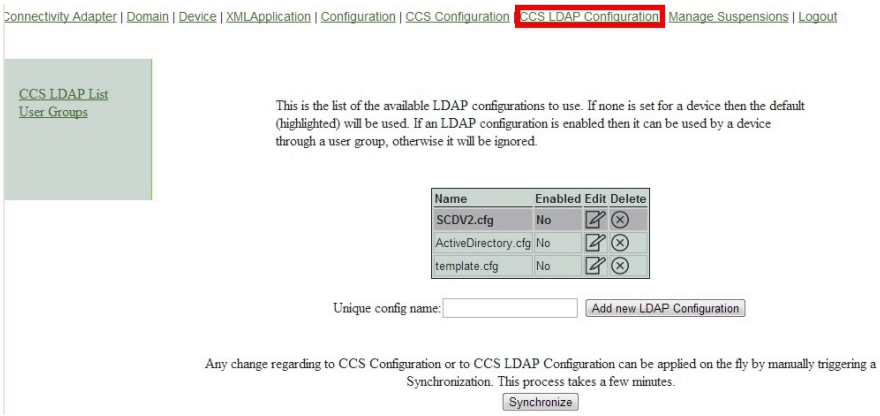


Figure 82: List of LDAP configurations

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.

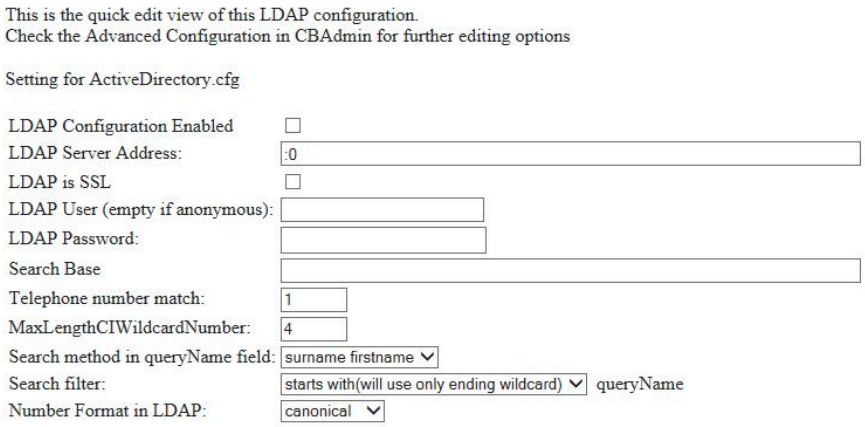


Figure 83: General LDAP settings

- **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.
- Search filter
- New in V8, the search filter allows customization of the wildcard(*) automatic insertion during the searches done with EasyLookup. By adjusting the

wildcard position, performance may be improved depending on the LDAP size.

Possible values:

1) starts with(will use only the ending wildcard) (default)

This is the default filter and it keeps the previous logic. Depending on the search, the result will start with the queried name.

1) ends with(will use only the starting wildcard)

The result will end with the queried name. This filter is useful if the LDAP directory is small because users can be found by their first name.

1) contains(will use both wildcards)

This is a more permissive and extended filter. Users can search for parts of the full name. This filter can cause performance issues because some queries may take longer due to a bigger set of results. In this case, the results will contain the queried name.

