



# HiPath 4000 HiPath 4000 CSTA V1 and Phone Services

**Service Documentation**

A31003-H3100-S102-6-7620

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

© Unify Software and Solutions GmbH & Co. KG 12/2015  
Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany

All rights reserved.

Reference No.: A31003-H3100-S102-6-7620

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

Availability and technical specifications are subject to change without notice.

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

# HiPath 4000 CSTA V1 and Phone Services - Contents

<b>1 Introduction</b>	<b>5</b>
1.1 Important Information	5
1.2 General Information	5
<b>2 Scenarios</b>	<b>7</b>
2.1 HiPath 4000 V6 Maximum Values	7
2.2 Internal Integration	7
2.3 External Installation	9
<b>3 Requirements</b>	<b>11</b>
3.1 Hardware Requirements	11
3.2 Software Requirements	11
3.2.1 Operating System	11
3.2.2 Other Supported Software	11
3.2.3 PBX Support	12
3.3 Configuration Batch Description	12
3.4 Configuration Requirements	13
3.5 HiPath 4000 CSTA Software Packages	13
<b>4 Licensing</b>	<b>15</b>
<b>5 Software Installation</b>	<b>19</b>
5.1 Installation and Program Start with Linux	19
5.1.1 Software Installation	19
5.1.2 Program Start	21
5.2 Installation and Program Start with Windows	22
5.2.1 Software Installation	22
5.2.2 Program Start	27
<b>6 Port List</b>	<b>29</b>
<b>7 CBAAdmin Configuration Management</b>	<b>31</b>
7.1 Configuration	31
7.2 Status – Connection Check	37
7.3 Logging	38
7.3.1 Logging for SMR 13	38
7.3.2 Logging for SMR 11/SMR 12	41
7.4 Statistics	42
7.5 Version	45
7.6 Phone Service UI	45
7.7 Settings	46
7.7.1 User/Password	46
7.7.2 HTTPS Connection	47
7.8 Advanced Configuration for SMR 13	49
7.9 Logout	51
<b>8 HiPath 4000 CSTA Switch Integrated – Introduction</b>	<b>53</b>
8.1 Application Environment	53
8.2 Portal – IP Address Configuration	55
8.3 CBAAdmin – Trusted IP Addresses	58
8.4 CBAAdmin – CA Instance Configuration	59

## HiPath 4000 CSTA V1 and Phone Services - Contents

8.5 Additional Supported Services . . . . .	64
8.6 Changing of the Configuration File . . . . .	66
8.6.1 Configuration Change for SMR 11. . . . .	66
8.6.2 Configuration Change for SMR 13. . . . .	66
8.6.3 Special Settings . . . . .	68
8.6.3.1 Concept of “Presentation Indicator for Devices” in CSTA Events . . . . .	68
8.6.3.2 Delayed CSTA Request Features . . . . .	69
8.6.3.3 CSTA Accept Call and Offered Event. . . . .	70
8.6.3.4 Delivering deviceIDs in E.164 Format (SFR international) . . . . .	70
8.6.3.5 Special Settings to Application Connection . . . . .	72
8.6.3.6 Special setting to deliver keyset information via HiPath 4000 CSTA . . . . .	73
8.6.3.7 Umlaut Characters . . . . .	73
8.6.3.8 Hunt Group Behavior . . . . .	74
8.6.3.9 UserToUser Info (SMR 13). . . . .	74
8.6.3.10 Usage with OpenSape Contact Center (OSCC). . . . .	74
<b>9 Phone Services – Introduction . . . . .</b>	<b>75</b>
9.1 Overview . . . . .	75
9.1.1 EasyLookup . . . . .	75
9.1.2 EasySee. . . . .	76
9.1.3 EasyMail . . . . .	77
9.1.4 EasyShare . . . . .	78
9.1.5 EasyUC . . . . .	79
9.2 Structure . . . . .	80
9.3 Requirements . . . . .	85
9.4 Configuration . . . . .	85
9.4.1 Configuration Steps . . . . .	85
9.4.2 AMO Configuration HiPath 4000 V5, V6 . . . . .	86
9.4.3 HiPath 4000 CSTA. . . . .	87
9.5 LDAP Connection Configuration for EasyLookup (SMR 13 specific) . . . . .	93
9.5.1 CCS Configuration. . . . .	93
9.5.2 CCS LDAP Configuration. . . . .	95
9.5.3 Phone Services with Multiple LDAP Servers . . . . .	98
9.5.4 Configuration Example: Web Page Design . . . . .	100
9.6 LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12) . . . . .	101
9.7 Suspension . . . . .	111
9.8 HiPath 4000 Phone Services HiPath 4000 Phone Services (prev. XCI Tray). . . . .	112
<b>List of Figures . . . . .</b>	<b>117</b>
<b>List of Tables . . . . .</b>	<b>121</b>
<b>Index . . . . .</b>	<b>122</b>

# 1 Introduction

## 1.1 Important Information

From HiPath 4000 V6 all CSTA applications must use the CA4000 adaptor of the integrated HiPath 4000 CSTA. This includes HiPath CAP V3.0 when used. 3rd party application integrations using direct ACL connectivity are no longer supported.

Regression- and Security tests are only performed with the “integrated HiPath 4000 CSTA” and GVS can only provide Software corrections for that “internal HiPath 4000 CSTA”.

## 1.2 General Information

HiPath 4000 CSTA...

- is a protocol converter, which converts the internal **HiPath 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 HiPath 4000 V6 integrated installation or as an external installation on Linux SLES 10, SLES 11 or on Windows operating systems.

---

**IMPORTANT:** The R13.20x.x versions and upwards support only internal installation.

---

- is an improved development and merges the advantages of HiPath CAP V3.0 and CAP Inside V1.
  - CSTA III, ASN.1 and CSTA III, XML support
  - HiPath 4000 integration
  - High performance interface
  - HiPath 4000 Phone Services
  - HBR integration
  - Licensing via CLA (10 clients, 100 clients, unlimited)
  - Configuration management via Web interface

## **Introduction**

### General Information

## 2 Scenarios

### 2.1 HiPath 4000 V6 Maximum Values

Based on **HiPath 4000 V6 Memory Allocation**, the following maximum values affect the maximum number of supported ACL-C – HiPath 4000 CSTA connections:

AMO DIMSU: ECCS 50

AMO DIMSU: APPL 98

AMO XAPPL: SUBAPPL 32

AMO DIMSU: ACDMONID 5000

See the AMO description for more details.

---

**NOTE:** One Connectivity Adapter can support 4 application links simultaneously. In case of HiPath 4000 V6 R0 installation: 16, in case of HiPath 4000 V6 R1 and higher: 32 CSTA links are supported theoretically.

This is valid only in case of the HiPath 4000 CSTA integrated version.

---

### 2.2 Internal Integration

#### 1 CSTA link

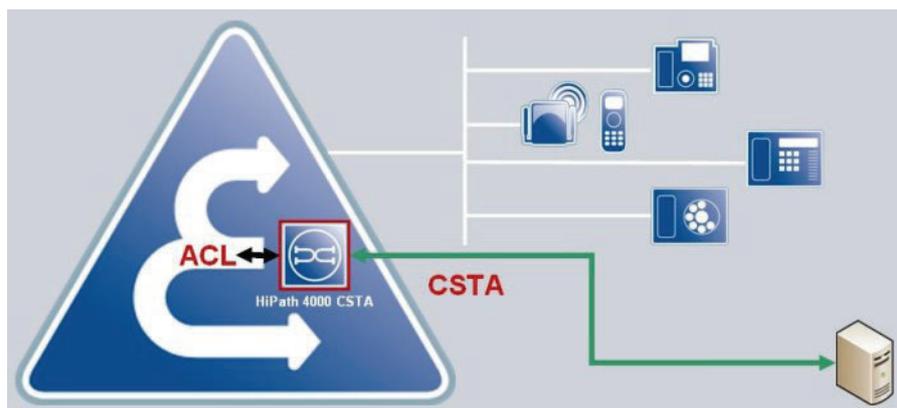


Figure 1 Scenarios - Internal integration - One CSTA link

**A maximum of 4 CSTA links per process – ConnectivityAdapter (CA)**

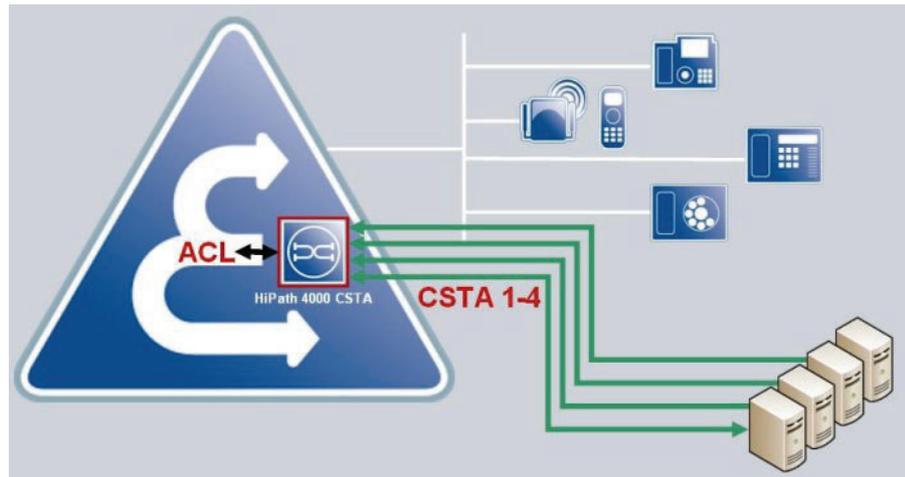


Figure 2 Scenarios - Internal integration - Four CSTA links

**1 to 4 CSTA links per process – ConnectivityAdapter (CA) (max 32 application connections)**

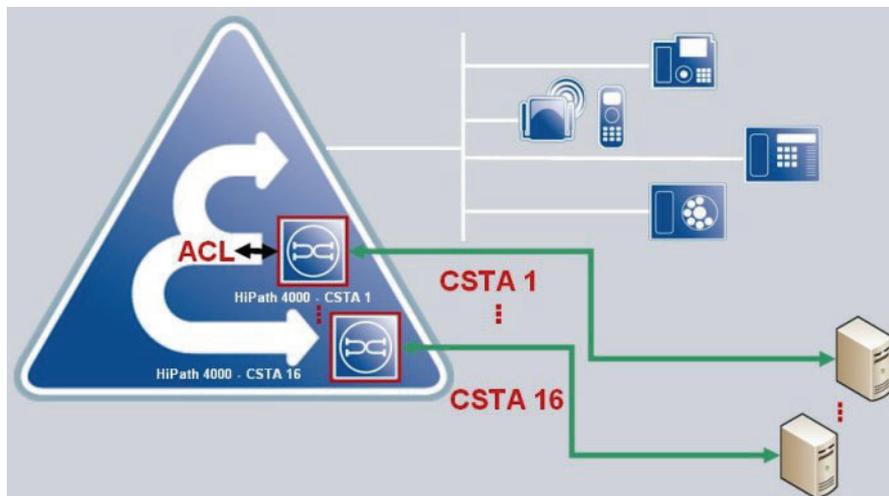


Figure 3 Scenarios - Internal integration - 1 to 4 CSTA links per process

## 2.3 External Installation

---

**IMPORTANT:** There is no external installation released for SMR 13. External installation is only possible with SMR 11 and SMR 12.

---

### 1 CSTA link



Figure 4 Scenarios - External installation - One CSTA link

### 1 to 4 CSTA links per process – ConnectivityAdapter (CA)

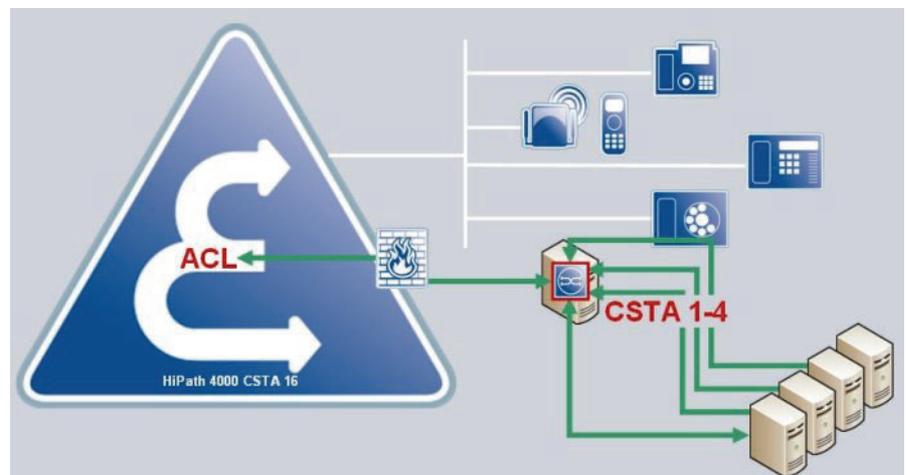


Figure 5 Scenarios - External installation - Four CSTA links

## Scenarios

### External Installation

#### 1 to 4 CSTA links per process – ConnectivityAdapter (CA)

A maximum of 128 application connections because of AMO XAPPL - SUBAPPL: 32.

---

**NOTE:** 128 application connections = 32 ACL-C link pairs \* (4 application connections per CA).

---

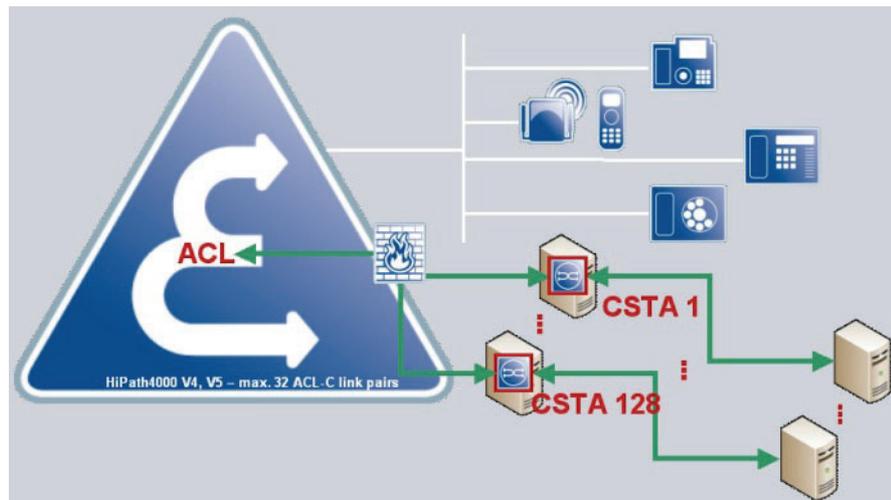


Figure 6 Scenarios - External installation - 1 to 4 CSTA links per process

## 3 Requirements

### 3.1 Hardware Requirements

- An external HiPath 4000 CSTA server requires at least the same hardware as is required by the supported operating systems.
- Care must be taken with memory usage, because one installation can support more than one HiPath 4000 CSTA Connectivity Adapter (CA - `cbdriver4000`) process running at the same time!

### 3.2 Software Requirements

#### 3.2.1 Operating System

Integrated HiPath 4000 CSTA is running on a Novell SuSE Linux Enterprise Server 10 SP4.

In case of external installation:

- Novell SuSE Linux Enterprise Server 10, 11
- Windows 2003 - SP1
- Windows XP - SP2
- Windows 2008, Windows 2008 R2
- Windows 2008 Hyper-V
- Window 7
- VMWare 1.0.1
- VMWare ESX 4.0

#### 3.2.2 Other Supported Software

IBM Java 6 is used for the integrated HiPath 4000 CSTA as operating system.

In case of external installation: Java2 Standard Edition Runtime Environment V6.0 Update 27 (JRE 1.6.0.27 or upper).

## Requirements

### Configuration Batch Description

### 3.2.3 PBX Support

- HiPath 4000 V4.0 - stand alone/external variant (SMR 11, SMR 12)
- HiPath 4000 V5.0 - stand alone/external variant (SMR 11, SMR 12)
- HiPath 4000 V6 - integrated variant (SMR 11, SMR 13)

## 3.3 Configuration Batch Description

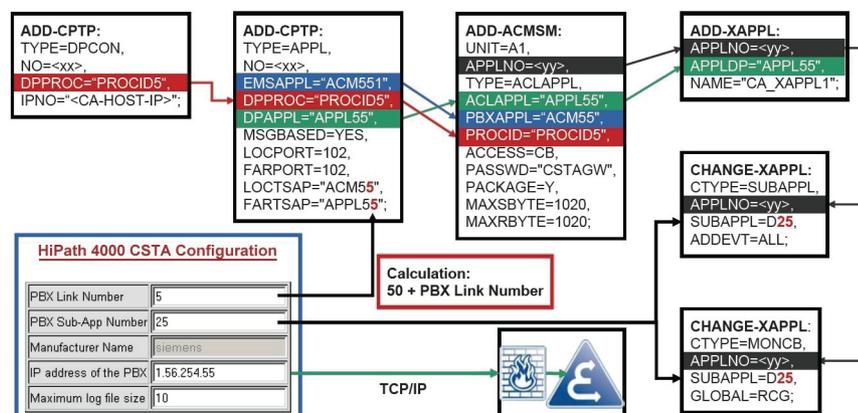


Figure 7 Configuration batch description

The following basic activities must always be carried out for each CA instance:

1. Maximum number of ACL-C applications must be set  
AMO: DIMSU parameter: ECCS:
2. Maximum number of monitored devices must be set  
AMO: DIMSU (dimensioning of features, switching unit) parameter:  
ACDMONID, number of monitored id sets (e.g. acdagents -only acd-g). The maximum number of permitted monitored devices. Any attempt by the application to set more monitoring points than permitted by the maximum number of monitored devices will be rejected.
3. Call processing timers must be set  
AMO: CTIME, customer-specific CP1 timers, switching unit manages the call processing timers, which are evaluated by the MakeCall requests.
4. Initial communication ACL-C Link must be configured  
AMO: CPTP, communication parameters for tcp/ip connection (as ACL-C identifier only) TYPE:DPCON
5. Application interface parameters must be set (transport address)

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

6. ACL Manager parameters must be configured

AMO: ACMSM, aclmanager communication parameter APPLTYP= ACLAPPL

7. XAPPL application must be configured

AMO: XAPPL, DVA -application ACL

8. XAPPL sub-application parameters must be configured

AMO: XAPPL, CTYPE: SUBAPPL.

9. XAPPL sub-application parameters must be configured

AMO: XAPPL, CTYPE: MONCB.

### 3.4 Configuration Requirements

For ACL-C connections outside Atlantic LAN:

- The IP address of the host on which the CA instance is running has to be added into the **HiPath 4000 Unix firewall** access list.

### 3.5 HiPath 4000 CSTA Software Packages

In case of external/stand alone variant the following software packages are provided.

- As Linux rpm:  
CSTA-V1\_R1x.20y.0-0.i586.rpm  
(where x, y correspond to the actual release)
- As Windows zip file:  
setup.exe (inside the iso zip file on SWS)

## Requirements

HiPath 4000 CSTA Software Packages

## 4 Licensing

HiPath 4000 CSTA uses the **CLA** for licensing purposes.

- The V6 integrated version uses the CLA installed on the SOCO2 machine.
- In the case of a standalone installation, the CLA must be installed on the local machine.

CAP Inside V1.0 has different kinds of licenses for different types of applications. The application type has to be specified in the ACSE message that establishes the connection; the license check then uses this information.

HiPath 4000 CSTA has three license modes, which differ in the number of possible monitor points. The three modes are: **no license**, **100 clients** and **unlimited**.

A license is required for the two latter modes, which is checked when the application connects (Product ID: L30001-B39-A1, Version: V3.0, Feature IDs: *100\_Clients* and *Unlimited*). The maximum number of monitor points allowed in the different modes are as follows:

<b>No license</b>	10
<b>100 clients</b>	100
<b>Unlimited</b>	100000

Monitor points are counted per application connection. If the same device has multiple monitor points, each of them is counted.

Licensing can be defined through the Web-based configuration interface in the application configuration dialog under the **License type** option. When the license mode is changed, the application connection is automatically closed by the cb driver and the application has to reconnect.

The license mode is stored in the cb driver's configuration in case of SMR 13 and can be set through the Advanced Configuration.

In case of SMR 11 and SMR 12 the license mode is stored in the cb driver's configuration file. The license mode can be set with the following command:

```
LICENSE_TYPE_<application id> = <license mode>
```

Where the application id is a digit from 1 to 4 and `<license mode>` is either **no\_license**, **100\_clients** or **unlimited**.

Unify internal applications are not really affected by the licensing change. They should connect the same way as for CAP Inside (see CAP Inside External Interface Specification for HiPath Applications), but the license mode **no license** must be defined for the given application connection.