- **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

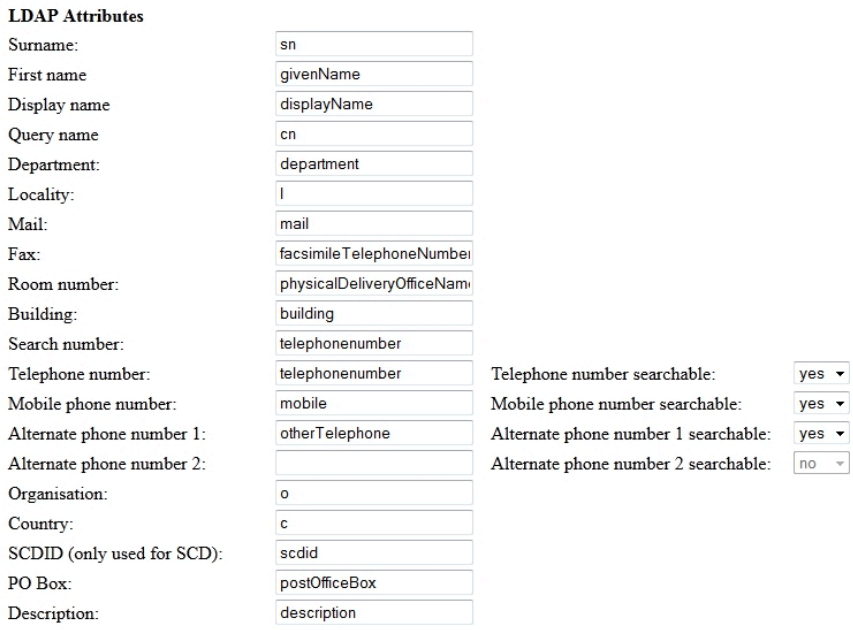


Figure 84: LDAP attribute specification

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.

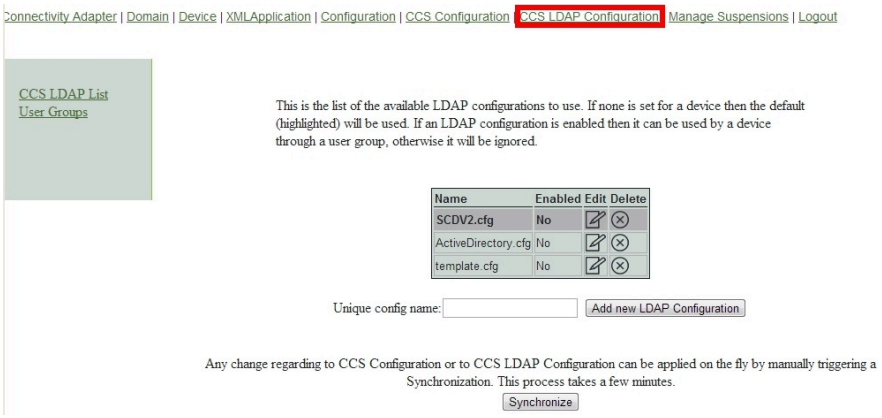


Figure 85: CCS LDAP Configuration

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).

6.6.3 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.

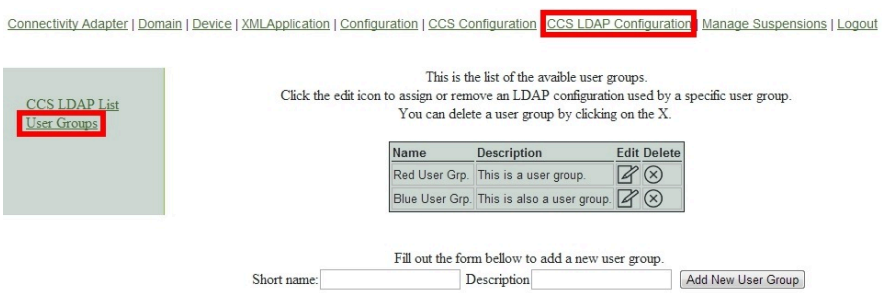


Figure 86: User groups

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.

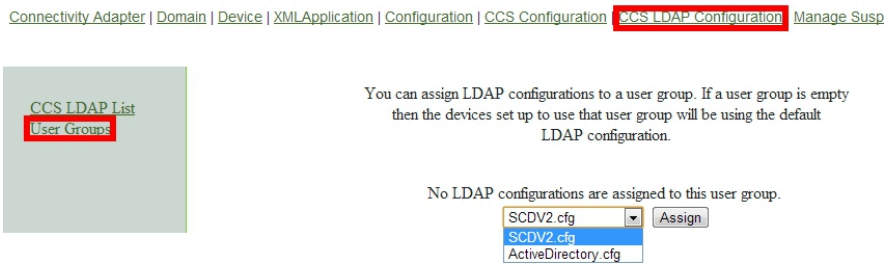


Figure 87: User group - assign LDAP Configuration

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.

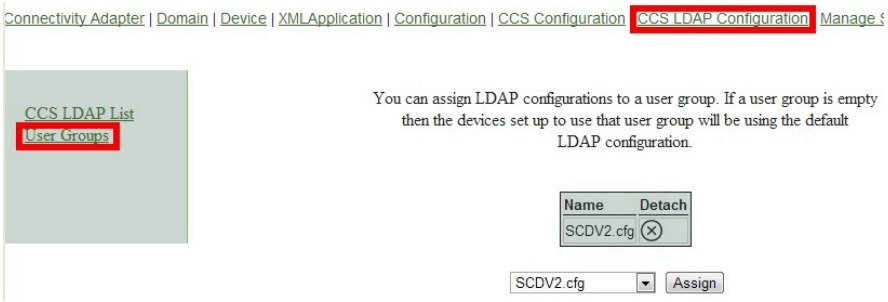


Figure 88: User group - detaching a configuration

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**).

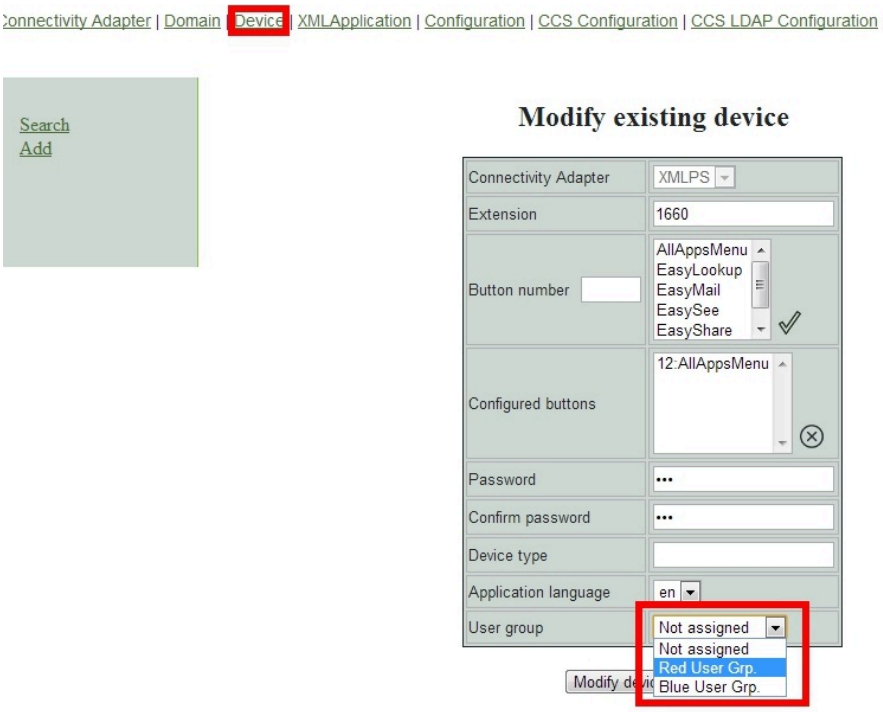


Figure 89: Device modify - assigning a user group

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.