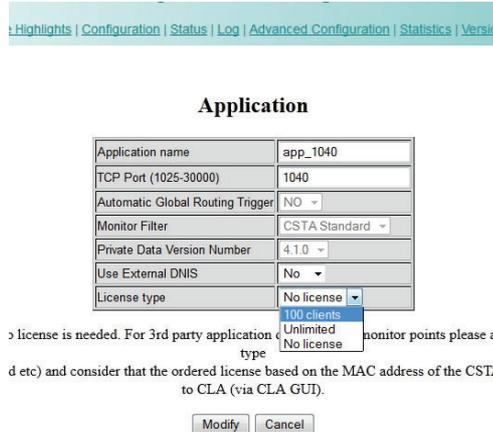


Figure 8 HiPath 4000 CSTA CBAAdmin configuration management

The **Add application - License type** option defines the number of supported monitored devices for this configured CSTA link.

**No license:** max 10 monitored devices, no CLA link required.  
 This license type is proposed to use for test purpose only.

**100 clients:** max 100 monitored devices, CLA link/license required.

**unlimited:** max 100000 monitored devices, CLA link/license required.

---

**NOTE:** Because of AMO limitation (**ACMONID**) 5000 RCG specific monitor points are supported.

---

It is possible to check the available and currently used licenses via the menu option **License Highlights**.



Figure 9 License Highlights

On the top of this page there is a summary of the available and used licenses grouped by license type. Under this there is a detailed list about the connectivity adapters and the applications configured to them. What type of license and which

specific application it has been set to can be seen here. In case an application consumes a license then it is marked with a “Used” notation, otherwise “---” can be seen.



## 5 Software Installation

---

**NOTE:** Please consider that the installation packages do not include any JRE installation packages (because of licensing reason), as pre-requirement of the HiPath 4000 CSTA installation, Oracle JRE 1.6.x must be installed previously.

---

In case of stand alone/external installation there are three different ways to install the software:

### As a Linux installation

```
rpm -ivh CSTA-V1_R1x.20y.0-0.i586.rpm
```

(where x, y depend on the actual release)

### As a Linux upgrade installation

```
rpm -Uvh CSTA-V1_R1x.20y.0-0.i586.rpm
```

---

**NOTE:** In the case of a HiPath 4000 V6 switch Integrated installation, this RPM installs further files. In this environment, the `/etc/v6maker.conf` file is used as an identifier for the automatically modified installation!

---

### As a Windows installation

Unzip the CSTA-V1\_R1x.20y.0.zip (where x, y depend on the actual release) and start the `setup.exe`.

---

**NOTE:** Please take care to have Administrator rights under Windows 7.

---

## 5.1 Installation and Program Start with Linux

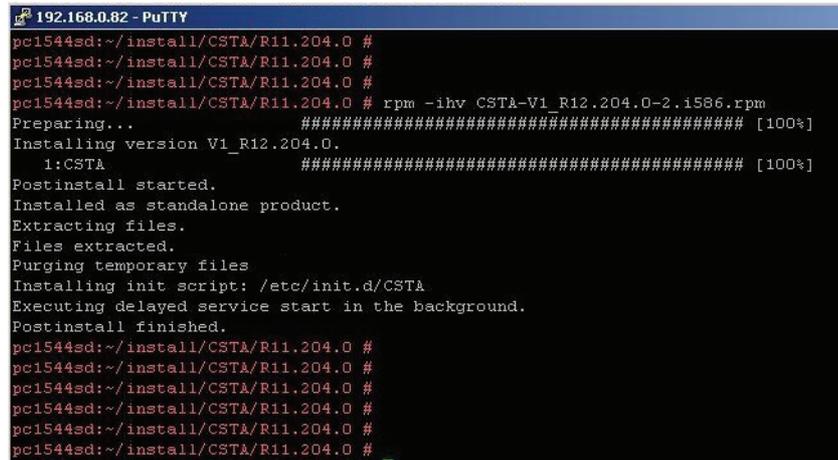
### 5.1.1 Software Installation

#### Linux installation

```
rpm -ivh CSTA-V1_R1x.20y.0-0.i586.rpm
```

## Software Installation

### Installation and Program Start with Linux



```
192.168.0.82 - PuTTY
pc1544sd:~/install/CSTA/R11.204.0 #
pc1544sd:~/install/CSTA/R11.204.0 #
pc1544sd:~/install/CSTA/R11.204.0 #
pc1544sd:~/install/CSTA/R11.204.0 # rpm -ihv CSTA-V1_R12.204.0-2.i586.rpm
Preparing... ##### [100%]
Installing version V1_R12.204.0.
 1:CSTA ##### [100%]
Postinstall started.
Installed as standalone product.
Extracting files.
Files extracted.
Purging temporary files
Installing init script: /etc/init.d/CSTA
Executing delayed service start in the background.
Postinstall finished.
pc1544sd:~/install/CSTA/R11.204.0 #
pc1544sd:~/install/CSTA/R11.204.0 #
pc1544sd:~/install/CSTA/R11.204.0 #
pc1544sd:~/install/CSTA/R11.204.0 #
pc1544sd:~/install/CSTA/R11.204.0 #
pc1544sd:~/install/CSTA/R11.204.0 #
```

Figure 10 Linux installation

Following successful installation, the `jss` process starts up automatically.

The HiPath 4000 CSTA processes are started automatically when the system reboots.

`/etc/init.d/CSTA` or `service CSTA`

`{start|stop|status|try-restart|restart|force-reload|reload}`

The daemon is started at run level:

2 | 3 | 5

The default installation directory is:

`/opt/siemens/CSTA`

The default installation directory contains the following subdirectories:

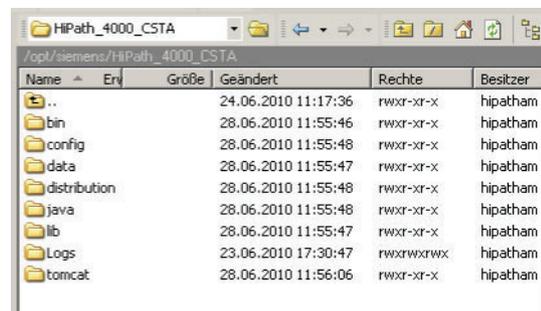
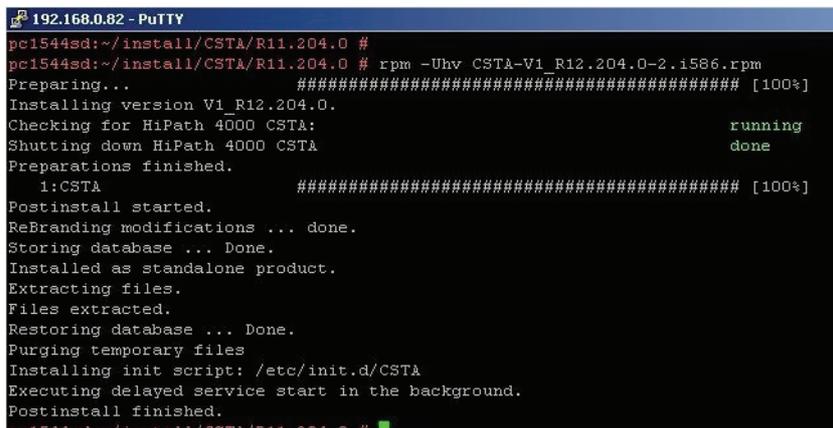


Figure 11 Subdirectories

**NOTE:** As mentioned before, `java` is no longer part of the HiPath 4000 CSTA installation due to licensing issues, therefore the `java` directory cannot be found here.

## Linux upgrade installation

```
rpm -Uvh CSTA-V1_R1x.20y.0-0.i586.rpm
```

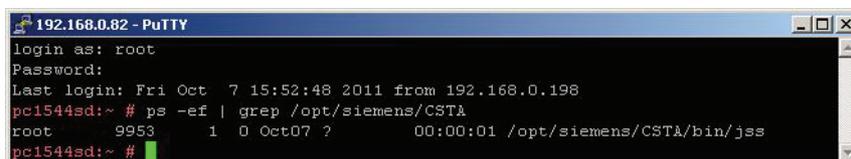


```
192.168.0.82 - PuTTY
pc1544sd:~/install/CSTA/R11.204.0 #
pc1544sd:~/install/CSTA/R11.204.0 # rpm -Uvh CSTA-V1_R12.204.0-2.i586.rpm
Preparing... ##### [100%]
Installing version V1_R12.204.0.
Checking for HiPath 4000 CSTA: running
Shutting down HiPath 4000 CSTA done
Preparations finished.
 1:CSTA ##### [100%]
Postinstall started.
Rebranding modifications ... done.
Storing database ... Done.
Installed as standalone product.
Extracting files.
Files extracted.
Restoring database ... Done.
Purging temporary files
Installing init script: /etc/init.d/CSTA
Executing delayed service start in the background.
Postinstall finished.
pc1544sd:~/install/CSTA/R11.204.0 #
```

Figure 12 Linux upgrade installation

## 5.1.2 Program Start

Based on the daemon run level, the HiPath 4000 CSTA Web Administration Server starts at run level 2, 3 or 5. The process name is jss.



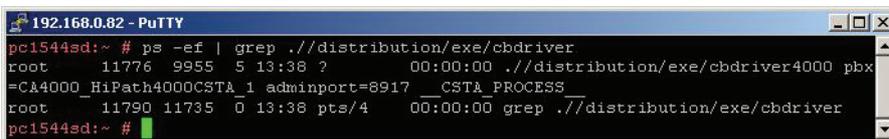
```
192.168.0.82 - PuTTY
login as: root
Password:
Last login: Fri Oct 7 15:52:48 2011 from 192.168.0.198
pc1544sd:~ # ps -ef | grep /opt/siemens/CSTA
root      9953      1  0 Oct07 ?        00:00:01 /opt/siemens/CSTA/bin/jss
pc1544sd:~ #
```

Figure 13 Program start jss

---

**NOTE:** For every CA instance configured on this Web server, an individual cbdriver4000 process is also started.

---



```
192.168.0.82 - PuTTY
pc1544sd:~ # ps -ef | grep //distribution/exe/cbdriver
root      11776  9955  5 13:38 ?        00:00:00 //distribution/exe/cbdriver4000 pbx
=CA4000_HiPath4000CSTA_1 adminport=8917 CSTA_PROCESS
root      11790 11735  0 13:38 pts/4    00:00:00 grep //distribution/exe/cbdriver
pc1544sd:~ #
```

Figure 14 Program start cbdriver4000

## Software Installation

### Installation and Program Start with Windows

## 5.2 Installation and Program Start with Windows

### 5.2.1 Software Installation

Unpack the zip file and run `Setup.exe`.

---

**NOTE:** Under Windows 7 Administrator rights are necessary for the installation.

---

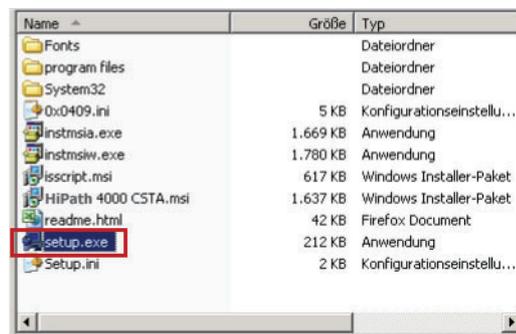


Figure 15 Run setup.exe

Follow the **InstallShield Wizard** and wait for the next messages.

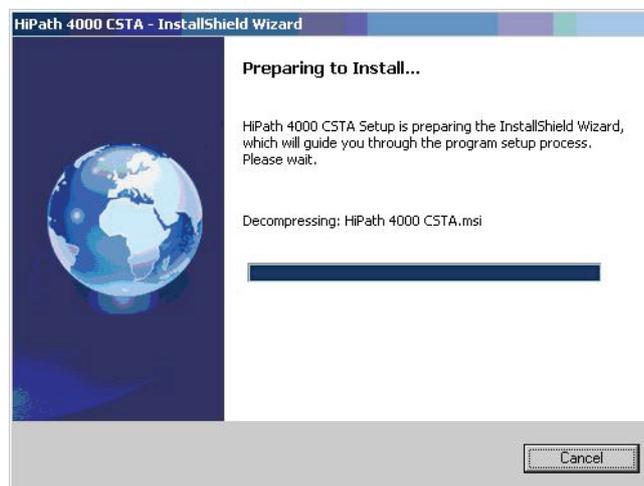


Figure 16 InstallShield Wizard - Step 1

Press **Next** to continue the installation.



Figure 17 *InstallShield Wizard - Step 2*

Press **Next** to continue the installation.

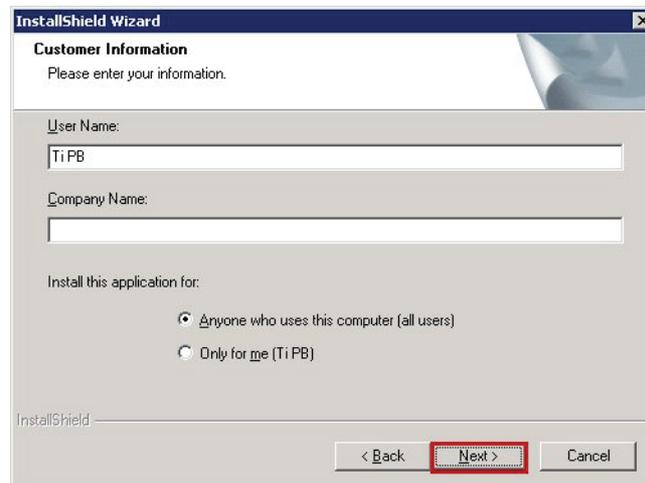


Figure 18 *InstallShield Wizard - Step 3*

Press **Next** to continue the installation.

## Software Installation

### Installation and Program Start with Windows

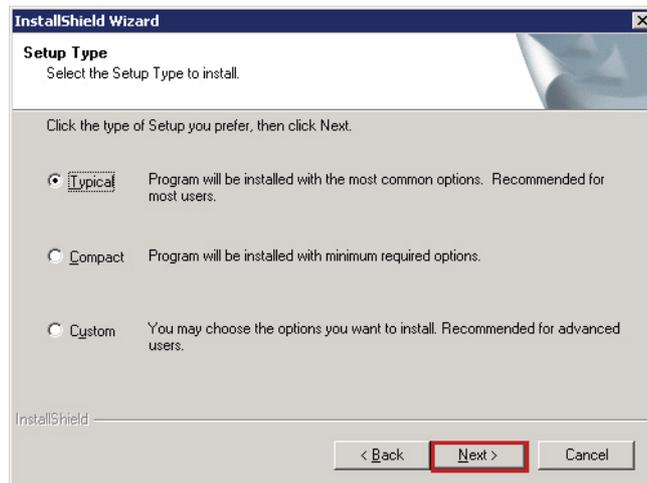


Figure 19 *InstallShield Wizard - Step 4*

Press **Next** to continue the installation.

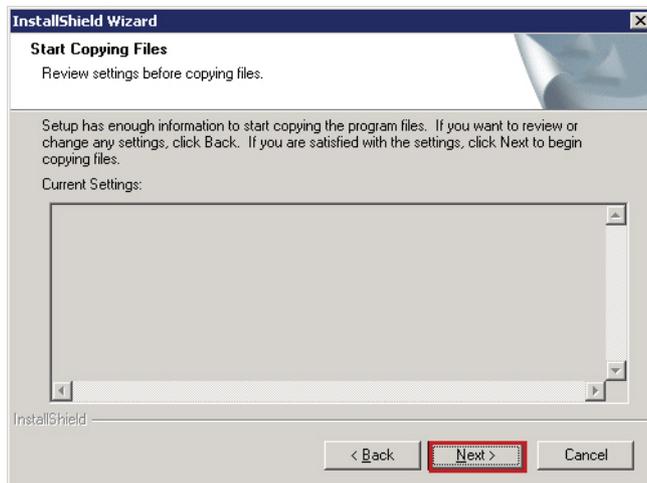


Figure 20 *InstallShield Wizard - Step 5*

Follow the InstallShield Wizard and wait for the next messages.

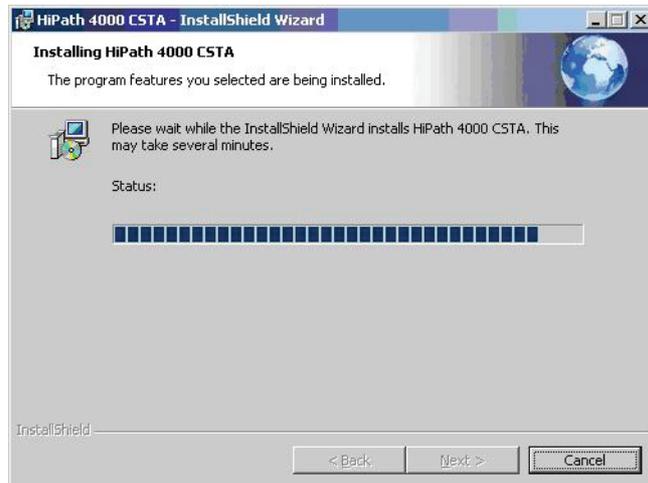


Figure 21 *InstallShield Wizard - Step 6*

Press **Finish** to complete the installation.

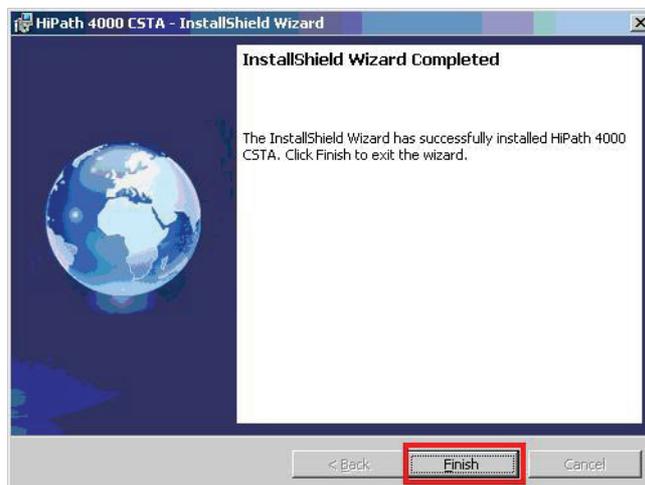


Figure 22 *InstallShield Wizard - Step 7*

Following successful installation, you will find the installed directories and files in:

C:\Program Files\Siemens\CSTA

## Software Installation

### Installation and Program Start with Windows



Figure 23 HiPath 4000 CSTA

A new program menu **CSTA** offers links to the **HiPath 4000 CSTA Administration Web Page (CBAAdmin)** and the **HiPath 4000 Phone Service Administration Web Page (XCIAdmin)**.

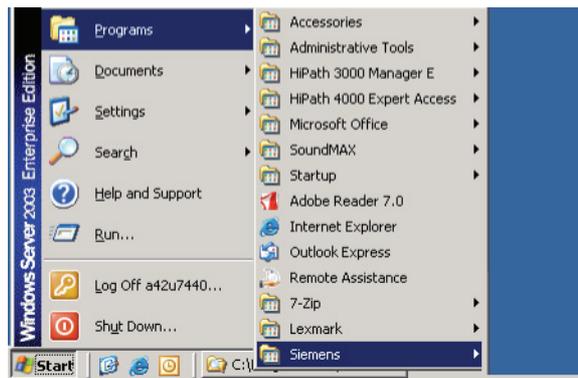


Figure 24 Start menu

A new Windows service has been created during the installation:

HiPath 4000 CSTA

This service will be started automatically when the system boots.

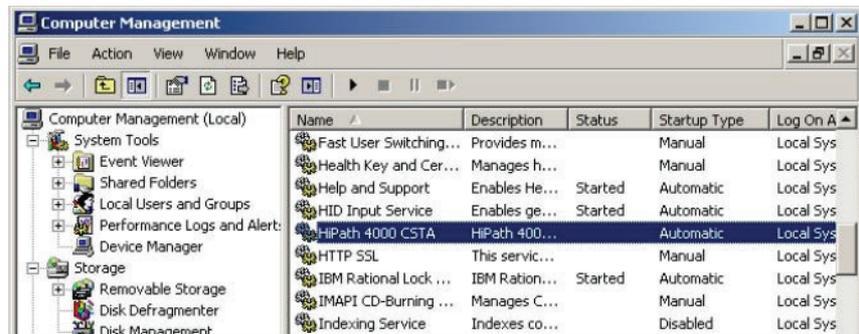


Figure 25 Service

## 5.2.2 Program Start

The Windows **HiPath 4000 CSTA** service starts automatically when the system boots. Please start this service manually directly after the installation in order to start the **HiPath 4000 CSTA CBAAdmin Web server**. This Web server is required to configure ConnectivityAdapter instances for HiPath 4000 V6 CSTA support.

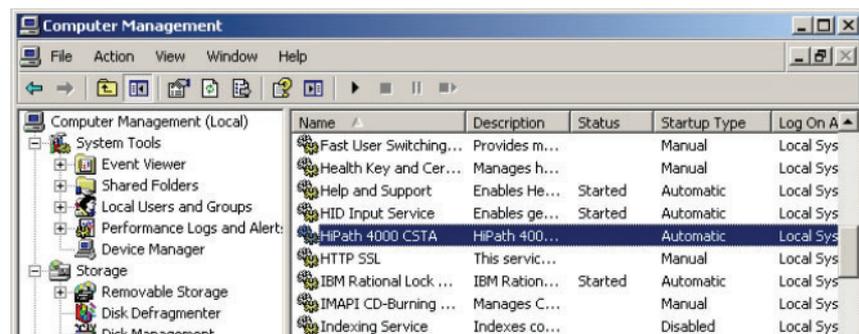


Figure 26 Program Start manually

Once the **HiPath 4000 CSTA** Windows service has started up successfully, you will find the active process `JSS.exe` listed in the Task Manager.

## Software Installation

### Installation and Program Start with Windows

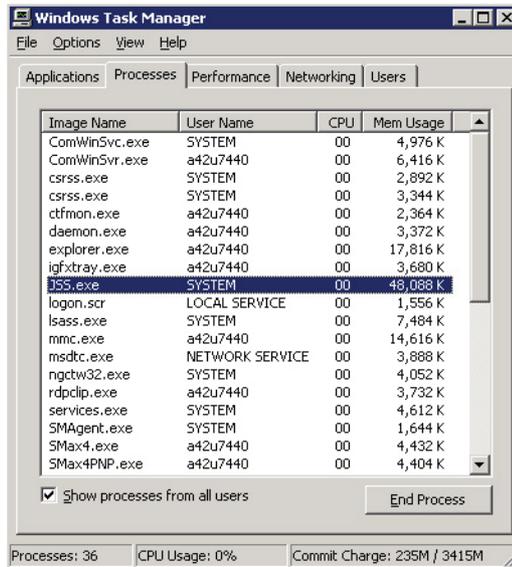


Figure 27 Windows Task Manager

---

**NOTE:** For each CA instance configured on this Web server, an individual `cbdriver4000.exe` process is also started.

---

## 6 Port List

The active **HiPath 4000 CSTA** process `jss` (or `jss.exe`) listens on the following ports (as tomcat);

- `http: 8080`
- `https: 8443/8081 - stand alone/V6 integrated variant`

In the case of a standalone installation, these are configurable. You can edit the file `../config/tomcat.cfg`.

This port offers Web access to:

- HiPath 4000 CSTA CAdmin Configuration Management
- HiPath 4000 Phone Service Management
- HiPath 4000 Phone Services

**XML Phone Service:** the `xci core java` process listens on port 3102 instead of `jss` (only a `java` process can be seen in `tcpview` or `netstat`).

The HiPath 4000 CSTA integrated version has a default configuration. A CA instance (`CA4000_Default`) is configured automatically during the rpm installation.

```
./distribution/exe/cbdriver4000 pbx=CA4000_HiPath4000_1
adminport=8914
```

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

1040 (HPPC), 2205 (XPR), 2209 (DTB) and 27535 (LiRus).

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

The PBX IP address is set to `192.0.2.3` which is the fixed Atlantic LAN IP address. This can only be modified in the stand alone version.

These application links are configured for internal products. The licensing mode is set to `no_license` for all of them.



## 7 CBAdmin Configuration Management

### Configuration steps - stand alone/external variant:

1. Add a new ConnectivityAdapter.
2. Select a Connectivity Adapter and modify the HiPath 4000 V6 connection parameters.
3. The ConnectivityAdapter will be restarted automatically.
4. Add a new application (link).

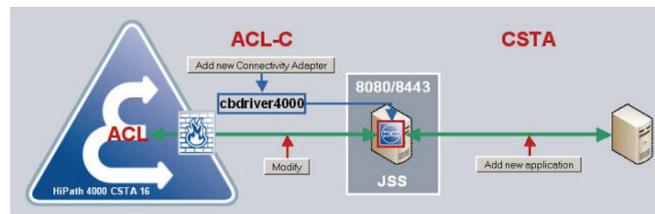


Figure 28 Configuration steps - stand alone/external variant

### Web connection

To reach the Admin Configuration Management site of HiPath 4000 CSTA integrated into the HiPath 400 V6 open the site of the **HiPath 4000 Assistant** and under the **Expert Mode** menu you can find the link to HiPath 4000 CSTA. See Chapter 8, “HiPath 4000 CSTA Switch Integrated – Introduction” for more information.

In case of stand alone/external installation use the Windows menu program link **CBAdmin** or enter the following URL in the address line of your browser:

`http://<HiPath 4000_CSTA_Server>:8080/CBAdmin`

or

`https://<HiPath 4000_CSTA_Server>:8443/CBAdmin`

### 7.1 Configuration

In case of stand alone/external variant/installation of HiPath 4000 CSTA enter the user name `Admin` and the default password `Admin` to log on to **HiPath 4000 CSTA CBAdmin Configuration Management**.

OpenScape4000 CSTA CBAAdmin	
User name	Admin
Password	*****
<input type="button" value="Login"/>	

Figure 29 Logon

---

**NOTE:** Make sure to change the default password the first time you log on!

---

---

**NOTE:** HiPath 4000 CSTA is integrated into the HiPath 4000 V6. SingleSignOn is used from the HiPath 4000 Assistant site to the HiPath 4000 CSTA Administration site so no additional manual authentication is needed - no account needs to be entered additionally into the HiPath 4000 CSTA site.

---

Once the software is installed, only the Web server is running.

No other **Connectivity Adapter** instance is configured yet (with the exception of the DEFAULT instance in case of HiPath 4000 V6 integrated installation).

A Connectivity Adapter can connect to the following HiPath 4000 versions:

- HiPath 4000 V6 - only in case of the HiPath 4000 CSTA integrated variant in HiPath 4000 V6
- HiPath 4000 V5
- HiPath 4000 V4

### HiPath 4000 CSTA CBAAdmin Configuration Management

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

#### Select Connectivity Adapter

Select Connectivity Adapter

Select Connectivity Adapter

Add new Connectivity Adapter

Remove selected Connectivity Adapter

Figure 30 Connectivity Adapter List - Add New ConnectivityAdapter

Enter the CA identification name and press **Add CA**.

#### Add New Connectivity Adapter



Figure 31 Connectivity Adapter List - Add CA

Based on this name, a configuration directory will be created in:

`<instDir>/config/<host name>/`

The full directory path is:

`<instDir>/config/<host name>/CA4000_HiPath 4000_1`

In case of SMR 13, a new component will be created in the database containing the settings of this CA (see also [Section 7.8, “Advanced Configuration for SMR 13”](#)), while in case of SMR 11 the above mentioned directory will contain the CA configuration file `ca4000.cfg`.

#### HiPath 4000 CSTA CBAAdmin Configuration Management

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

#### Select Connectivity Adapter

Connectivity Adapter successfully added!



Figure 32 Settings - Select Connectivity Adapter

Select the new CA instance and press **Select Connectivity Adapter** to

- enter the connection parameters for establishing the ACL-C link to HiPath 4000 Vx.
- add new HiPath 4000 CSTA application links.

## HiPath 4000 CSTA CBAAdmin Configuration Management

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

### CA4000\_HiPath4000CSTA\_1 Configuration

[advanced](#)

PBX Link Number	13
PBX Sub-App Number	23
IP address of the PBX	172.27.16.165
Maximum log file size	10

**Configured applications**

Status: RUNNING

Update Device List

Figure 33 Configuration - Modify

Enter the connection parameters to establish the ACL-C link to HiPath 4000 V6. Press **Modify** to restart the CA instance and to activate the new parameters.

---

**NOTE:** Make sure that only one CA instance is using this ACL link configuration. If a second CA instance uses the same link, neither of them will work! From HF R11.202.5 it is not possible to enter the same PBX Link and Sub-App. Number.

---

### CA4000\_Default Configuration

PBX Link Number	5
PBX Sub-App Number	25
Manufacturer Name	siemens
IP address of the PBX	192.0.2.3
Maximum log file size	10

**Configured applications**

Status: RUNNING

Update Device List

Figure 34 Configuration - Existing configuration

**Remark** to HiPath 4000 V6 integration: The ACL configuration for the first CA CA4000\_DEFAULT already exists with HiPath 4000 V6 KV18.

Press **Modify** to restart the CA instance and to activate the new parameters.

HiPath 4000 CSTA CBAAdmin Configuration Management

[Settings](#) | [Connectivity Adapter List](#) | [License Highlights](#) | [Configuration](#) | [Status](#) | [Log](#) | [Advanced Configuration](#) | [Statistics](#) | [Ver](#)

CA4000\_HiPath4000CSTA\_1 Configuration

Figure 35 Configuration

Press **OK** to restart the CA instance.

This means that after the initial configuration, the CA instance process will be started.

The process name is:

cbdriver4000  
cbdriver4000.exe for Windows.

Each individual CA instance will start up its own cbdriver4000 process. In fact, depending on the configuration, multiple cbdriver4000 processes could appear.

**Remark:** under Linux the new active process cbdriver4000, listed via `ps - ef`.

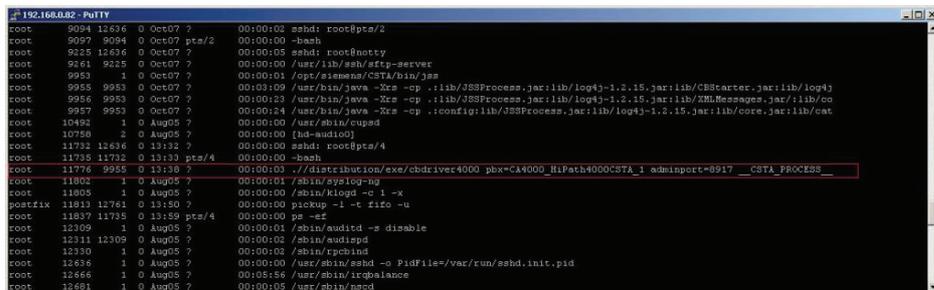


Figure 36 cbdriver4000 process

The new current status of the CA instance has to be **RUNNING**.

CA4000\_HiPath4000CSTA\_1 Configuration

[advanced](#)

PBX Link Number	13
PBX Sub-App Number	23
IP address of the PBX	172.27.16.165
Maximum log file size	10

Figure 37 Configuration - Add new application

Now add a new HiPath 4000 CSTA application link and press **Add new application**.

**Add new application**

Application name	CallCenter
TCP Port (1025-30000)	1040
Automatic Global Routing Trigger	NO
Monitor Filter	CSTA Standard
Private Data Version Number	4.1.0
Use External DNIS	No
License type	No license 100 clients Unlimited No license

For SEN application no license is needed. For 3rd party application type monitor points please apply the corresponding (100 clients / Unlimited etc) and consider that the ordered license based on the MAC address of the CSTA PC must be uploaded to CLA (via CLA GUI).

*Figure 38 Configuration - Add new application*

Enter an **Application name** (identifier) and a **TCP Port Number (1025-30000)**. The setting for **Use External DNIS** is optional and has to be set with respect to the connected application.

Select the application required **License type**:

- **No license**: max 10 monitored devices
- **100 clients**: max 100 monitored devices
- **Unlimited**: max 100000 monitored devices

---

**NOTE:** For Unify applications select **No license!**

---

Press **Add application** to complete this configuration.

**CA4000\_HiPath4000CSTA\_1 Configuration**

Application successfully added

PBX Link Number	5
PBX Sub-App Number	25
Manufacturer Name	siemens
IP address of the PBX	156.254.55
Maximum log file size	10

Configured applications	
CallCenter	
CommandControl	
PhoneService	
CallRecording	

Configured applications	
CallCenter	

Status: RUNNING

*Figure 39 Configuration - Configured applications*

The HiPath 4000 CSTA application's port configuration can then be modified or deleted.

The maximum number of supported HiPath 4000 CSTA connection ports per CA instance is 4.

---

**NOTE:** Every application link supports one CSTA III, ASN.1 or CSTA III, XML application connection.

---

## 7.2 Status – Connection Check

### ACL-C active, HiPath 4000 CSTA inactive

As can be seen from the current status, there is an active ACL-C connection (**PBX Link**) to HiPath 4000.

However, no application (**CallCenter**) has established a CSTA link.

In fact, no devices are monitored (**Used licenses**)!



CA4000\_HiPath4000CSTA\_1 Status

Used licenses	0
PBX Link	ConnectedAndActive
CallCenter	Disconnected

Figure 40

Status (CBAAdmin Configuration Management): ACL-C active, HiPath 4000 CSTA inactive

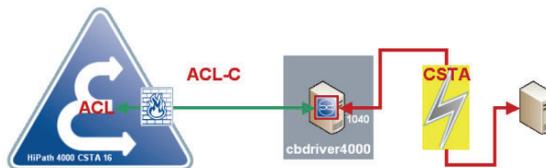


Figure 41

Status: ACL-C active, HiPath 4000 CSTA inactive

### ACL-C active, HiPath 4000 CSTA active

As can be seen from the current status, there is an active ACL-C connection (PBX-Link) to HiPath 4000.

The application (**CallCenter**) has established the CSTA link.

And 11 devices are monitored (**Used licenses**)!



CA4000\_HiPath4000CSTA\_1 Status

Used licenses	11
PBX Link	ConnectedAndActive
CallCenter	Connected

Figure 42

Status (CBAAdmin Configuration Management): ACL-C active, HiPath 4000 CSTA active

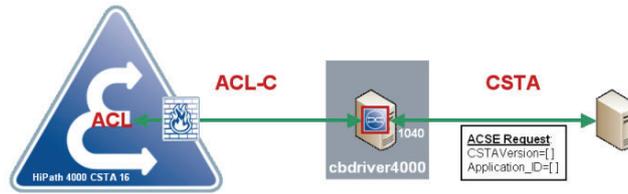


Figure 43

Status: ACL-C active, HiPath 4000 CSTA active

## 7.3 Logging

Every CA instance uses its own log directory! The default max log file size is set to 10 MB and can be modified via the CA instance configuration.

The active default log files are:

- error.log
- system.log
- debug.log

---

**NOTE:** Log file path structure: /<instDir>/siemens/CSTA/Logs/<host-name>/CA4000\_<instance-name>.

---

The logging menu differs in SMR 13 and in SMR 11/SMR 12.

### 7.3.1 Logging for SMR 13

Log > CA4000\_HiPath4000CSTA\_1\_logs



**CA4000\_HiPath4000CSTA\_1 log levels**

Error log	Show	Clear
System log	Show	Clear
Trace log	Show	Clear
Debug log	Show	Clear
All Logs		Clear All Logs

**Trace Control**

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

Figure 44 Log - Show/Clear

- **Show**  
Press **Show** to get an online log file output.
- **Clear**  
Press **Clear** to delete the log file contents.
- **Trace Control**  
The ACL/CSTA conversation trace can be enabled for a certain time.  
Select the messages you would like to write to the `trace.log`.  
Set the time **Time to trace (mins)**, this trace has to be active.
- **Update**  
Press **Update** to save your trace settings.

**Log > Download**

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



**Log**

Download System Diagnostic Data	
Configuration files	<input checked="" type="checkbox"/>
Log files	<input checked="" type="checkbox"/>
Download	

Figure 45 Log - Data download

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

**Log > Component log properties**

The log level (**Log level**), number of backup files (**Backup files count**) and log file size (**Max file size**) can be set for the different HiPath 4000 CSTA system components at the **Component log properties**.



**Component log properties**

Component	Log level	Backup files count	Max file size	
cbadmin	TRACE	5	5000	KB
cbstarter	TRACE	5	5000	KB
ccs	OFF	5	5000	KB
configdb	TRACE	5	5000	KB
jss	OFF	3	100	KB
oami	TRACE	5	5000	KB
tomcat	OFF	5	1000	KB
xci_core	TRACE	5	5000	KB
xci_gui	TRACE	5	5000	KB
Change				

Figure 46 Component log properties

### 7.3.2 Logging for SMR 11/SMR 12

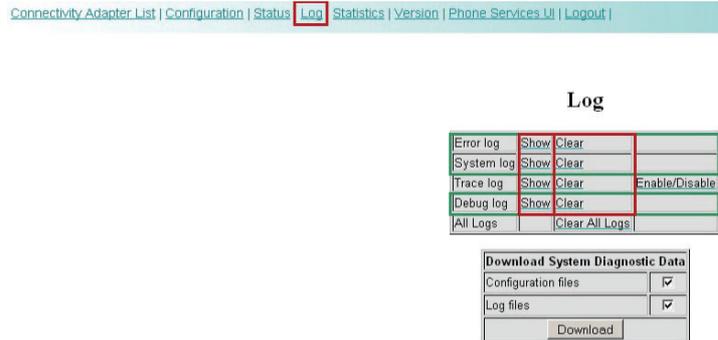


Figure 47 Log - Show/Clear

- **Show**  
Press **Show** to get an online log file output.
- **Clear**  
Press **Clear** to delete the log file contents.
- **Enable/Disable**  
The ACL/CSTA conversation trace can be enabled for a certain time.

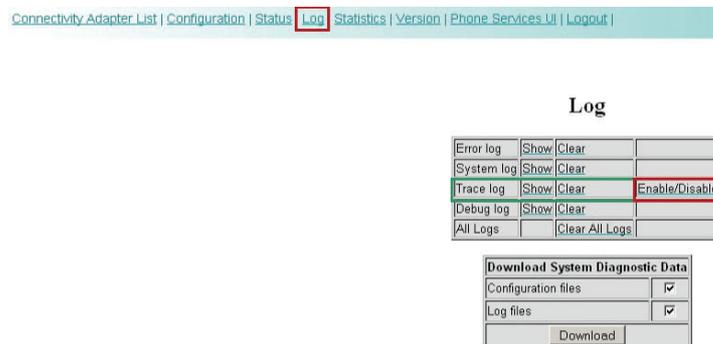


Figure 48 Log - Enable/Disable

Press **Enable/Disable**.

Select the messages you would like to write to the `trace.log`.

- **Download System Diagnostic Data**  
The complete configuration of all CA instances and all associated log files can be downloaded via the Admin Web page.

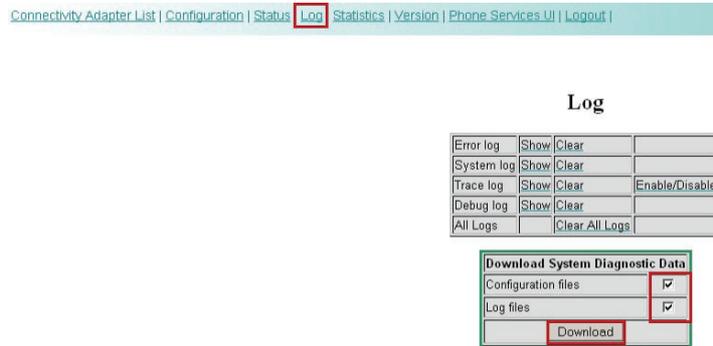


Figure 49 Log - Data download

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

- **Trace Control**

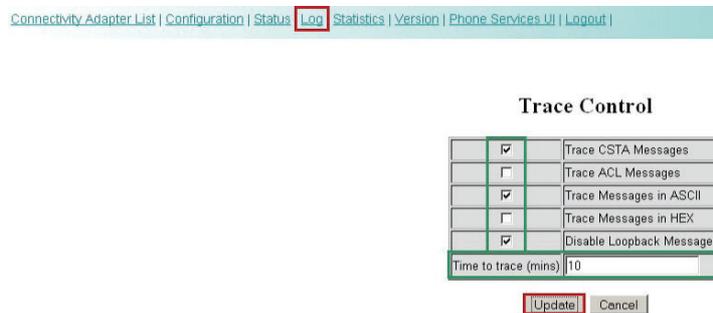


Figure 50 Log - Start trace

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

- **Update**

Press **Update** to save your trace settings.

## 7.4 Statistics

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

HiPath 4000 CSTA CBAAdmin Configuration Management

Settings | Connectivity Adapter List | License Highlights | Configuration | Status | Log | Advanced Configuration | **Statistics** | Version | Phone Services UI | Logout

CA4000\_HiPath4000CSTA\_1 Statistics

Refresh  
Clear All Stats  
Statistics from: Tue Nov 13 09:58:02 CET 2012  
To: Tue Nov 13 10:20:28 CET 2012

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

Connectivity Adapter -- PBX Communication		
	Received	Sent
ACL Msgs	98	95

Figure 51 Statistics

- Link Status**

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

Definition of the fields:

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

Table 1 Statistics - Link Status" section

- Connectivity Adapter – PBX Communication**

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

Definition of the fields:

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

Table 2 Statistics - "PBX Communication" section

- Application link

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

Definition of the fields:

Field	Explanation
Link Status	Indicates the link status. Possible values are: <b>Disconnected</b> – The CSTA link is down. <b>Active</b> – The CSTA link is up and messages have been transferred within the last 60 seconds . <b>Established</b> – The CSTA link is up but messages haven't been transferred within the last 60 seconds. <b>Missing heartbeat</b> – 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 HiPath 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. <b>Y</b> – ACSE session successfully negotiated. <b>N</b> – ACSE session not established.