6.6.4 Configuration Example: Web Page Design

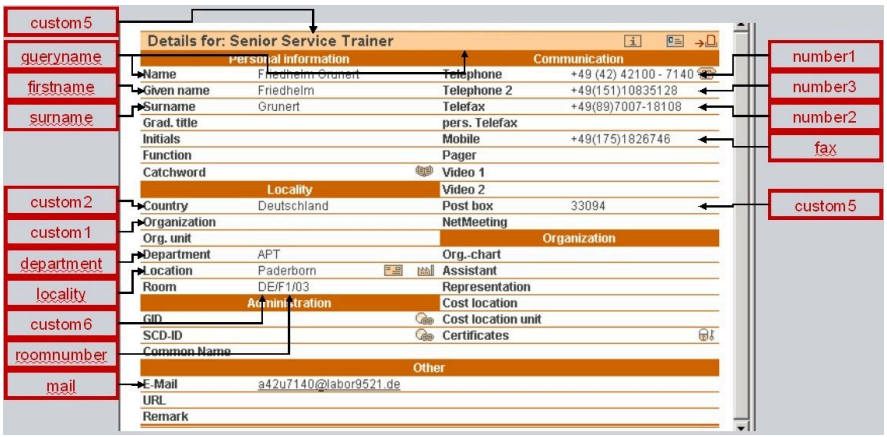


Figure 90: Configuration parameter EasySee Web page

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!

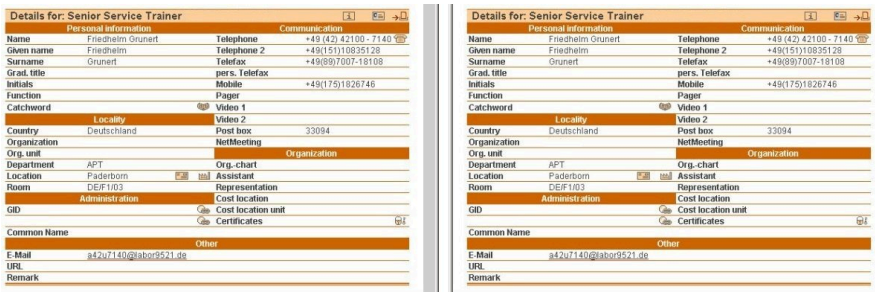


Figure 91: Web page design

6.7 Suspension

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

Temporary login lock

Both CBAdmin 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.

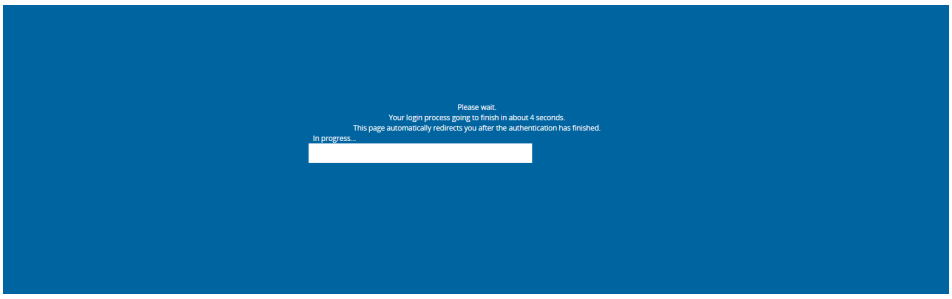


Figure 92: CBAdmin - delayed login progress

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

Suspension List

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

Manage Supsensions > Show List

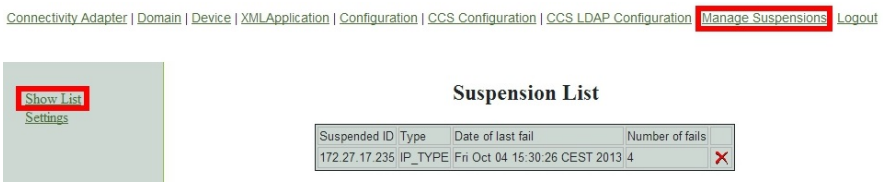


Figure 93: Manage Suspension - suspended addresses

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 Suspension > Settings

Figure 94: 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.