Table 3 Statistics - "Application" section

Field	Explanation
CSTA Msgs	The total number of application level messages the CA-Driver received from and sent to the HiPath 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 HiPath 4000 CSTA application.
Peak Avg CSTA Msgs/sec	The highest number of CSTA messages sent per second and received from the HiPath 4000 CSTA application since the last clearing.
Peak Avg CSTA Msgs at	The date and time peak when CSTA message traffic occurred.

Table 3 Statistics - "Application" section

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

## 7.5 Version

Information about program components is provided in **Version**.

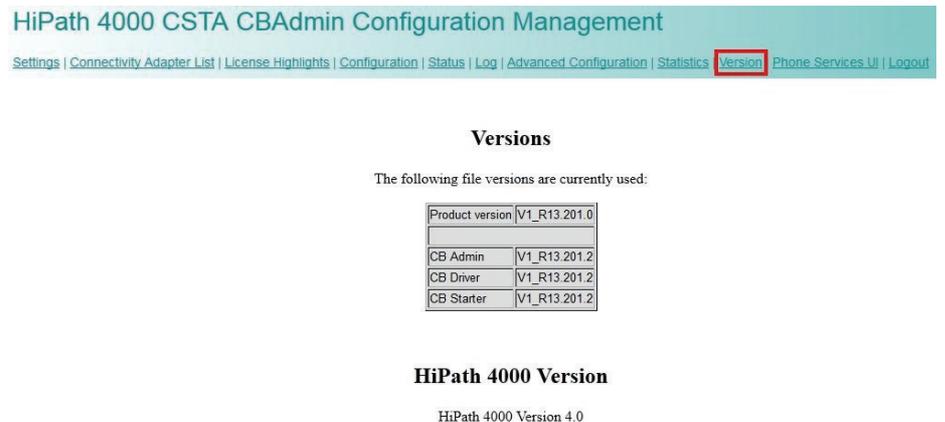


Figure 52 Version

## 7.6 Phone Service UI

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

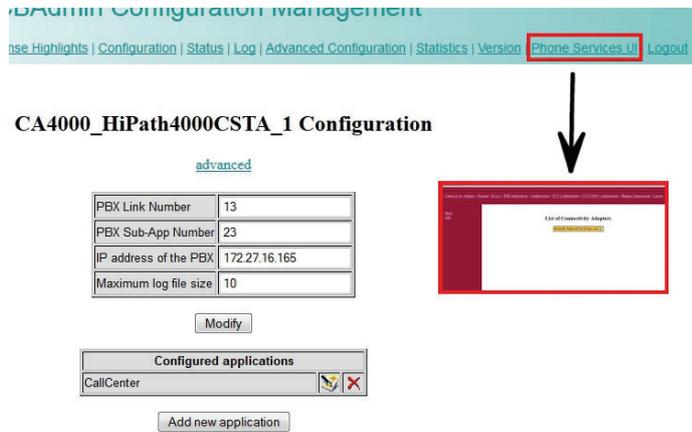


Figure 53 Phone Service UI

**NOTE:** This configuration will be explained later!

## 7.7 Settings

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

### 7.7.1 User/Password

For instance the default user and password can be changed.



**Settings**

**Change Administrator password**

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

Change password Cancel

Figure 54 Change default user and password

## 7.7.2 HTTPS Connection

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

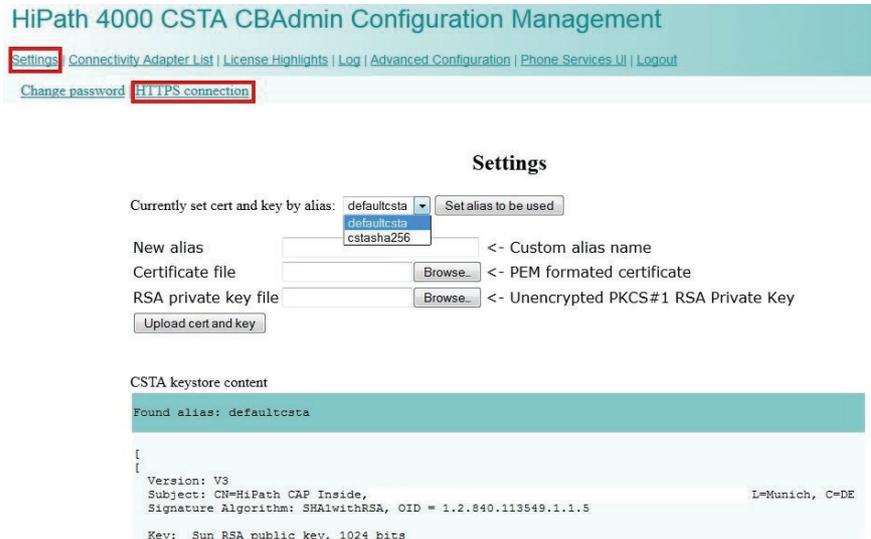


Figure 55 HTTPS Connections

### 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 must be restarted.

There are two built-in certificates/private keys in HiPath 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 HiPath 4000 Phone Services software won’t be able to connect to HiPath 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, HiPath 4000 CSTA provides a way to upload these files into HiPath 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.

#### HiPath 4000 CSTA keystore content

This is the full content of HiPath 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).

---

**NOTE:** In case of HiPath 4000 V6 integrated HiPath 4000 CSTA, the CBAAdmin and Phone Services graphical user interface is accessed through the HiPath 4000 Assistant, therefore its certificate is being used as well. The communication with the HiPath 4000 Phone Services (prev. XCI Tray) is still done using HiPath 4000 CSTA's own certificate.

---

## 7.8 Advanced Configuration for SMR 13

In SMR 11 and SMR 12 of HiPath 4000 CSTA the configurations were stored in configuration files. In SMR 13, all of the configurations are stored in HiPath 4000 CSTA's own database, and an easy to use graphical user interface is presented in case any modification is required.

### HiPath 4000 CSTA CBAAdmin Configuration Management

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

#### Advanced Configuration

Component type: ca4000 Component: CA4000\_HiPath4000CSTA\_1

Name	Value	Delete
ACL_SERVER_IP_ADDR	172.27.16.165	<input type="checkbox"/>
GW_LINK_ID	13	<input type="checkbox"/>
GW_SUBAPPL_ID	23	<input type="checkbox"/>
GW_TRACE_CONTROL	0	<input type="checkbox"/>
GW_TRACE_TIME_END	0	<input type="checkbox"/>
KEEPALIVE	1	<input type="checkbox"/>
TCP_PORT_TYPE_2	2	<input type="checkbox"/>
USE_EXTERNAL_DNIS_2	0	<input type="checkbox"/>

Export	Import
<input type="button" value="Export"/>	<input checked="" type="checkbox"/> Keep values <input type="button" value="Browse..."/>
	<input type="button" value="Import"/>

New component	
Component type:	log4j.properties
Name:	<input type="text"/>
<input type="button" value="Add"/>	

Figure 56 Advanced Configuration - Component selection

#### Structure of the page:

Two listboxes are on the top of the page. With these, the user can select the configuration type (**Component type**) and the configuration (**Component**) which he wants to view/edit. After the selection the page will reload, and will show the configuration parameters and values in a table. Then the user can modify, delete or add entries.

The user can do more than one modifications at the same time and save them all together at the same time at the end.

#### Delete, modify or add entries

- Delete

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

- Modify

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

- **New setting**

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

**Save**

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

**Export/Import:**

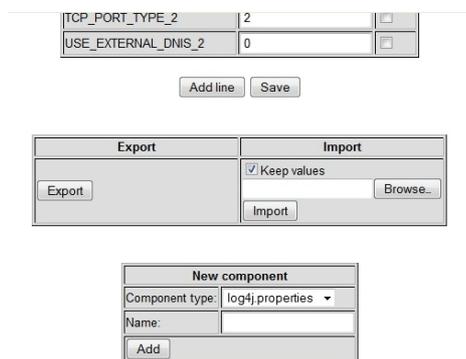


Figure 57 Advanced Configuration - Export/Import

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 part of or the whole configuration in a zip file. If nothing is selected then the whole configuration will be downloaded. If any of the component or the component type is chosen then the appropriate part will be downloaded.

Structure of the .zip file:

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

- **Import**

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

The user can create its own components. For this, a name and a type have to be chosen. The name should be unique in its component type.

For the modification to take effect the user needs to restart the HiPath 4000 CSTA service (in HiPath 4000 V6 systems the tomcat5 service too). If the config type is **ca4000** it is enough to restart the **cbdriver**. The application offers the possibility to restart it (or the user can do it later himself).

## 7.9 Logout

**Logout** will terminate the current session.

HiPath 4000 CSTA CBAAdmin Configuration Management

Logged out! Please close the browser!

*Figure 58*

*Logout*



## 8 HiPath 4000 CSTA Switch Integrated – Introduction

HiPath 4000 CSTA Switch Integrated is installed as part of the image installation of a HiPath 4000 V6 installation and offers some additional useful features:

- CBAAdmin Web server **single sign on** access via HiPath 4000 Assistant
- Default configuration of the first CA instance during the rpm 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 HiPath 4000 Assistant (Software Activation)
- HiPath backup and restore support for configuration data only
- Full image system backup and restore (only in case of SMR 11)

### 8.1 Application Environment

#### Port list

HiPath 4000 CSTA Switch Integrated image installation is preconfigured. A cbdriver instance (CA4000\_Default) uses the ACL PBX Link=5 and SubApp1=25. The PBX IP address is set to 192.0.2.3 which is the fixed Atlantic LAN IP address.

This default CA has 4 applications configured, which listen on the following ports:

1040 (HPPC), 2205 (XPR), 2209 (DTB) and 27535 (LiRus).

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

These application links are configured for internal products. The licensing mode is set to `no_license`.

#### Daemons

The processes are started automatically when the system reboots.

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

- `/etc/init.d/tomcat5`
  - `{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

### Directories

The default installation directory for tomcat5 is:

```
/srv/www/tomcat5
```

The Web pages are hosted in:

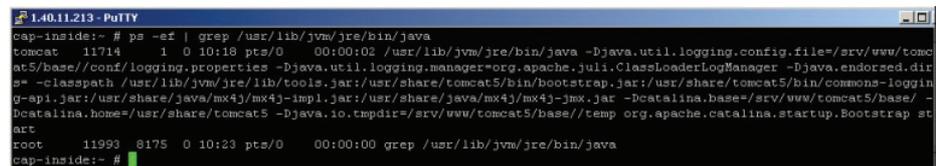
```
/srv/www/tomcat5/base/webapps
```

The default installation directory for HiPath\_4000\_CSTA is:

```
/opt/siemens/CSTA
```

### Active processes

Unlike a single installation, the HiPath 4000 CSTA Web Administration Server starts at run level 3 - 5. The demon name is tomcat5. A new process is responsible for this: java.



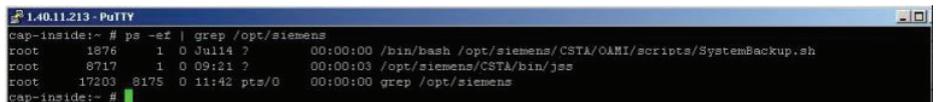
```
cap-inside:~ # ps -ef | grep /usr/lib/jvm/jre/bin/java
tomcat 11714 1 0 10:18 pts/0 00:00:02 /usr/lib/jvm/jre/bin/java -Djava.util.logging.config.file=/srv/www/tomcat5/base/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.endorsed.dirs=-classpath /usr/lib/jvm/jre/lib/tools.jar:/usr/share/tomcat5/bin/bootstrap.j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

Figure 59 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 the system backup.



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

Figure 60 bash process

By default, the CA instance **CA4000\_Default** is created automatically during the rpm installation. It includes the complete HiPath 4000 ACL AMO configuration.

```

1.40.11.213 - PuTTY
cap-inside:~ # ps -ef | grep .//distribution/exe/cbdriver4000
root      8743  8717  0 09:22 ?        00:00:00 .//distribution/exe/cbdriver4000 pbx=CI4000_Default adminport=8914
    
```

Figure 61 *cbdriver4000 process*

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

### HiPath 4000 V6 Switch Integrated HiPath 4000 CSTA IP configuration

As for the HiPath 4000 Platform Administration (Portal) and HiPath 4000 Assistant, the HiPath 4000 CSTA needs its own IP address in the customer LAN, which is configured on `eth1`.

`eth2` is configured on the other side for internal communication. Another process is therefore started to link the internal Web services to the NIC `eth2`.

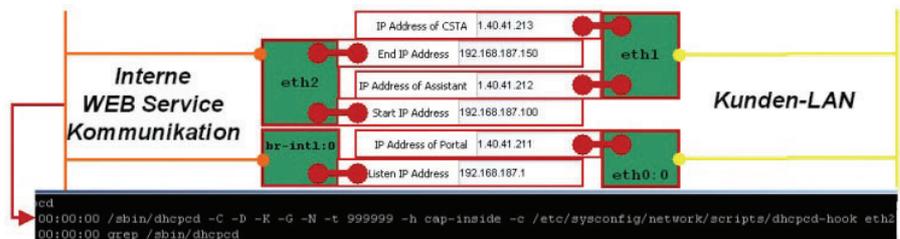


Figure 62 *Internal WEB Service Communication*

The portal also has connections to both LAN networks.

`eth0` 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.

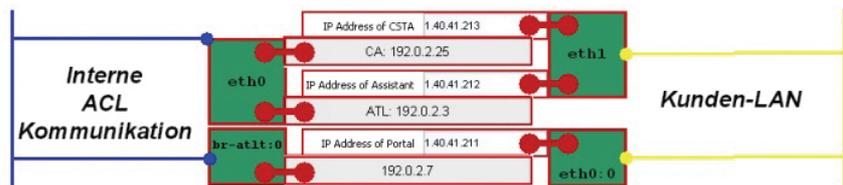


Figure 63 *Internal ACL Communication*

## 8.2 Portal – IP Address Configuration

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

**Expert Mode > Platform Portal**

**HiPath 4000 CSTA Switch Integrated – Introduction**  
**Portal – IP Address Configuration**

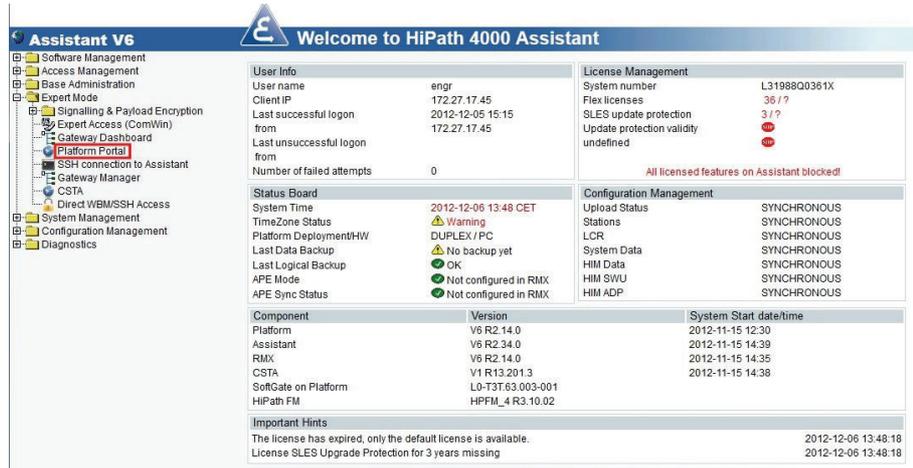


Figure 64 Connect to HiPath 4000 Platform Administration (Portal)

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



Figure 65 System

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

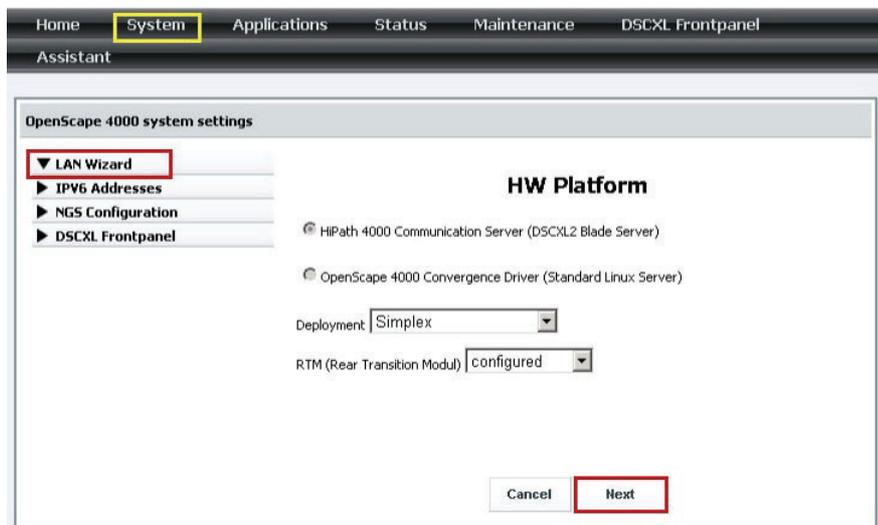


Figure 66 System - LAN Wizard - Step 1

Press **Next**.

Home **System** Applications Status Maintenance DSCXL Frontpanel  
Assistant

OpenScape 4000 system settings

- LAN Wizard
- IPV6 Addresses
- NGS Configuration
- DSCXL Frontpanel

### IPDA LAN

Ethernet Interface Node	eth0
Netmask	255.255.255.0
VLAN ID	0
VLAN Tag	0
CCA IP Address	1.40.41.70
Default Router	1.40.41.254
NGS IP Address	1.40.41.214

Back Cancel **Next**

Figure 67 System - LAN Wizard - Step 2

Enter the HiPath 4000 CSTA IP address.

- LAN Wizard
- IPV6 Addresses
- NGS Configuration
- DSCXL Frontpanel

### Customer LAN

Ethernet Interface Node	eth0
IP Address of Portal	1.40.41.211
Netmask	255.255.255.0
VLAN ID	0
VLAN Tag	0
IP Address of Assistant	1.40.41.212
IP Address of CSTA	1.40.41.213
Default Router of Customer LAN	1.40.41.254

### Atlantic LAN

Ethernet Interface Node	eth6
Ethernet Interface 2 Node	eth7
Ethernet Interface 3 Node	
Ethernet Interface 4 Node	

Back Cancel **Next**

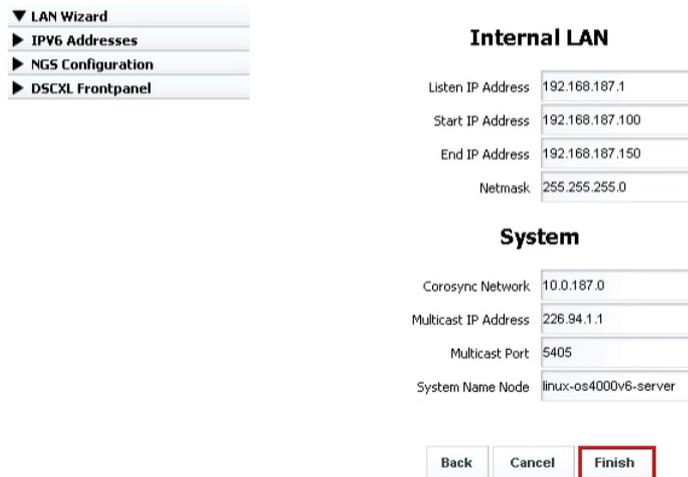
Figure 68 System - LAN Wizard - Step 3

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

Press **Next**.

## HiPath 4000 CSTA Switch Integrated – Introduction

### CBAdmin – Trusted IP Addresses



Internal LAN	
Listen IP Address	192.168.187.1
Start IP Address	192.168.187.100
End IP Address	192.168.187.150
Netmask	255.255.255.0

System	
Corosync Network	10.0.187.0
Multicast IP Address	226.94.1.1
Multicast Port	5405
System Name Node	linux-os4000v6-server

Back Cancel **Finish**

Figure 69 System - LAN Wizard - Step 4

Press **Finish**.



Home **System** Applications Status Maintenance DSCXL Frontpanel

Assistant

OpenScope 4000 system settings

- ▼ LAN Wizard
- ▶ IPV6 Addresses
- ▶ NGS Configuration
- ▶ DSCXL Frontpanel

**Action successfully completed.**

Installation Log File

Figure 70 Wizard completed

## 8.3 CBAdmin – Trusted IP Addresses

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



Settings

**Trusted IP addresses/masks**

172.27.17.45

Remove

Add

Save changes    Cancel

**What is this?**

These are the ip addresses (and netmasks) that are allowed to access the CSTA VM on port 102. For example the following entries would be valid:

192.168.0.63  
 172.36.27.174/255.255.255.0  
 112.87.63.108/255.255.255.192

Note that there is no validity check, however in case a malformed expression is beings used then it will be automatically skipped at the actual firewall settings.

Figure 71 Trusted IP addresses

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

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

## 8.4 CBAAdmin – CA Instance Configuration

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

**Expert Mode > CSTA**

Component	Version	System Start date/time
Platform	V6 R2-14.0	2012-11-15 12:30
Assistant	V6 R2-34.0	2012-11-15 14:39
RMX	V6 R2-14.0	2012-11-15 14:35
CSTA	V1 R13 201.3	2012-11-15 14:38
SoftGate on Platform	L0-T3T.63.003-001	
HiPath FM	HPFM_4 R3.10.02	

Figure 72 Connect to HiPath 4000 CSTA

The CA instance **CA4000\_Default** is created and configured automatically during the rpm installation.

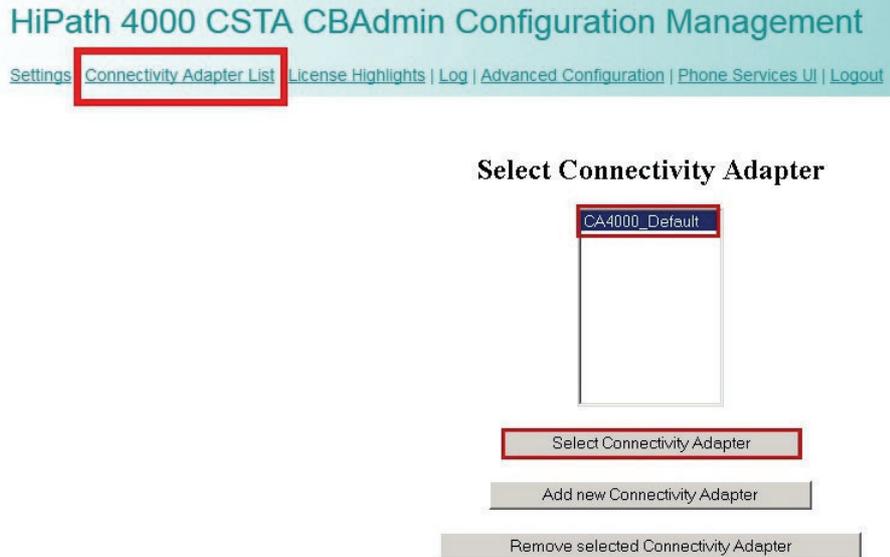


Figure 73 Connectivity Adapter List - Select Connectivity Adapter

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

### CA4000\_Default Configuration

PBX Link Number	5
PBX Sub-App Number	25
Manufacturer Name	siemens
IP address of the PBX	192.0.2.3
Maximum log file size	10

Modify

Configured applications	
app_1040	
app_27535	
app_2205	
app_2209	

Add new application

Status: RUNNING

Start Stop

Update Device List

Figure 74 Configuration - CA4000\_Default Configuration

The default connection parameters are:

- **PBX-Link Number:** 5

- **PBX Sub-Appl Number:** 25
- **IP Address of the PBX:** 192.0.2.3

Configured applications:

- **app\_1040:** Port 1040
- **app\_27535:** Port 27535
- **app\_2205:** Port 2205
- **app\_2209:** Port 2209

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



### Select Connectivity Adapter



Figure 75 Connectivity Adapter List - Add New Connectivity Adapter

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

### Add New Connectivity Adapter



Figure 76 Add CA

Enter the name of the new CA Instance and press the button **Add CA**.

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

## HiPath 4000 CSTA CBAdmin Configuration Management

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

### Select Connectivity Adapter

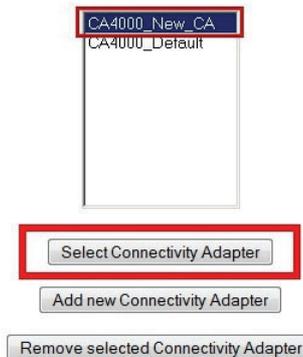


Figure 77 Connectivity Adapter List - Select Connectivity Adapter

Enter new and not yet existing (used) **PBX-Link Number**, **PBX Sub-App Number** and the **IP Address of the PBX**:

- **PBX-Link Number:** 6
- **PBX Sub-App Number:** 26
- **IP Address of the PBX:** 192.0.2.3

## HiPath 4000 CSTA CBAdmin Configuration Management

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

### CA4000\_New\_CA Configuration

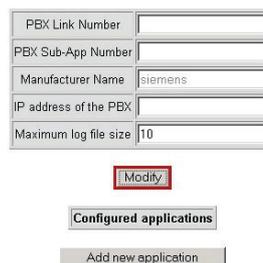


Figure 78 Configuration - Modify

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

Press **Modify**.

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

## HiPath 4000 CSTA CBAAdmin Configuration Management

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

### CA4000\_New\_CA Configuration

PBX Link Number	6
PBX Sub-App Number	26
Manufacturer Name	siemens
IP address of the PBX	192.0.2.3
Maximum log file size	10

Figure 79 Configuration - Add new application

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

## HiPath 4000 CSTA CBAAdmin Configuration Management

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

### Add new application

Application name	<input type="text"/>
TCP Port (1025-30000)	<input type="text"/>
Automatic Global Routing Trigger	<input type="button" value="NO"/>
Monitor Filter	<input type="button" value="CSTA Standard"/>
Private Data Version Number	<input type="button" value="4.1.0"/>
Use External DNIS	<input type="button" value="No"/>
License type	<input type="button" value="No license"/> <input type="button" value="100 clients"/> <input type="button" value="Unlimited"/> <input type="button" value="No license"/>
<input type="button" value="Add application"/>	

Figure 80 Configuration - Add application

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

Select a **License type** and press **Add application**.

---

**NOTE:** For internal Unify applications, select No license.

---

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

### CA4000\_New\_CA Configuration

Application successfully added

PBX Link Number	6
PBX Sub-App Number	26
Manufacturer Name	siemens
IP address of the PBX	192.0.2.3
Maximum log file size	10

Modify

Configured applications	
XMLPS	

Add new application

Status: RUNNING

Figure 81 Configuration - XMLPS

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

### HiPath 4000 CSTA CBAAdmin Configuration Management

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

#### Status

Used licenses	0
PBX Link	ConnectedAndActive
XMLPS	Disconnected

Figure 82 Status - PBX Link

Also the link status of the application connection is shown as well as the number of **Used licenses** (number of active monitor flags)

## 8.5 Additional Supported Services

Log on to **HiPath 4000 V6 Assistant** and select.

- **Software Management**
  - **Backup & Restore**
  - **Software Activation**
  - **Software Transfer**

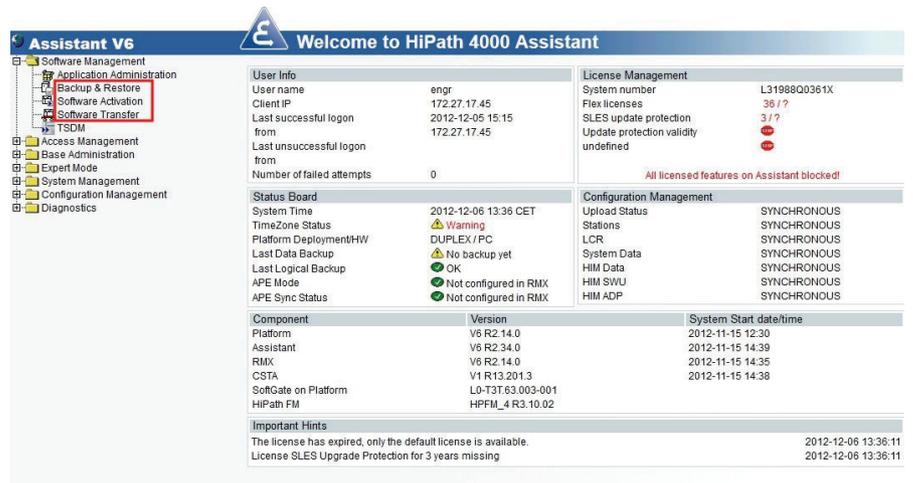


Figure 83 Connection to Backup & Restore, Software Activation/Transfer

- **Backup & Restore**
  - **BEER\_CSTA (configuration)**
    - **Backup**
    - **Restore**

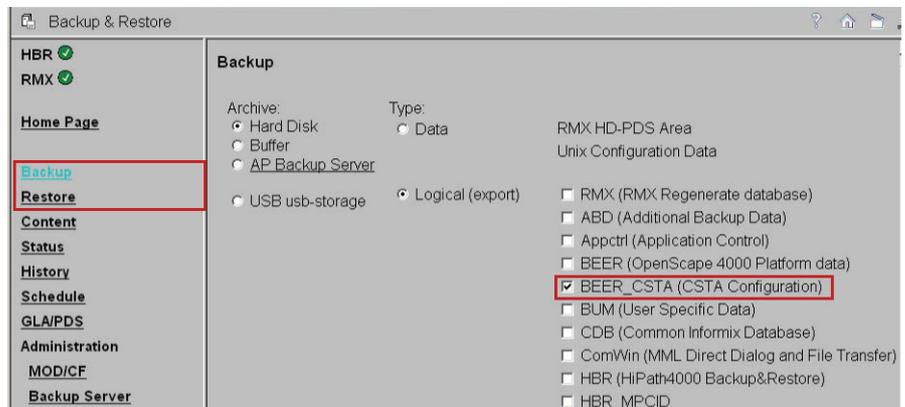


Figure 84 Backup & Restore - BEER\_CSTA (configuration)

In case of SMR 11 System Backup and Restore are supported:

Log on to **HiPath 4000 V6 Assistant** and select the option below:

**Expert Mode > Platform Portal**

In HiPath 4000 Platform Administration (Portal) select

**Maintenance > System Backup > Backup**

or

**Maintenance > System Backup > Restore**

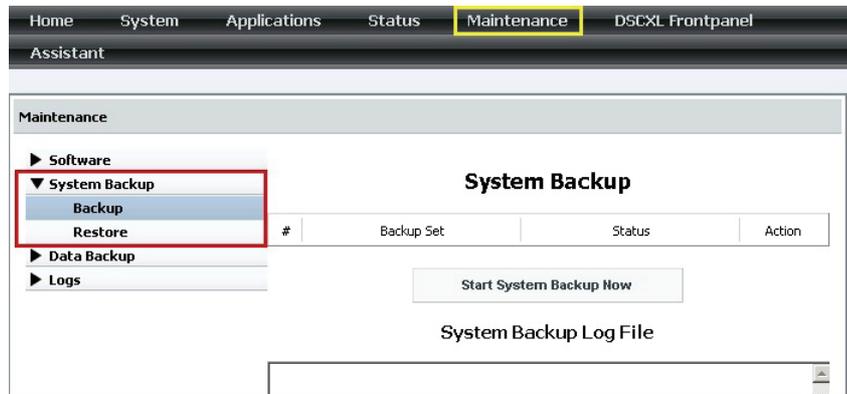


Figure 85 Maintenance - System Backup - Backup

## 8.6 Changing of the Configuration File

### 8.6.1 Configuration Change for SMR 11

In case of SMR 11 for some specific Connectivity Adapter configuration settings there is no possibility to change these via the HiPath 4000 CSTA graphical user interface. The changes must be done in the configuration files.

Therefore it is needed to log into the HiPath 4000 CSTA VM, for example with **putty** application. Use the CLAN IP address of the HiPath 4000 CSTA VM and the root account.

Under the directory `/opt/siemens/CSTA/config/Connections` you can find the configuration files of the corresponding Connectivity Adapter, that you can edit with an editor like `joe`.

After changing the configuration file you need to restart the corresponding Connectivity Adapter to take the changes effect.

### 8.6.2 Configuration Change for SMR 13

In case of SM 13 some specific Connectivity Adapter configuration settings can be changed only in the **Advanced Configuration** menu. There are two ways to reach the cbdriver specific settings in the CBAAdmin graphical user interface.

Select the **Advanced Configuration** menu and pick the ca4000 **Component type** and the Connectivity Adapter that needs to be modified from the **Component** drop down menu.

HiPath 4000 CSTA CBAAdmin Configuration Management  
[Settings](#) | [Connectivity Adapter List](#) | [License Highlights](#) | [Configuration](#) | [Status](#) | [Log](#) | **Advanced Configuration** | [Statistics](#) | [Version](#) | [Phone Services UI](#) | [Logout](#)

Advanced Configuration

Component type: ca4000    Component: CA4000\_HiPath4000CSTA\_1

Name	Value	Delete
ACL_SERVER_IP_ADDR	172.27.16.165	<input type="checkbox"/>
GW_LINK_ID	13	<input type="checkbox"/>
GW_SUBAPPL_ID	23	<input type="checkbox"/>
GW_TRACE_CONTROL	0	<input type="checkbox"/>
GW_TRACE_TIME_END	0	<input type="checkbox"/>
KEEPALIVE	1	<input type="checkbox"/>

Figure 86      Advanced Configuration - ca4000 component

If a connectivity adapter is already selected from the Connectivity Adapter list then there is also a direct link to this page named **advanced** from the **Configuration** menu.

HiPath 4000 CSTA CBAAdmin Configuration Management  
[Settings](#) | [Connectivity Adapter List](#) | [License Highlights](#) | [Configuration](#) | [Status](#) | [Log](#) | **Advanced Configuration** | [Statistics](#) | [Version](#) | [Phone Services UI](#) | [Logout](#)

CA4000\_HiPath4000CSTA\_1 Configuration

[advanced](#)

PBX Link Number	
PBX Sub-App Number	
IP address of the PBX	192.0.2.3
Maximum log file size	10

**Configured applications**

Status: RUNNING

Update Device List

Figure 87      Advanced Configuration - ca4000 direct link

Changes made in connectivity adapter settings require the CA to be restarted. This can be done on the Connectivity Adapters **Configuration** page.

## 8.6.3 Special Settings

### 8.6.3.1 Concept of “Presentation Indicator for Devices” in CSTA Events

To provide adaptable working cases for every application, CA4000 will have three different ways to handle the presentation indicator for devices. The different solutions can be activated in the configuration of CA4000. The parameter PRESENTATION\_RESTRICTED should be set to the following values:

- **normal**: to provide the old concept as it worked in the past (valid for CSTA3)
- **ignore**: to have the presentation restricted **partially ignored** (valid for CSTA3); this is **only a work around** for HiPath ProCenter, which should also use **private data** from now on.
- **private data**: presentation indicator will be shown by the private data (valid only for CSTA3 interface, in case this solution is set in the configuration file)  
e.g.: PRESENTATION\_RESTRICTED = private data

- **extended private data**: a new concept of the presentation indicator introduced in HiPath 4000 V4 and V5 with which the switch delivers presentation restricted information not only in the case of calling and called party.

All presentation indicators will be represented by private data (valid only for CSTA3 interface, in case this solution is set in the configuration file, CSTA1 will work as **normal**)

PRESENTATION\_RESTRICTED=private data

ALLOW\_ALL\_PRIVATE\_DATA=True

- **special**: similar to the function of **normal** but instead provides possibility for the HiPath 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>

---

**NOTE:** The application offers the choice when to switch-over to one of the **private data**. By default, the parameter PRESENTATION\_RESTRICTED and ALLOW\_ALL\_PRIVATE\_DATA are not included in the CA4000 configuration.

---

If these parameters are not in the configuration then the **normal** behavior will be activated automatically. CA4000 reads the configuration in case of start or restart, so any change will only be valid after the **start** or **restart**.

### 8.6.3.2 Delayed CSTA Request 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 was always posAck'ed by ACL and the application is not informed about any failure of the diversion.

There are options in HiPath 4000 CSTA to configure it for special cases (i.e. for Deflect and Single Step Transfer services) 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:

---

**NOTE:** ACL changes were necessary to support this option, hence the relevance of the used HiPath 4000 versions.

---

1. CSTA3\_DELAY\_DEFLECT\_CALL\_RESP=1

If the CSTA Deflect Call is used only for RCGs and the target is the calling party.

The option can be used from HiPath 4000 V5.

2. CSTA3\_DELAY\_DEVICE\_DEFLECT\_CALL\_RESP=1

If the CSTA Deflect Call is applied on digital and analog subscribers, 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 posAck'ed by ACL and the application is not informed about any failure of the transfer.

---

**NOTE:** ACL changes were necessary to support this option, hence the relevance of the used HiPath 4000 version.

---

3. CSTA3\_DELAY\_SST\_CALL\_RESP=1

The 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.

#### 8.6.3.3 CSTA Accept Call and Offered Event

In HiPath 4000 V6 R1 a new feature was introduced and HiPath 4000 CSTA provides the support of CSTA Accept Call service in case of offered mode of a digital device.

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

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

---

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

---

Please be aware that switching on the offered mode will result in a delay of 2 seconds of the ring tone and the DELIVERED events.

Offered mode can be switched on, on a per cbdriver basis and the 2 seconds delay will appear on the phones monitored by an application connected to this cbdriver.

In the HiPath 4000 CSTA no special setting is needed to be able to use this feature.

#### 8.6.3.4 Delivering deviceIDs in E.164 Format (SFR international)

This feature is introduced in HiPath 4000 V6 R2. The feature can be switched on using a configuration parameter in the corresponding ca4000 configuration:

```
E164_NUMBER_FORMAT=1
```

You can add this parameter into the corresponding configuration file. This Connectivity Adapter must be restarted to take effect this setting.

This modification can be made in the **Advanced Configuration** menu by selecting the cbdriver that you wish to edit.

This configuration parameter is valid for a cbdriver, so if it is switched on, all the applications connected to it will have the numbers in E.164 format.

##### Monitor events

E.164 number format is provided in the DeviceID field that normally contains a dialed number if it is provided for every call control and agent state events, maintenance events. It will appear in the following fields:

- Added party

- Alerting device
- Answering device
- Associated called device
- Associated calling device
- Called device
- Calling device
- Conferencing device
- Dialling device
- Diverting device
- Failing device
- Holding device
- Initiating device
- Last redirection device
- Network called device (if the information is provided)
- Network calling device (if the information is provided)
- New destination
- Offered device
- Releasing device
- Retrieving device
- Transferred to device
- Transferring device

#### **Services**

- If the feature is switched on, Monitor Start Request must contain the E.164 number. Monitor start request without it is rejected on HiPath 4000 CSTA level.
- Conference, Alternate, Transfer and Reconnect requests are only sent to ACL when the device IDs are the same. As the whole E.164 logic is in the switch, it can not be read on CA4000 level if it is the same number just in different formats. Requests with a different device ID format will be rejected because CA4000 is unable to tell which number is supposed to be sent to ACL.
- Other service requests are let through HiPath 4000 CSTA with either extension or E.164 number. ACL will determine the extension from it.

#### Restrictions, limitations

- During a normal call setup the called party in the ORIGINATED event there, is not in E.164 format. At this point the party belonging to the dialed number could 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.

#### 8.6.3.5 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 HiPath 4000 CSTA again, since the corresponding application port of the HiPath 4000 CSTA remains busy for a longer time.

From the version HiPath 4000 CSTA HF R11.202.13 the following additional special settings have been introduced to solve this issue. This is 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 ca4000 configuration.

If not configured in ca4000, 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.

### 8.6.3.6 Special setting to deliver keyset information via HiPath 4000 CSTA

No multiline appearance (keyset) support via HiPath 4000 CSTA.

However in case of a special problem, there are changes introduced in the product, which can be activated.

Problem with a CTI application: When a call arrived to the keyset device, which is monitored, the call was answered by its secondary line, and in this case the middleware delivered no information in the Established Event about the real answering device (secondary line), only the keyset number - the information of the logical device is delivered to the Called Device file. So the CTI application could've used only the keyset number as a source in the ConnectTimeslot Request, however that was not in call, but instead its secondary line. Therefore the recording of that call was not possible.

Solution is implemented for this problem:

Physical device ID is sent out in the private data field of the CSTA\_ESTABLISHED\_EVENT. New private data field i.e. 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 ca4000 entry:

```
ALLOW_PHYSICAL_APPEARANCE = 1
```

This feature is inactive, if no such entry is written in the configuration file of the corresponding Connectivity Adapter.

### 8.6.3.7 Umlaut Characters

The CSTA ASN1 does not support umlaut characters. CA4000 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 HiPath 4000 CSTA, ASN1 interface is used, you must use a configuration parameter in ca4000 configuration (**Advanced Configuration** menu in SMR 13 or the corresponding ca4000.cfg file in SMR 11) to "de-umlaut" them. This activates a conversion from CORNET TS characters to latin ascii.