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

> **NOTICE:** You can download **OpenScape 4000 Phone Services (prev. XCI Tray)** from the OpenScape 4000 Phone Service Web page. OpenScape 4000 V8 integrated variant: `https://<CLAN IP fo CSTA VM>:8081/ccs/html/index.html`

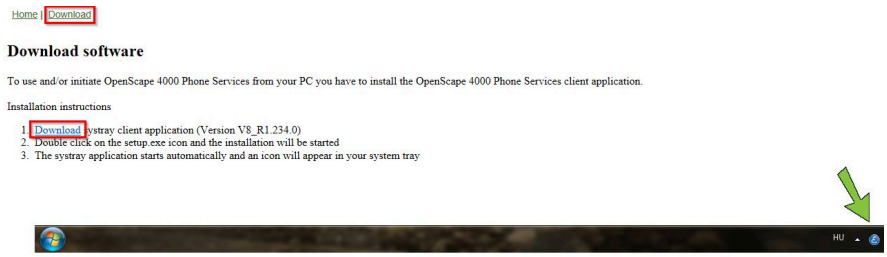


Figure 95: Download OpenScape 4000 Phone Services

Select **Download** to download the program.

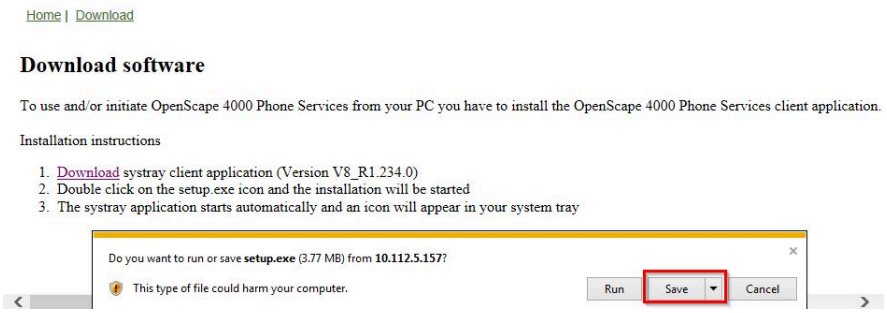


Figure 96: Run or Save

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

Figure 97: 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:

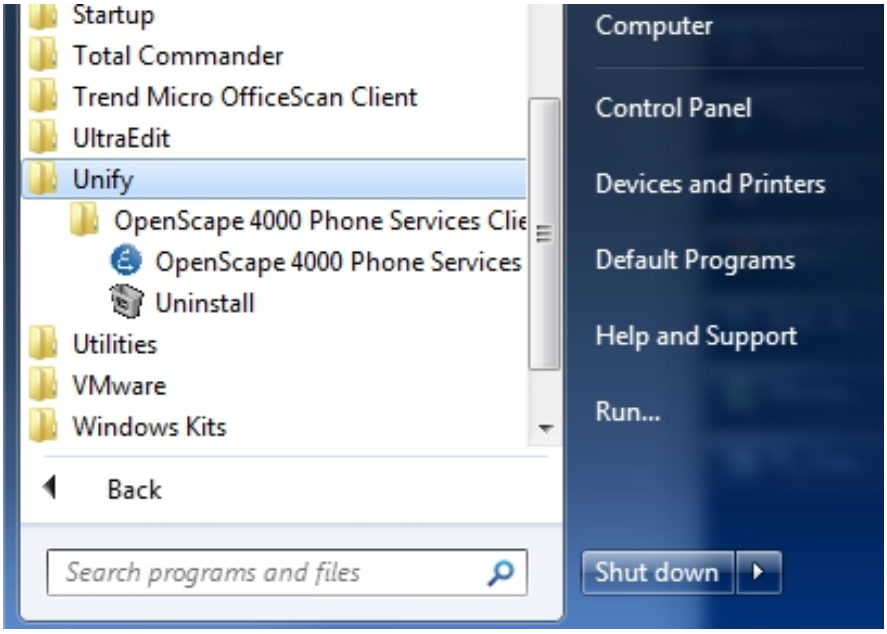


Figure 98: OpenScape 4000 Phone Services in Start menu

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

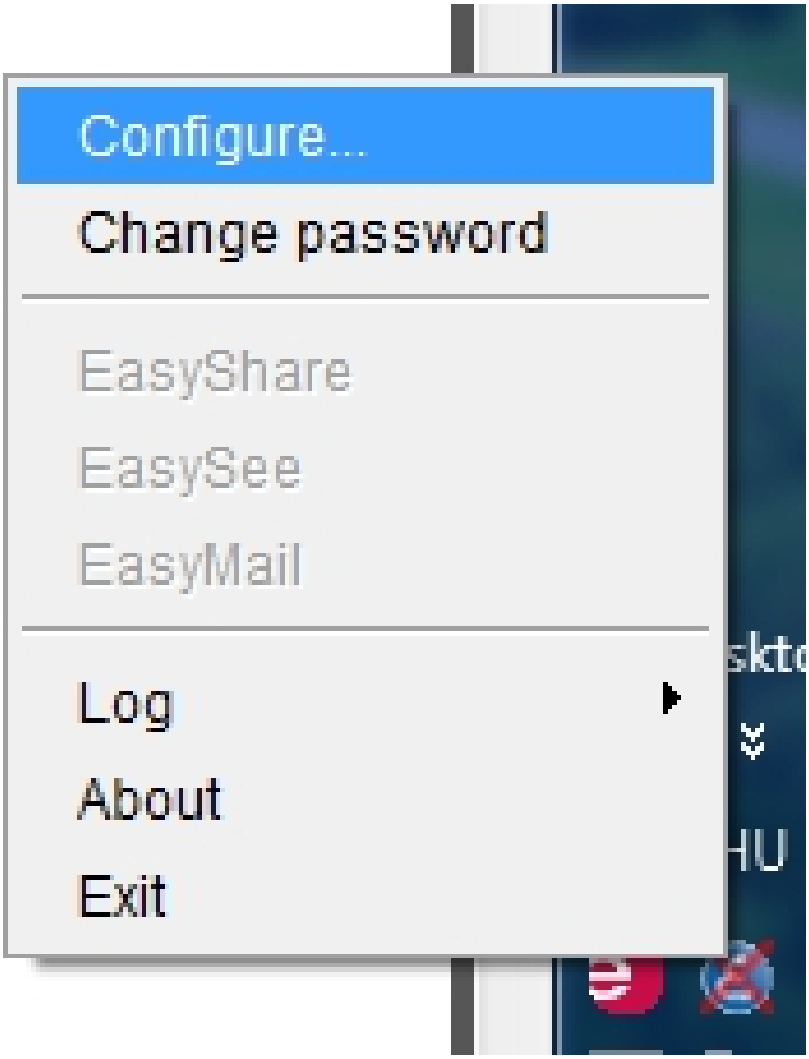


Figure 99: OpenScape 4000 Phone Services - Configuration menu

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):