```
USE_ACCENTED_CHARACTERS=0
```

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

#### 8.6.3.8 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.

#### 8.6.3.9 UserToUser Info (SMR 13)

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

```
CALL_FAILED
CALL_FORWARDED
CALL_GROUP-QUEUED
CALL_OFFERED
CALL_QUEUED
HOLDING_STATE
ORIGINATED_STATE
RING_STATE
ROUTE_TABLE_SELECTED
```

Make call request will also support the private element.

#### 8.6.3.10 Usage with OpenSape Contact Center (OSCC)

In case HiPath 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
```

## 9 Phone Services – Introduction

HiPath 4000 V6 offers a number of small, user-friendly applications that are integrated and *free of charge*:

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

**HiPath 4000 Phone Services** is a package of XMLPS applications provided together with HiPath 4000 CSTA and therefore also with HiPath 4000 V6. It is aimed at optiPoint and OpenStage display phone and optiClient and CMI/ Cordless phone users and offers a set of innovative features to enhance productivity at the workplace.

**HiPath 4000 Phone Services** functions as described subsequently are implemented as XMLPS applications in HiPath 4000 CSTA. They are available on every type of installation, integrated, external Linux and external Windows. Multiple HiPath 4000 V6 can be connected to the same **HiPath 4000 Phone Service Server**.

### 9.1 Overview

#### 9.1.1 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 a calling party (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 88 *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, press **OK** key (as illustrated).

### 9.1.2 EasySee

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

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

#### Example of use:

- Identification of unknown called / calling parties

---

**NOTE:** **EasySee** requires a locally installed program **HiPath 4000 Phone Services (prev. XCI Tray)**. The **EasySee** function can also be invoked from the HiPath 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 89 EasySee

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

### 9.1.3 EasyMail

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

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

#### Example of use:

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

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



Figure 90 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.

### 9.1.4 EasyShare

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

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

---

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

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

---



Figure 91 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.

## 9.1.5 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 HiPath 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)

---

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

---

**Phone Services – Introduction**  
**Structure**



Figure 92 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).

**9.2 Structure**

**Overview – Single connected HiPath 4000 CSTA in case of HiPath 4000 V6**

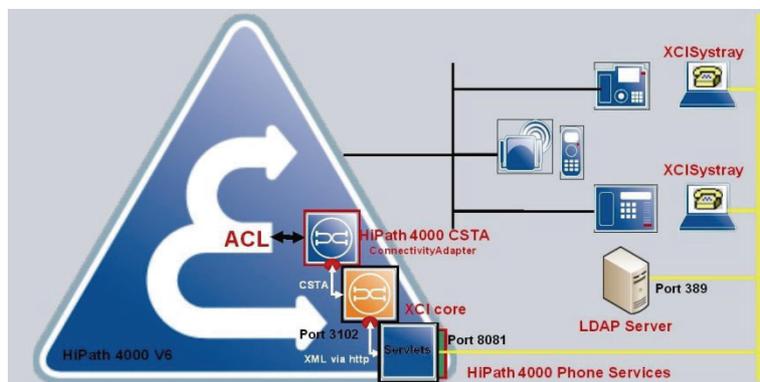


Figure 93 Single connected HiPath 4000 CSTA (HiPath 4000 V6)

Overview – Single connected HiPath 4000 CSTA in case of HiPath 4000 V4, V5 connection

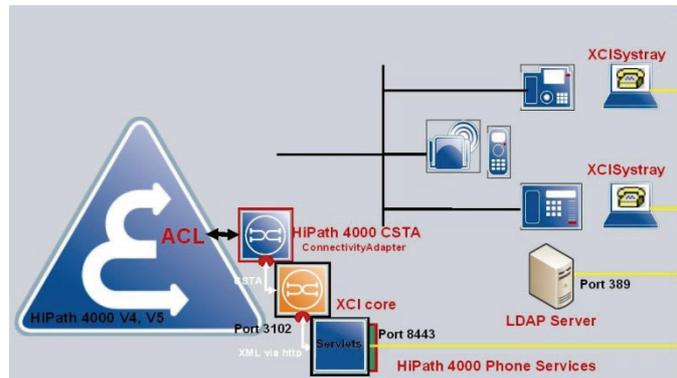


Figure 94 Single connected HiPath 4000 CSTA (HiPath 4000 V4, V5)

Overview – Multiple connected HiPath 4000 CSTA

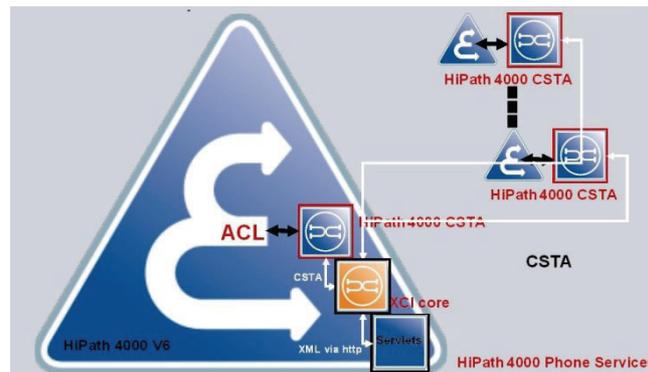


Figure 95 Multiple connected HiPath 4000 CSTA (HiPath 4000 V6)

### Administration URLs – in case of standalone / external installation

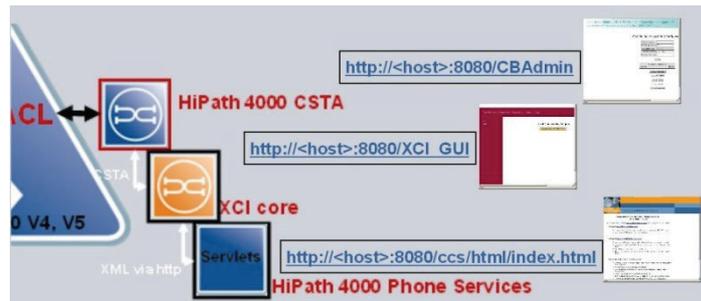


Figure 96 Administration URLs – in case of standalone / external installation

- **HiPath 4000 CSTA:** <http://<host>:8080/CBAdmin>
- **XCI core:** [http://<host>:8080/XCI\\_GUI](http://<host>:8080/XCI_GUI)
- **HiPath 4000 Phone Services:** <http://<host>:8080/ccs/html/index.html>

---

**NOTE:** Some HiPath 4000 Phone Service Administration Web pages are available via **localhost** only! Please note that the protocol and used ports are configurable in `<installDir>\tomcat.cfg`.

---

### Administration URLs – in case of HiPath 4000 V6 integrated variant



Figure 97 Administration URLs – in case of HiPath 4000 V6 integrated variant

- **HiPath 4000 CSTA:** From HiPath 4000 Assistant > ExpertMode/CSTA
- **XCI core:** From CBAAdmin with Phone Services UI link

- **HiPath 4000 Phone Services:** <https://<CLAN IP of CSTA VM>:8081/ccs/html/index.html>

---

**NOTE:** Some HiPath 4000 Phone Service Administration Web pages are available via **localhost** only! From R11.202.6 HF version of HiPath 4000 CSTA these sites are integrated into the XCI-Administration graphical user interface.

---



List of Connectivity Adapters

Name	IP Address	Port	Chars coll.		
XCI	127.0.0.1	1111	2		

---

**NOTE:** Please note that in case of HiPath 4000 V6, the HiPath 4000 CSTA and XCI administration pages are available via HiPath 4000 Assistant only.

---

### Phone Service URLs

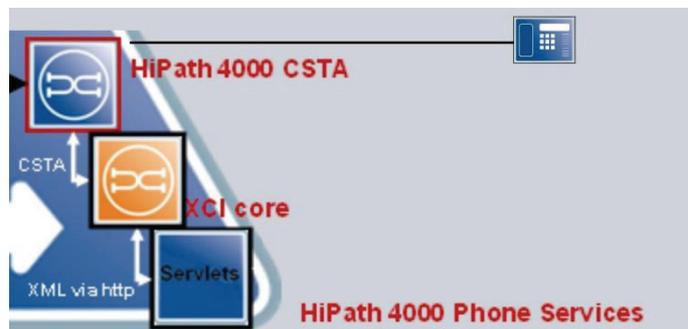


Figure 98 Phone Service URLs

- **AllAppsMenu:** <http<s>://<host>:<port>/ccs/menu>
- **EasySee:** <http<s>://<host>:<port>/ccs/pc?PHONE=%phone%>
- **EasyMail:** <http<s>://<host>:<port>/ccs/mailme?PHONE=%phone%>
- **EasyLookup:** <http<s>://<host>:<port>/ccs/ccs?PHONE=%phone%>
- **EasyShare:** <http<s>://<host>:<port>/ccs/WCServlet?PHONE=%phone%>

- **EasyUC:** `http<s>://<host>:<port>/ccs/UCMenu?PHONE=%phone%`

---

**NOTE:** Please note that in the case of the HiPath 4000 V6 integrated variant https can be used and the <host> is CLAN IP of the CSTA VM and the <port> is 8081;  
for standalone / external installations use http and the default port is 8080 (configurable in <installDir>\tomcat.cfg).

---

### Phone Service XML Service Tray Port - In case of standalone / external installation 8443

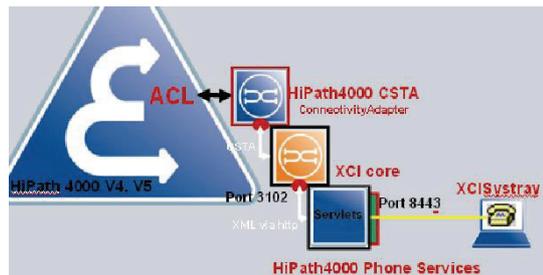


Figure 99 Phone Service XML Service Tray Port In case of standalone / external installation 8443

### Phone Service XML Service Tray Port - In case of HiPath 4000 V6 integration 8081

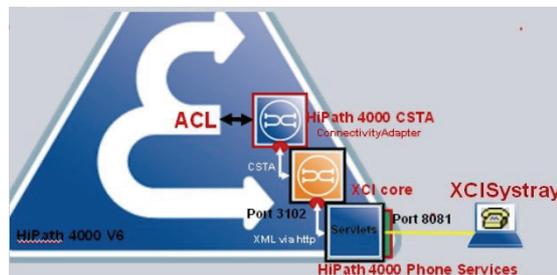


Figure 100 Phone Service XML Service Tray Port in case of HiPath 4000 V6 integration 8081

## 9.3 Requirements

### Hardware and Software Requirements

- HiPath 4000 Phone Services is installed automatically together with HiPath 4000 CSTA
- HiPath 4000 digital phones with display and cordless phones
- PC (with Windows OS) with the HiPath 4000 Phone Service (Tray – i.e. **XCITray**) application installed; XCITray can be downloaded from the HiPath 4000 Phone Service Administration Web page.

---

**NOTE:** XCITray is not required for either EasyLookup or EasyUC, however with XCITray 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 HiPath 4000 system via the same Connectivity Adapter of HiPath 4000 CSTA (e.g. Phone Services of the HiPath 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!

---

## 9.4 Configuration

### 9.4.1 Configuration Steps

- Complete the HiPath 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 a new **CA instance** and a new application link in **CBAdmin**. Set the licensing type to **no license**.
- Add an XMLPS service in **XCI\_GUI** (including **domain** information). Add devices, set user passwords and assign keys for HiPath 4000 Phone Services Application URLs.

- Set up the CCS and LDAP configurations (see the related sections in this document:
  - For SMR 13 and higher: Abschnitt 9.5, “LDAP Connection Configuration for EasyLookup (SMR 13 specific)”
  - SMR11/SMR12: Abschnitt 9.6, “LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)”

## 9.4.2 AMO Configuration HiPath 4000 V5, V6

### Redial pause timer

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

Keypad change if that is not default:

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

### For digital phones

```
ADD-
```

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

### For cordless phones/CMI key 9 only:

```
ADD-
```

```
ZIEL: TYP=NAME, SRCNO=<stno>, KYNO=09, DESTNON=C1eC1399909, DEV=<device>, [PROTECT=YES];
```

---

**NOTE:** In case of keymodule used, then the led-id starts from 21 - so by the setting in XCI and AMO it must take care to configure it accordingly.

---

---

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

---

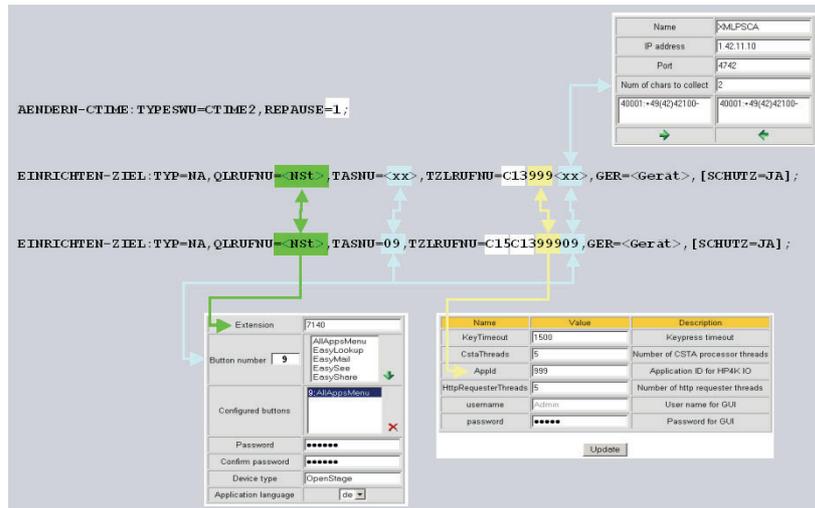


Figure 101 AMO Configuration

### 9.4.3 HiPath 4000 CSTA

- As described in the previous sections, a **CA instance** is up and running.
- The ACL link to HiPath 4000 has to be established.
- A CSTA link has been configured and is to listen on one connection port.
- The license type is set to **no license**.

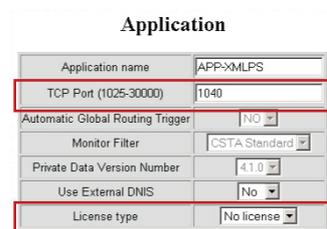


Figure 102 Application

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

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

## Phone Services – Introduction Configuration

The image shows a login form titled "XMLPS for OpenScape4000 CSTA". It contains two input fields: "Login:" and "Password:". Below these fields is a "Login" button, which is highlighted with a red rectangular box.

Figure 103 Login

The image shows a configuration page titled "CA4000\_OpenScape4000\_1 Configurati...". It features a table of configuration parameters:

PBX Link Number	10
PBX Sub-App Number	20
Manufacturer Name	HiPath
IP address of the PBX	10.254.4.5
Maximum log file size	10

Below the table is a "Modify" button. At the bottom, there is a section for "Configured applications" with a "CallCenter" entry and an "Add new application" button.

Figure 104 Phone Services UI

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

The image shows a navigation bar with "Connectivity Adapter", "Domain", "Device", "XML Application", "Configuration", and "Logout". Below the bar, there is a "List of domains" section. On the left, there are "Show" and "Add" buttons. A red arrow points from the "Add" button to the "Domain" tab in the navigation bar.

Figure 105 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.

The image shows the "Add new domain" configuration form. It includes a navigation bar with "Connectivity Adapter", "Domain", "Device", "XML Application", "Configuration", and "Logout". On the left, there are "Show" and "Add" buttons. The main form contains the following fields:

Name	<input type="text"/>
Country code	<input type="text"/>
National prefix	<input type="text"/>
International prefix	<input type="text"/>
Outside line access	<input type="text"/>
Area code (optional)	<input type="text"/>
Main number	<input type="text"/>
Virtual node code (optional)	<input type="text"/>

At the bottom right of the form is an "Add domain" button, highlighted with a red rectangular box.

Figure 106 Add new domain

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

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

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



Figure 107 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 108 List of Connectivity Adapters

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



Figure 109 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\*\*).

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

**Phone Services – Introduction**  
**Configuration**

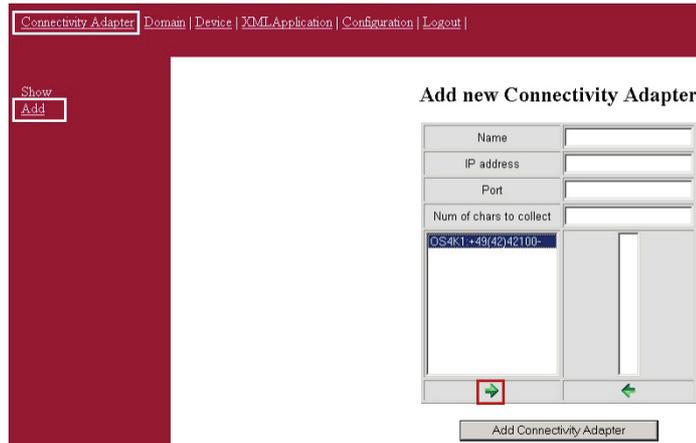


Figure 110 Add ConnectivityAdapter

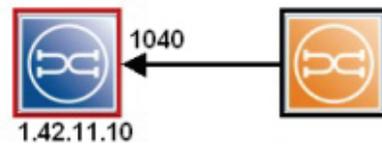


Figure 111 XMLPS - Add new domain

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

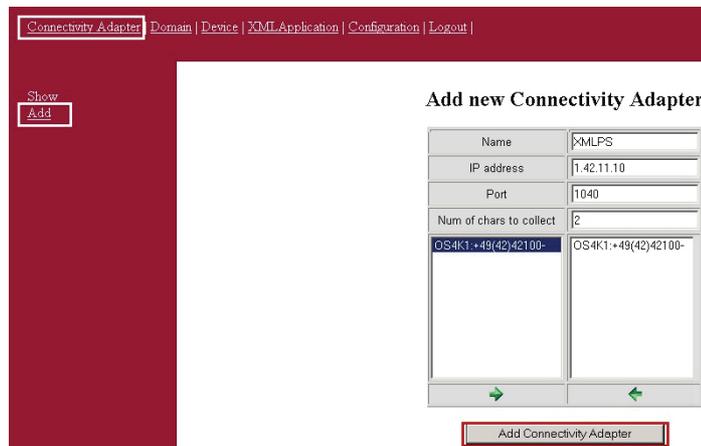


Figure 112 Add new Connectivity Adapter

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



Figure 113 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 **Service Tray**.

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

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

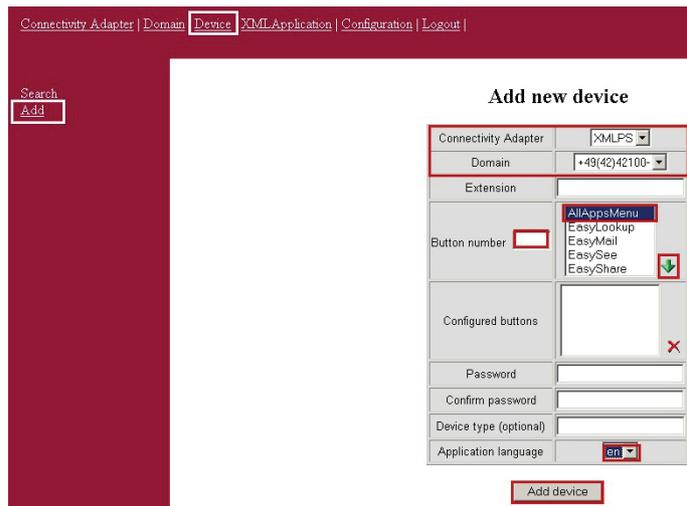


Figure 114 Add new device

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

---

**NOTE:** For R13.201.0 and onwards, 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.

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

Figure 115 Device added

**Do not change anything in this configuration!!**

Switch to the **Configuration** Web page.

Name	Description	URL
AllAppsMenu	Menu for Applications: EasyLookup, EasySee, EasyMail, and EasyShare	http://localhost:8080/ccs/menu
EasyLookup	Display additional information for connected person(s)	http://localhost:8080/ccs/ccs?PHONE=%
EasyMail	Opens blank email-form with filled-out email addresses for connected persons	http://localhost:8080/ccs/mailme?PHONE=phone%
EasySee	Display of Directory Information	http://localhost:8080/ccs/pc?PHONE=%f
EasyShare	starts a collaboration session with all participants of a phone conference	http://localhost:8080/ccs/netmeeting?PHONE=phone%

Figure 116 List of XML applications

It is recommended to change the **Admin user password**.

Name	Value	Description
KeyTimeout	1500	Keypress timeout
CstaThreads	5	Number of CSTA processor threads
ApplId	999	Application ID for HP4K IO
HttpRequesterThreads	5	Number of http requester threads
username	Admin	User name for GUI
password	****	Password for GUI
UCProtocolName	https	UC connection protocol
UCProtocolPort	4709	UC connection port
UCServerName	jmeaos global-voip.net	UC server name
UCDefaultURL	http://localhost:4709/	UC default URL
RepeatedSendDataDelay	0	Remove repeated SendData requests within the given time (ms, 0: turned off)
PingerThreads	3	Number of tray pinger threads
PingTime	60	Time between two ping requests (to tray)
UCAwaysLoggedOn	1	Keep users with UC username/password always logged on to UC
MaxScheduledThreadCount	30	Max number of scheduled task executor threads
UCSessionTime	600	Connection to UC for a user is kept alive that long (0: forever)
FvServerList	10000-99999:openscapew	Openscape Web Collaboration Server list. Format: {history} {last} {server1}, {server2}, ...
FvMailSubject	OpenScape Web Collabor	Subject of the invitation emails.
FvMailBody	Ladies and Gentlemen, Y	Body of the invitation emails. %SESSION_ID% is replaced with the actual session id. * is the new line marker.

Update

Figure 117 Configuration

The **ApplId** 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 HiPath 4000.

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

---

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

---

Log out to exit the XMLPS configuration.

## 9.5 LDAP Connection Configuration for EasyLookup (SMR 13 specific)

### 9.5.1 CCS Configuration

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

## Phone Services – Introduction

### LDAP Connection Configuration for EasyLookup (SMR 13 specific)

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

EasySee URL:

EasySee Card URL:

LDAP Config File:    
 (see the Advanced configuration page in CBAAdmin for template configurations (Component type: LDAPConfigFile, component: template.cfg))

Default Country Code:

Default Area Code:

Default Main Number:

Outside Line Access:

National Prefix:

International Prefix:

Menu order:

SAT activated:

Figure 118 CCS Configuration - CCS LDAP Configuration

EasySee URL:

EasySee Card URL:

LDAP Config File:    
 (see the Advanced configuration page in CBAAdmin for template configurations (Component type: LDAPConfigFile, component: template.cfg))

Default Country Code:

Default Area Code:

Default Main Number:

Outside Line Access:

National Prefix:

International Prefix:

Menu order:

SAT activated:

Figure 119 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 HiPath 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 by SAT.

## 9.5.2 CCS LDAP Configuration

LDAP specific settings can be configured on the **CCS LDAP Configuration** page. From R13.201.0 on, multiple LDAP server can be used with Phone Services, however it requires a more detailed setup. First let's go over a scenario when only one LDAP server is used.

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

CCS LDAP List  
User Groups

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

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

Unique config name:

In case there was a new LDAP configuration added through CBAAdmin's Advanced Configuration synchronization might be necessary. This process takes a few minutes.

Figure 120 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 pink. 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:** The on the **CCS Configuration** page chosen LDAP configuration cannot be deleted.

---

- **Editing and viewing configurations**

## Phone Services – Introduction

### LDAP Connection Configuration for EasyLookup (SMR 13 specific)

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

- **General settings**

On the upper section the general settings can be seen.

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

Setting for ActiveDirectory.cfg

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

Figure 121 General LDAP settings

- **LDAP Configuration Enabled**

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

- **LDAP Server Address**

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

- **LDAP User**

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

- **LDAP Password**

Password for the user mentioned above.

- **Search base**

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

- **Telephone number match**

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

0 - if Phone Services has to do this manually.

- **MaxLengthCIWildcardNumber**

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

- **Search Method in queryName field**

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

- **Number format in LDAP**

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

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

---

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

---

### LDAP Attributes

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

Figure 122 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 restarted.

---

## Phone Services – Introduction

### LDAP Connection Configuration for EasyLookup (SMR 13 specific)

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

CCS LDAP List  
User Groups

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

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

Unique config name:

In case there was a new LDAP configuration added through CBAAdmin's Advanced Configuration synchronization might be necessary. This process takes a few minutes.

Figure 123 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).

### 9.5.3 Phone Services with Multiple LDAP Servers

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

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

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

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

CCS LDAP List  
User Groups

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

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

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

Short name:  Description:

Figure 124 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.

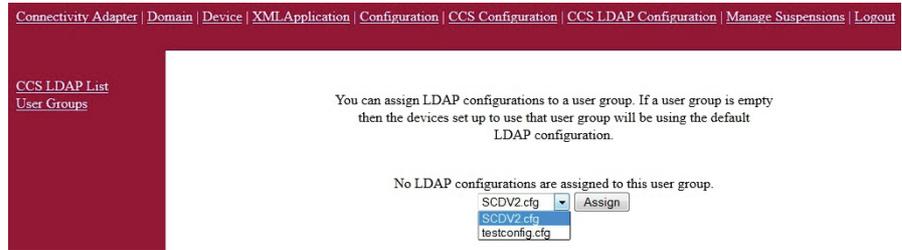


Figure 125 User group - assign LDAP Configuration

As mentioned before the first option in an LDAP configuration is an enabled/disabled flag. A 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.

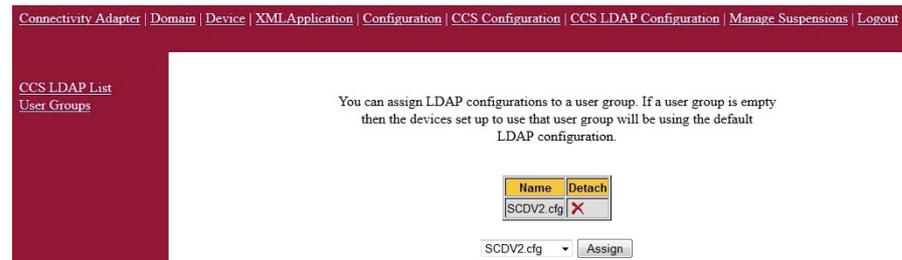


Figure 126 User group - detaching a configuration

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**).

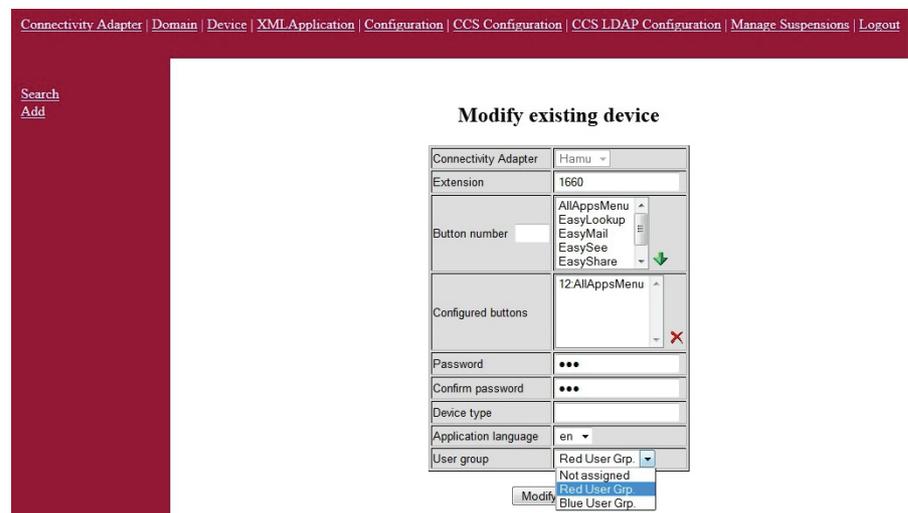


Figure 127 Device modify - assigning a user group

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.

### 9.5.4 Configuration Example: Web Page Design

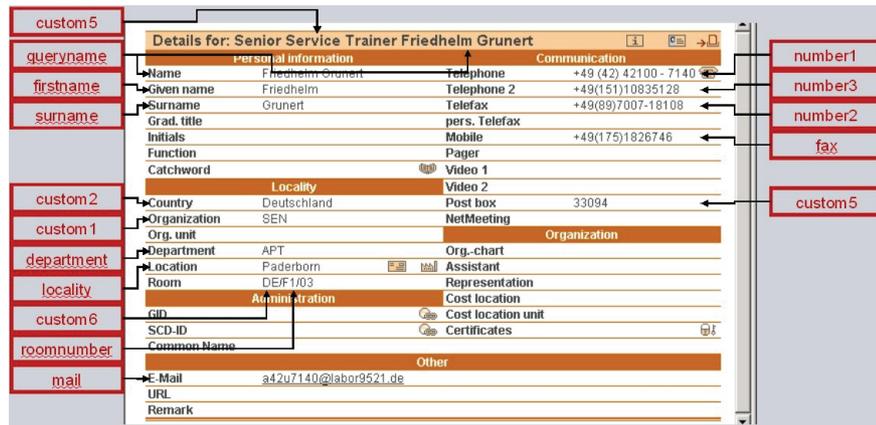


Figure 128 Configuration parameter EasySee Web page

The EasySee Web page is based on the html file: `template.html`.

- `<instDir>\CSTA\tomcat\webapps\ccs\html\template.html` - in the case of standalone / external installation
- `... \srv\www\tomcat5\webapps\ccs\html\template.html` - in the case of HiPath 4000 V6 integration

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

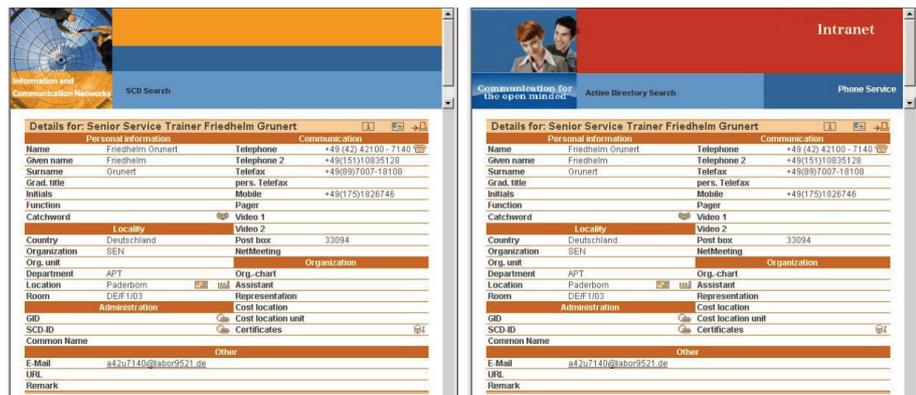


Figure 129 Web page design

## 9.6 LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)

### Remember: Have you done this?

Have you made the following changes in

`<instDir>\CSTA\config\ccs\config.xml`:

- Change the XML tag value `<BasePcAppUri>` and modify the URL to address the HiPath 4000 CSTA server.
- Change the XML tag value `<LDAPConfigFile>` to the file name you have already configured for LDAP access.
- Change the XML tag value `<ScdUrl>` to:  
`http://<PhoneServiceServer-IP>:<port>/ccs/d4w?sclid=`
- Change the XML tags values, which have to match the HiPath 4000 V4,5,6 office code and outside line access code configuration.

---

**NOTE:** While it is possible to change this file manually, it is also possible to set these parameters via the user interface, whichever option is preferred.

---

Have you made the following changes in

`<instDir>\CSTA\config\ccs\config.xml`:

- Change the XML tag value `<LDAPConfigFile>` to the file name you have already configured for LDAP access.

Open the file in `<instDir>\CSTA\config\ccs\`, which is defined in `<LDAPConfigFile>` and change the parameters to connect the LDAP server.

---

**NOTE:** The example on the next pages of connecting an Active Directory Server can also be used for any other LDAP server connection if the connection parameters are set correctly!

---

Make the following changes in `<instDir>\CSTA\config\ccs\config.xml`:

- Change the XML tag value `<LDAPConfigFile>` to the file name you have already configured for LDAP access.

## Phone Services – Introduction

### LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)

Open the file in `<instDir>\CSTA\config\ccs\`, which is defined in the XML tag `<LDAPConfigFile>` and change the parameters to connect the LDAP server.

---

**NOTE:** In an **HiPath 4000 CSTA Integrated Environment** (in HiPath 4000 V6), the tomcat path is: `/srv/www/tomcat5/`. For standalone / external installations, tomcat is integrated in the installation and can be found under: `<instDir>\CSTA\tomcat`.

---

Configuration example: `ActiveDirectory.cfg`

- The XML tag value for `<LDAPConfigFile>` is set to `ActiveDirectory.cfg` in the `<instDir>\CSTA\config\ccs\config.xml` file. This file exists by default and has a predefined setting for Active Directory LDAP access.
- Open the `ActiveDirectory.cfg` file in the `<instDir>\CSTA\config\ccs` directory, which is defined in the XML tag `<LDAPConfigFile>` and change the parameters to connect an Active Directory server.

#### Configuration Example

```
#-----  
# Configuration of Microsoft Active Directory LDAP Server  
#-----  
TemplateName = Microsoft Active Directory LDAP Server  
#  
# Version of the Configuration file  
#  
DBEnv.Version = 3.1
```

---

**NOTE:** You must leave the values as are!

---

```
# Server address of the database Server.  
# Multiple server addresses can be specified, separated by  
spaces.  
# The address has the following format:  
# <IP address (or DNS name)>:<port number>  
# For example: 139.23.81.108:389  
#
```

## LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)

```
DBEnv.ServerAddress = 1.95.21.20:389
```

---

**NOTE:** Enter the IP address and port number for LDAP access of at least one Active Directory server.

---

```
# Port number to be used for SSL connections (Secure Sockets Layer).
```

```
# If no port number is specified and DBEnv.DatabaseType = WEBDAV,
```

```
# the default port number 443 is used.
```

```
#
```

```
DBEnv.SSLPort =
```

---

**NOTE:** As an optional connection option, enter the port number for LDAP SSL access. In the case of multiple server connections, this port must be identical on all servers.

---

```
# Root node (node from which addresses should be accessed)
```

```
# If no root is specified, the root of the database is taken
```

```
#
```

```
DBEnv.Root = DC=labor9521,DC=de
```

```
#
```

```
# Search base (relative to DBEnv.Root)
```

```
# If no SearchBase is specified, DBEnv.Root is taken
```

```
#
```

```
DBEnv.SearchBase = OU=Raum9
```

---

**NOTE:** Define the LDAP root and the LDAP search base. Optionally, you can enter the complete path in one string only.

---

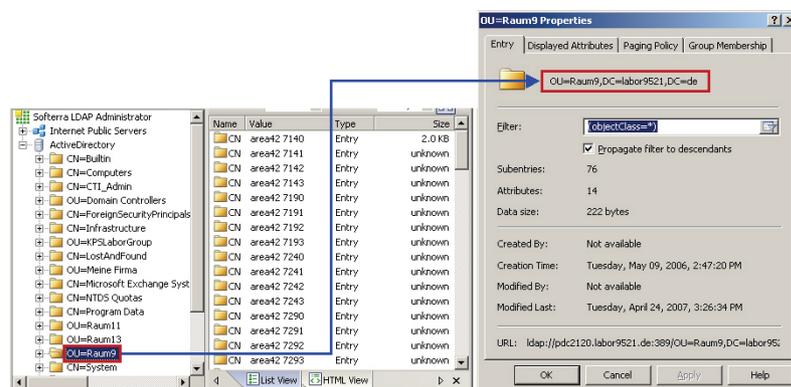


Figure 130

LDAP configuration parameters

## Phone Services – Introduction

### LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)

```
# Database type (Access Protocol)
# Valid database types: LDAP, WEBDAV (for future use)
# Default value: LDAP
#
DBEnv.DatabaseType =
```

---

**NOTE:** Leave the value as is, only LDAP is supported.

---

```
# Database display name (used to select a database in query
dialog)
# The display name has the following format:
#
# <lang1>:<name in lang1>; <lang2>:<name in lang2>; ...
#
# The tag <langx> consists of two letters (case insensitive) and
indicates
# the language of the display name according to the ISO 639
standard
# (e.g.: EN - English, DE - German, FR - French ...).
# This format allows one display name to be specified in
different languages.
#
DBEnv.DisplayName =
```

---

**NOTE:** This parameter is not supported by HiPath 4000 Phone Services.

---

```
# Default access rights
# Possible values:
#
# read: The database can be read
# write: The database can be written (implies read access)
#
# NOTE: These access rights are on a database level, permissions
are granted
# to all users. TelasWeb can grant permissions to individual
users and thus
# provide a finer degree of control. But the TelasWeb
permissions can only
# more restrict the default access rights specified in this
file.
# E.g. you cannot grant "write" access to an individual user if
the default
```

## LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)

```
# access rights are "read".
# Default value: read
#
DBEnv.DefaultAccess =
```

---

**NOTE:** Leave the value as is, only read is supported.

---

```
# Specifies the authentication mechanism to use.
# This can be one of the following strings:
#
# none: No authentication (anonymous)
# No user name (property DBEnv.AuthUser) and password (property
# DBEnv.AuthPW) are required to retrieve information.
# simple: Weak authentication (unencrypted user name and
password)
# User name (property DBEnv.AuthUser) and password (property
# DBEnv.AuthPW) are required to retrieve information.
# The user name must be provided in clear text, the password
# in base64 encoded form.
# user-access: Per user authentication
# User name, password and additional access parameters are
# required to retrieve information. These parameters must be
# stored in the system database. The properties DBEnv.AuthUser
# and DBEnv.AuthPW are not considered. In contrast to
# simple authentication, individual settings for each user
# must be provided.
#
# Default value: none
#
DBEnv.AuthMechanism = simple
```

---

**NOTE:** The authentication mechanisms none (anonymous) and simple (basic user authentication) are supported.

---

```
# Specifies the name of the user/program performing the
authentication.
# Depends on the value of AuthMechanism property.
#
# Default values: empty string
#
```

## Phone Services – Introduction

### LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)

```
DBEnv.AuthUser = a42u7440@labor9521.de
```

```
DBEnv.AuthPW = admin
```

---

**NOTE:** If `DBEnv.AuthMechanism = simple` enter a valid Active Directory user name and his password for LDAP access authentication.

---

```
# Sharing mode of the database
```

```
#
```

```
# public: The database contains information to be shared  
# between users.
```

```
# personal: The database contains information to be secured  
# from other users (i.e. multiple users cannot access  
# the same data).
```

```
#
```

```
# Default value: public
```

```
#
```

```
DBEnv.ShareMode =
```

---

**NOTE:** Leave the value as is, only `public` is supported.

---

```
# Specifies whether the server supports the search matching rule  
# "Telephone-Number" (1 = supported, 0 = not supported).
```

```
#
```

```
# Default value: 1
```

```
#
```

```
DBEnv.TelePhoneNumberMatch = 0
```

---

**NOTE:** The value `DBEnv.TelePhoneNumberMatch` must be set to 0.

---

```
# Specifies whether the server supports wildcard search  
# (1 = supported, 0 = not supported).
```

```
#
```

```
# Default value: 1
```

```
#
```

```
DBEnv.WildcardSearch = 1
```

---

**NOTE:** The value `DBEnv.WildcardSearch` must be set to 1.

---

```
# Defines the max. length of a wildcard phone number string used
```

## LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)

```
# in a Caller Identification operation.
#
# Default value: 3
#
DBEnv.MaxLengthCIWildcardNumber = 4
```

---

**NOTE:** The value for `DBEnv.MaxLengthCIWildcardNumber` must be the same length as the extension number.

---

```
# Timelimit in seconds for searching (default is 0 - unlimited)
#
DBEnv.TimeLimit =
```

---

**NOTE:** Set the timer to the required value.

---

```
# Specifies the database used to dereference the alias attribute
# "AttrMap.alias". The alias attribute contains the DN of the
object
# it points to. It must be dereferenced by the client process
(the
# TelasWeb Address Service never dereferences this attribute!)
# NOTE: Do not confuse this kind of aliases with LDAP Aliases
#       and Referrals!
#
# The database must be specified by its ID (e.g.: Exc2K)
# Default value: empty string
#
DBEnv.AliasRefDatabase =
```

---

**NOTE:** The variable is for SimplyPhone for Outlook/Notes – CRI only! Leave it unset!

---

```
# Defines whether this database should be exposed to the client.
# (1 = exposed, 0 = not exposed).
# Default value: 1
#
```

## Phone Services – Introduction

### LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)

```
DBEnv.ExportDatabase =
```

---

**NOTE:** The variable is for Simply Phone for Outlook/Notes – CRI only! Leave it unset!

---

```
# Determines whether the personal database (the personal storage
# of a user) can be deleted. (1 = delete, 0 = not delete).
#
# when this entry is set to 1 and a user in the CAP User
# Management
# is deleted, then the associated personal database (personal
# storage of the user) is deleted too.
#
# This setting is only evaluated if DBEnv.ShareMode is set to
# "personal".
#
# Default value: 1
#
DBEnv.DeletePersonalStorage =
```

---

**NOTE:** Leave the value as is, this assigned feature is not supported!

---

```
# Mapping of attribute names to names used in directory scheme
# Syntax:
#   AttrMap.<int attr name> = <db attr name>
#   AttrMap.<int attr name>.type = <phone | dbstr>
#   AttrMap.<int attr name>.searchable = <yes | no>
#
# The attribute type "phone" indicates a telephone number,
# "dbstr" an ordinary attribute
# The default value of type is "dbstr", of searchable is "yes".
```

---

**NOTE:** Based on the default configuration file, the mapping has been correctly preconfigured for Active Directory Access. If a different LDAP server is connected, the internal **Attribute Name** has to match the LDAP server field names to display the field contents.