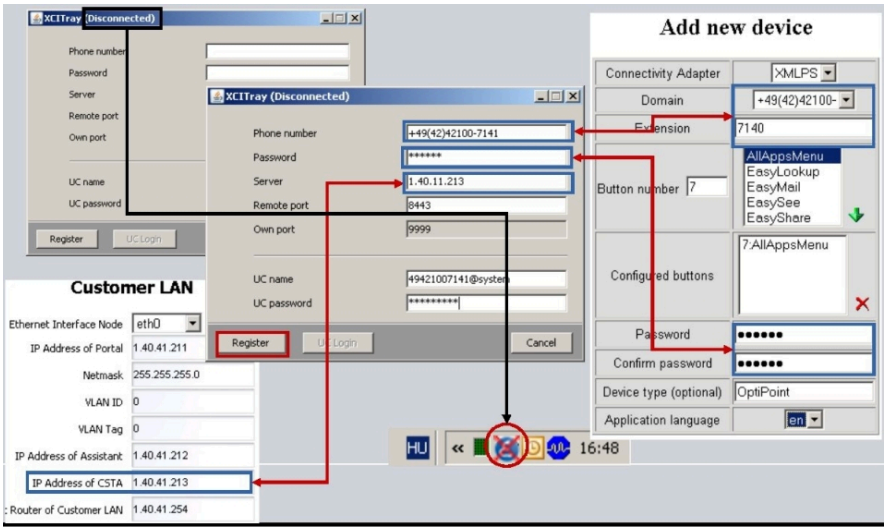


Figure 100: OpenScape 4000 Phone Services (prev. XCI Tray) configuration

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

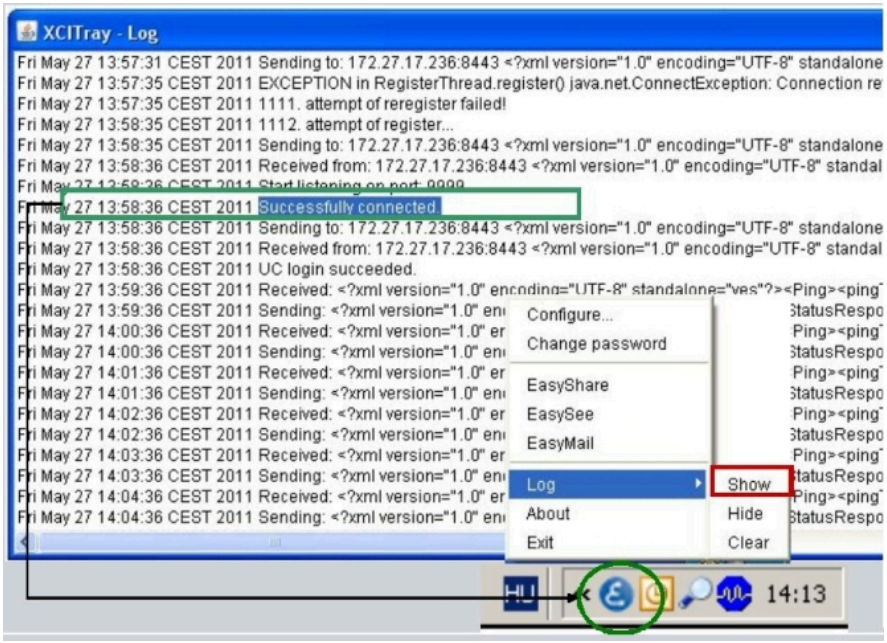


Figure 101: OpenScape 4000 Phone Services logs

This log message provides helpful information about the connection.

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

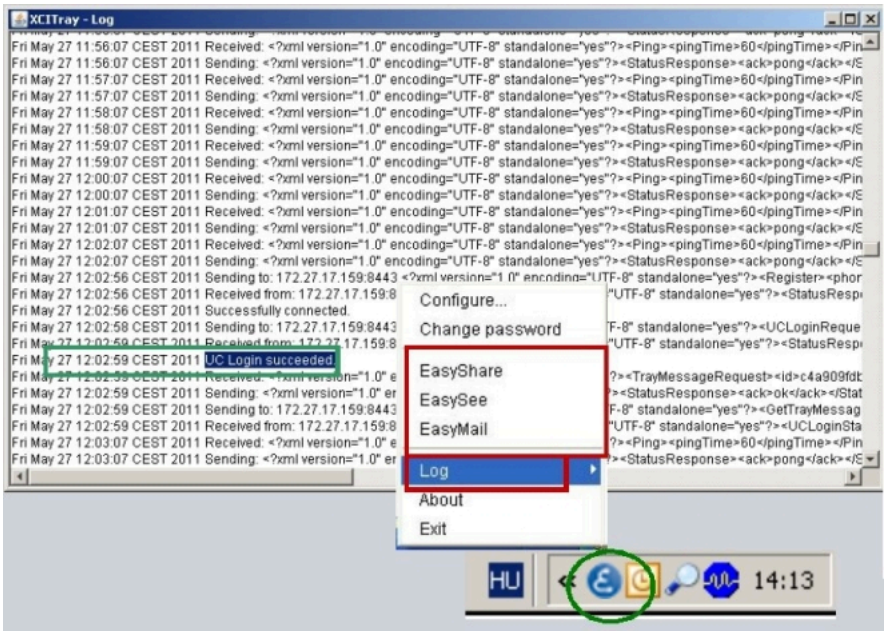


Figure 102: OpenScape 4000 Phone Services Menu - functions

If the OpenScape 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.

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

Index