---

```
AttrMap.surname = sn
AttrMap.firstname = givenName
AttrMap.displayname = displayName
```

```
AttrMap.queryname = cn
AttrMap.title =
AttrMap.department = department
AttrMap.locality = l
AttrMap.mail = mail
AttrMap.mail2 =
AttrMap.fax = facsimileTelephoneNumber
AttrMap.url =
AttrMap.comment =
AttrMap.notice =
AttrMap.roomnumber = physicalDeliveryOfficeName
AttrMap.costlocation =
AttrMap.number = telephonenumber
AttrMap.number1 = telephonenumber
AttrMap.number1.searchable = yes
AttrMap.number2 = mobile
AttrMap.number2.searchable = yes
AttrMap.number3 = otherTelephone
AttrMap.number3.searchable = yes
AttrMap.number4 =
AttrMap.number4.searchable = null
AttrMap.alias =
AttrMap.custom1 = company
AttrMap.custom2 = co
AttrMap.custom3 =
AttrMap.custom4 = postOfficeBox
AttrMap.custom5 = title
AttrMap.custom6 = c
AttrMap.custom7 =
AttrMap.custom8 =
AttrMap.custom9 =
```

---

**NOTE:** These parameters match the Active Directory LDAP field names! No other values are currently supported!

---

## Phone Services – Introduction

### LDAP Connection Configuration for EasyLookup (SMR 11 and SMR 12)

Figure 131 Configuration parameter EasySee Web page

### Configuration Example: Web Page Design

The EasySee Web page is based on the html file: template.html

- <instDir>\CSTA\tomcat\webapps\ccs\html\template.html – in case of standalone / external installation
- ... \srv\www\tomcat5\webapps\ccs\html\template.html – in case of HiPath 4000 V6 integration

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

Figure 132 Web page design

## 9.7 Suspension

---

**NOTE:** This feature is released for SMR 13 (HiPath 4000 V6 R2) and higher.

---



---

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

---

### Temporary login lock

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

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

#### HiPath 4000 CSTA CBAAdmin Configuration Management

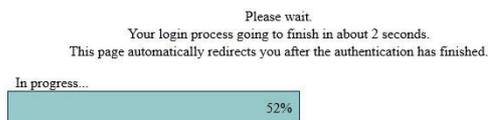


Figure 133 CBAAdmin - delayed login progress

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

### Suspension List

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

#### Manage Suspensions > Show List

The screenshot shows the 'Manage Suspensions > Show List' interface. It includes a navigation menu with links like 'Connectivity Adapter', 'Domain', 'Device', 'XMLApplication', 'Configuration', 'CCS Configuration', 'CCS LDAP Configuration', 'Manage Suspensions', and 'Logout'. The main content area is titled 'Suspension List' and contains a table with the following data:

Suspended ID	Type	Date of last fail	Number of fails
172.27.17.241	IP_TYPE	Tue Nov 13 11:08:15 CET 2012	1

Figure 134 Manage Suspension - suspended addresses

## Phone Services – Introduction

HiPath 4000 Phone Services HiPath 4000 Phone Services (prev. XCI Tray)

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

### Settings

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

### Manage Suspensions > Settings



Figure 135 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 HiPath 4000 CSTA is installed.

## 9.8 HiPath 4000 Phone Services HiPath 4000 Phone Services (prev. XCI Tray)

---

**NOTE:** You can download **HiPath 4000 Phone Services (prev. XCI Tray)** from the HiPath 4000 Phone Service Web page.

Stand alone/external variant: `http://<IP of PS server>:8080/ccs/html/index.html`

HiPath 4000 V6 integrated variant: `https://<CLAN IP fo CSTA VM>:8081/ccs/html/index.html`

---

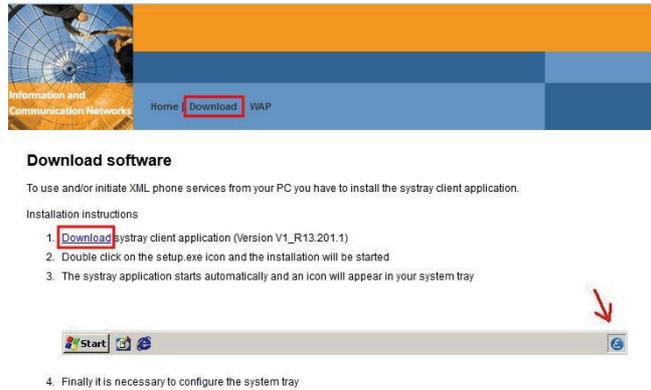


Figure 136 Download HiPath 4000 Phone Services  
Select **Download** to download the program.



Figure 137 Run or Save  
Press **Run** to execute and install or **Save** to save the program.



Figure 138 HiPath 4000 Phone Services (prev. XCI Tray) installation

## Phone Services – Introduction

HiPath 4000 Phone Services HiPath 4000 Phone Services (prev. XCI Tray)

After starting setup.exe, no further user interaction is needed to install the software – silent installation is used to support systems with automatic software distribution.

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

**Start > Programs > Siemens > HiPath4000PhoneServices > HiPath4000PhoneServices**

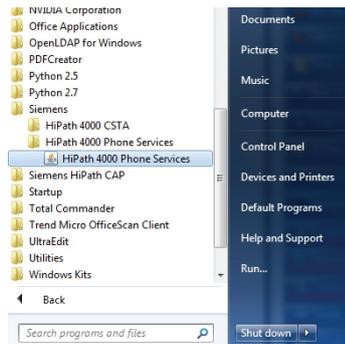


Figure 139 HiPath4000 Phone Services in Start menu

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

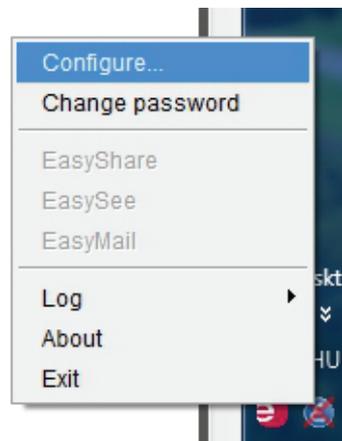


Figure 140 HiPath 4000 Phone Services - Configuration menu

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

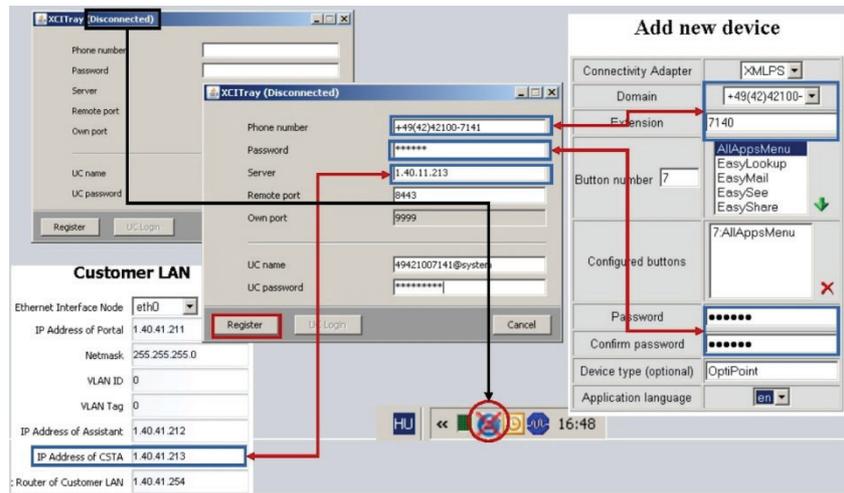


Figure 141 HiPath 4000 Phone Services (prev. XCI Tray) configuration

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

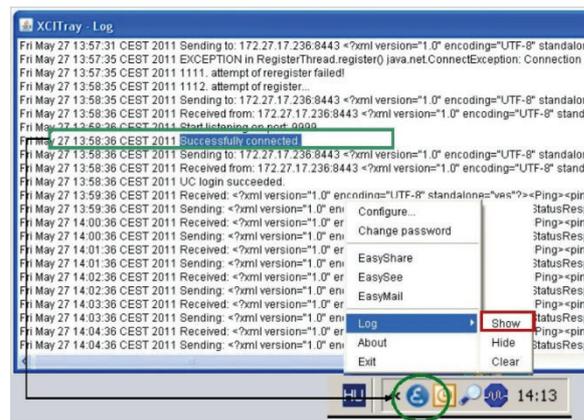


Figure 142 HiPath 4000 Phone Services logs

This log message provides helpful information about the connection.

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

## Phone Services – Introduction

### HiPath 4000 Phone Services HiPath 4000 Phone Services (prev. XCI Tray)

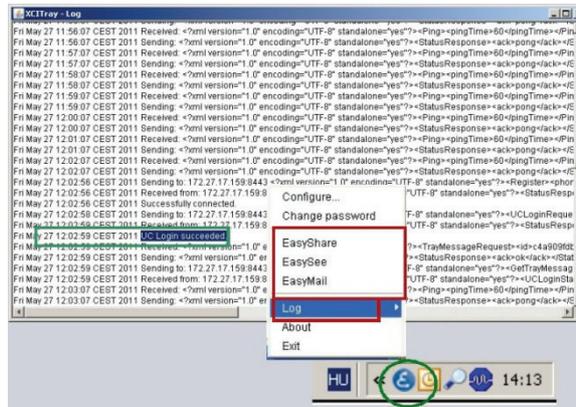


Figure 143 HiPath 4000 Phone Services Menu - functions

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

---

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

---

# List of Figures

Figure 1	Scenarios - Internal integration - One CSTA link . . . . .	7
Figure 2	Scenarios - Internal integration - Four CSTA links . . . . .	8
Figure 3	Scenarios - Internal integration - 1 to 4 CSTA links per process . . . . .	8
Figure 4	Scenarios - External installation - One CSTA link . . . . .	9
Figure 5	Scenarios - External installation - Four CSTA links . . . . .	9
Figure 6	Scenarios - External installation - 1 to 4 CSTA links per process . . . . .	10
Figure 7	Configuration batch description . . . . .	12
Figure 8	HiPath 4000 CSTA CBAAdmin configuration management . . . . .	16
Figure 9	License Highlights . . . . .	16
Figure 10	Linux installation . . . . .	20
Figure 11	Subdirectories . . . . .	20
Figure 12	Linux upgrade installation . . . . .	21
Figure 13	Program start jss . . . . .	21
Figure 14	Program start cbdriver4000 . . . . .	21
Figure 15	Run setup.exe . . . . .	22
Figure 16	InstallShield Wizard - Step 1 . . . . .	22
Figure 17	InstallShield Wizard - Step 2 . . . . .	23
Figure 18	InstallShield Wizard - Step 3 . . . . .	23
Figure 19	InstallShield Wizard - Step 4 . . . . .	24
Figure 20	InstallShield Wizard - Step 5 . . . . .	24
Figure 21	InstallShield Wizard - Step 6 . . . . .	25
Figure 22	InstallShield Wizard - Step 7 . . . . .	25
Figure 23	HiPath 4000 CSTA . . . . .	26
Figure 24	Start menu . . . . .	26
Figure 25	Service . . . . .	27
Figure 26	Program Start manually . . . . .	27
Figure 27	Windows Task Manager . . . . .	28
Figure 28	Configuration steps - stand alone/external variant . . . . .	31
Figure 29	Logon . . . . .	32
Figure 30	Connectivity Adapter List - Add New ConnectivityAdapter . . . . .	32
Figure 31	Connectivity Adapter List - Add CA . . . . .	33
Figure 32	Settings - Select Connectivity Adapter . . . . .	33
Figure 33	Configuration - Modify . . . . .	34
Figure 34	Configuration - Existing configuration . . . . .	34
Figure 35	Configuration . . . . .	35
Figure 36	cbdriver4000 process . . . . .	35
Figure 37	Configuration - Add new application . . . . .	35
Figure 38	Configuration - Add new application . . . . .	36
Figure 39	Configuration - Configured applications . . . . .	36
Figure 40	Status (CBAAdmin Configuration Management): ACL-C active, HiPath 4000 CSTA inactive . . . . .	37
Figure 41	Status: ACL-C active, HiPath 4000 CSTA inactive . . . . .	37
Figure 42	Status (CBAAdmin Configuration Management): ACL-C active, HiPath 4000 CSTA active . . . . .	38
Figure 43	Status: ACL-C active, HiPath 4000 CSTA active . . . . .	38
Figure 44	Log - Show/Clear . . . . .	39
Figure 45	Log - Data download . . . . .	40
Figure 46	Component log properties . . . . .	40
Figure 47	Log - Show/Clear . . . . .	41

## List of Figures

Figure 48	Log - Enable/Disable . . . . .	41
Figure 49	Log - Data download . . . . .	42
Figure 50	Log - Start trace . . . . .	42
Figure 51	Statistics . . . . .	43
Figure 52	Version . . . . .	45
Figure 53	Phone Service UI . . . . .	46
Figure 54	Change default user and password . . . . .	46
Figure 55	HTTPS Connections . . . . .	47
Figure 56	Advanced Configuration - Component selection . . . . .	49
Figure 57	Advanced Configuration - Export/Import . . . . .	50
Figure 58	Logout . . . . .	51
Figure 59	java process . . . . .	54
Figure 60	bash process . . . . .	54
Figure 61	cbdriver4000 process . . . . .	55
Figure 62	Internal WEB Service Communication . . . . .	55
Figure 63	Internal ACL Communication . . . . .	55
Figure 64	Connect to HiPath 4000 Platform Administration (Portal) . . . . .	56
Figure 65	System . . . . .	56
Figure 66	System - LAN Wizard - Step 1 . . . . .	56
Figure 67	System - LAN Wizard - Step 2 . . . . .	57
Figure 68	System - LAN Wizard - Step 3 . . . . .	57
Figure 69	System - LAN Wizard - Step 4 . . . . .	58
Figure 70	Wizard completed . . . . .	58
Figure 71	Trusted IP addresses . . . . .	59
Figure 72	Connect to HiPath 4000 CSTA . . . . .	59
Figure 73	Connectivity Adapter List - Select Connectivity Adapter . . . . .	60
Figure 74	Configuration - CA4000_Default Configuration . . . . .	60
Figure 75	Connectivity Adapter List - Add New Connectivity Adapter . . . . .	61
Figure 76	Add CA . . . . .	61
Figure 77	Connectivity Adapter List - Select Connectivity Adapter . . . . .	62
Figure 78	Configuration - Modify . . . . .	62
Figure 79	Configuration - Add new application . . . . .	63
Figure 80	Configuration - Add application . . . . .	63
Figure 81	Configuration - XMLPS . . . . .	64
Figure 82	Status - PBX Link . . . . .	64
Figure 83	Connection to Backup & Restore, Software Activation/Transfer . . . . .	65
Figure 84	Backup & Restore - BEER_CSTA (configuration) . . . . .	65
Figure 85	Maintenance - System Backup - Backup . . . . .	66
Figure 86	Advanced Configuration - ca4000 component . . . . .	67
Figure 87	Advanced Configuration - ca4000 direct link . . . . .	67
Figure 88	EasyLookup - Call the menu by pressing the application button on the device . . . . .	76
Figure 89	EasySee . . . . .	77
Figure 90	EasyMail . . . . .	78
Figure 91	WebCollaboration integration . . . . .	79
Figure 92	EasyUC . . . . .	80
Figure 93	Single connected HiPath 4000 CSTA (HiPath 4000 V6) . . . . .	80
Figure 94	Single connected HiPath 4000 CSTA (HiPath 4000 V4, V5) . . . . .	81
Figure 95	Multiple connected HiPath 4000 CSTA (HiPath 4000 V6) . . . . .	81
Figure 96	Administration URLs – in case of standalone / external installation . . . . .	82
Figure 97	Administration URLs – in case of HiPath 4000 V6 integrated variant . . . . .	82
Figure 98	Phone Service URLs . . . . .	83
Figure 99	Phone Service XML Service Tray Port In case of standalone / external installation 8443 . . . . .	84

Figure 100	Phone Service XML Service Tray Port in case of HiPath 4000 V6 integration 8081	84
Figure 101	AMO Configuration	87
Figure 102	Application	87
Figure 103	Login	88
Figure 104	Phone Services UI	88
Figure 105	Domain - Add	88
Figure 106	Add new domain	88
Figure 107	List of domains	89
Figure 108	List of Connectivity Adapters	89
Figure 109	XMLPS	89
Figure 110	Add ConnectivityAdapter	90
Figure 111	XMLPS - Add new domain	90
Figure 112	Add new Connectivity Adapter	90
Figure 113	Device	91
Figure 114	Add new device	91
Figure 115	Device added	92
Figure 116	List of XML applications	92
Figure 117	Configuration	93
Figure 118	CCS Configuration - CCS LDAP Configuration	94
Figure 119	CCS Configuration	94
Figure 120	List of LDAP configurations	95
Figure 121	General LDAP settings	96
Figure 122	LDAP attribute specification	97
Figure 123	CCS LDAP Configuration	98
Figure 124	User groups	98
Figure 125	User group - assign LDAP Configuration	99
Figure 126	User group - detaching a configuration	99
Figure 127	Device modify - assigning a user group	99
Figure 128	Configuration parameter EasySee Web page	100
Figure 129	Web page design	100
Figure 130	LDAP configuration parameters	103
Figure 131	Configuration parameter EasySee Web page	110
Figure 132	Web page design	110
Figure 133	CBAdmin - delayed login progress	111
Figure 134	Manage Suspension - suspended addresses	111
Figure 135	Manage Suspension - settings	112
Figure 136	Download HiPath 4000 Phone Services	113
Figure 137	Run or Save	113
Figure 138	HiPath 4000 Phone Services (prev. XCI Tray) installation	113
Figure 139	HiPath4000 Phone Services in Start menu	114
Figure 140	HiPath 4000 Phone Services - Configuration menu	114
Figure 141	HiPath 4000 Phone Services (prev. XCI Tray) configuration	115
Figure 142	HiPath 4000 Phone Services logs	115
Figure 143	HiPath 4000 Phone Services Menu - functions	116

## List of Figures

## List of Tables

Table 1	Statistics - Link Status” section . . . . .	43
Table 2	Statistics - “PBX Communication” section . . . . .	44
Table 3	Statistics - “Application” section . . . . .	44

# Index

## A

- Additional Supported Services 64
- Application Environment 53

## C

- CBAAdmin - CA Instance Configuration 59
- CBAAdmin – CA Instanz Konfiguration 66
- CBAAdmin Configuration Management 31
  - Configuration 31
  - Logging 38
  - Logout 51
  - Phone Service UI 45
  - Statistics 42
  - Status 37
  - Version 45
- Configuration Batch Description 12
- Configuration Example 102
  - Web Page Design 100, 110
- Configuration Requirements 13
- CSTA Switch Integrated – Introduction 53

## E

- EasyLookup 75
- EasyMail 77
- EasySee 76
- EasyShare 78
- EasyUC 79
- External Integration 9

## H

- Hardware Requirements 11
- HiPath 4000 CSTA 5
- HiPath 4000 Phone Services
  - Download 113
- HiPath 4000 Phone Services XCI Tray 112
- HiPath 4000 V6 Maximal Values 7

## I

- Installation and Program Start
  - Linux 19
  - Windows 22
- Internal Integration 7
- Introduction 5

## L

- Licensing 15
- Logging 38
- Logout 51

## P

- Phone Service UI 45
- Phone Services
  - Configuration
    - AMO Configuration HiPath 4000 V4, V5, V6 86
    - Configuration Steps 85
    - HiPath 4000 CSTA 87
  - EasyMail 77
  - EasySee 76
  - EasyShare 78
  - EasyUC 79
  - LDAP Connection
    - Configuration for EasyLookup 93, 101
  - Overview 75
  - Requirements 85
  - Structure 80
- Phone Services – Introduction 75
- Port List 29
- Portal – IP Address Configuration 55
- Program Start
  - with Linux 21
  - with Windows 27

## R

- Requirements 11

## S

- Scenarios 7
- Software Installation 19
  - with Linux 19
  - with Windows 22
- software packages 13
- Software Requirements 11
  - Operation System 11
  - PBX support 12
- Statistics 42
- Status – Connection Check 37

## V

- Version 45

## X

- XCI Tray
  - Configuration 115
  - Install 113
  - Logs 115