A MITEL
PRODUCT
GUIDE

Mitel OpenScape Concierge

OpenScape Concierge V4R2, Configuration

Administrator Documentation

03/2025

P31003S2242M1001876A9

Mitel

Notices

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

Trademarks

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

Contents

1 About this manual

IMPORTANT:
This manual is subject to change. Before using it, make sure you have the current version!

The manual provides a guideline for the configuration / design required after the installation of an OSC Server to run the OpenScape Concierge Application.

The first chapters describe architecture and deployment options of OpenScape Concierge and are followed by configuration of the switches.

Thereafter follow the basic settings in **System Management** and **Concierge Data Center** to successfully connect a Concierge system to an OpenScape Voice or OpenScape 4000 with or without OpenScape Contact Center integration.

NOTE:
The order of the given information in these chapters tries to reflect the order of configuration steps that are necessary after the installation.

NOTE:
The manual was written for technical specialists (e.g. personnel responsible for integrating, installing and managing the software).

1.1 Terms and notation

This section describes the terms and notation used in this manual.

1.1.1 Style

Table: Style

Convention	Meaning
Bold	On-screen buttons and icons, menu items
Cursive bold	Database names, variables, fields, file names
UPPERCASE	Buttons (SHIFT, CTRL, ALT)
Italics	Commands, examples, folder names
`Courier`	Output texts and error messages, parameters, source text

1.1.2 Terminology

The following terms describe actions that should be performed using the keyboard or mouse, as well as the command button statuses on the screen.

Table: Terminology

Term	Meaning
Press	Press a key on the keyboard.
Input	Enter letters, numbers, database names, variables.
Enter	Press the confirmation key (ENTER or Return).
Double-click	Click the left mouse button twice quickly.
Right-click / right mouse button	Click the right mouse button once.
Select or highlight	Click an item once with the left mouse button.
Drag	Select an object and click and hold the left mouse button while moving the object to a new position.
Drop	Release the left mouse button to drop the dragged object. This can only occur after you have dragged an item.
Active / released	Active commands are displayed as black text on the screen. This means that they are available to the user. Active icons are displayed in their usual colors if available.
Deactivated / not released	Deactivated command buttons and icons are displayed in gray on the screen, meaning that they are not available to the user.
Button / icon	Buttons for performing functions

1.1.3 Notes

The following notes are used in this manual:

NOTE:
Identifies useful information which is important for the working process.

IMPORTANT:
Indicates a situation that could result in functional disorders or damage to property.

1.2 Abbreviations

Table: Abbreviations

Abbreviation	Name	Meaning
ACD	Automatic Call Distribution	Automatic distribution of calls (call center telephone system)
ART	ACD Routing Table	OS4K ACD routing table
BDE	Borland Database Engine	
CBC	Concierge Button Config	Concierge Admin tool
CDC	Concierge Data Center	Concierge Admin tool
CF	Call Forward	Setting in OSV
CFU	Call Forward unconditional	Setting in OSV
CLM	Concierge Layout Manager	Concierge Admin tool
COS	Class of Service	
CPS	Concierge Provider Service	
CTI	Computer Telephony Integration	Integration of telephone system and supporting software
DB	Database	
DDI	Dialed Digits Inwards	Direct dial number
Dll	Dynamic link library	
ETB	Electronic phonebook	Part of the OpenScape Concierge application
MLHG	MultiLineHuntGroup	Multiline hunt group in OSV
MoH	MusicOnHold	Music on hold setting in OSV
OS4K	OpenScape4000	PABX / Telephone system
OSC	OpenScape Concierge	OpenScape Concierge application
OSCC	OpenScape Contact Center	ACD of OpenScape Voice
OSCC-E	OpenScape Contact Center Extension	Contact center solution package from the CoC environment
OSV	OpenScape Voice	Soft switch
OCX	OLE Control Extension	Program module
PABX	Private Automatic Branch Exchange	OpenScape 4000, or OpenScape Voice
RCF	Remote Call Forward	Setting in OSV
RCG	Route Control Group	Setting in OS4K

Abbreviation	Name	Meaning
SDK	Software Developer's Kit	Development software
SIP DN	Session Initiation Protocol	Setting in OSV

2 General

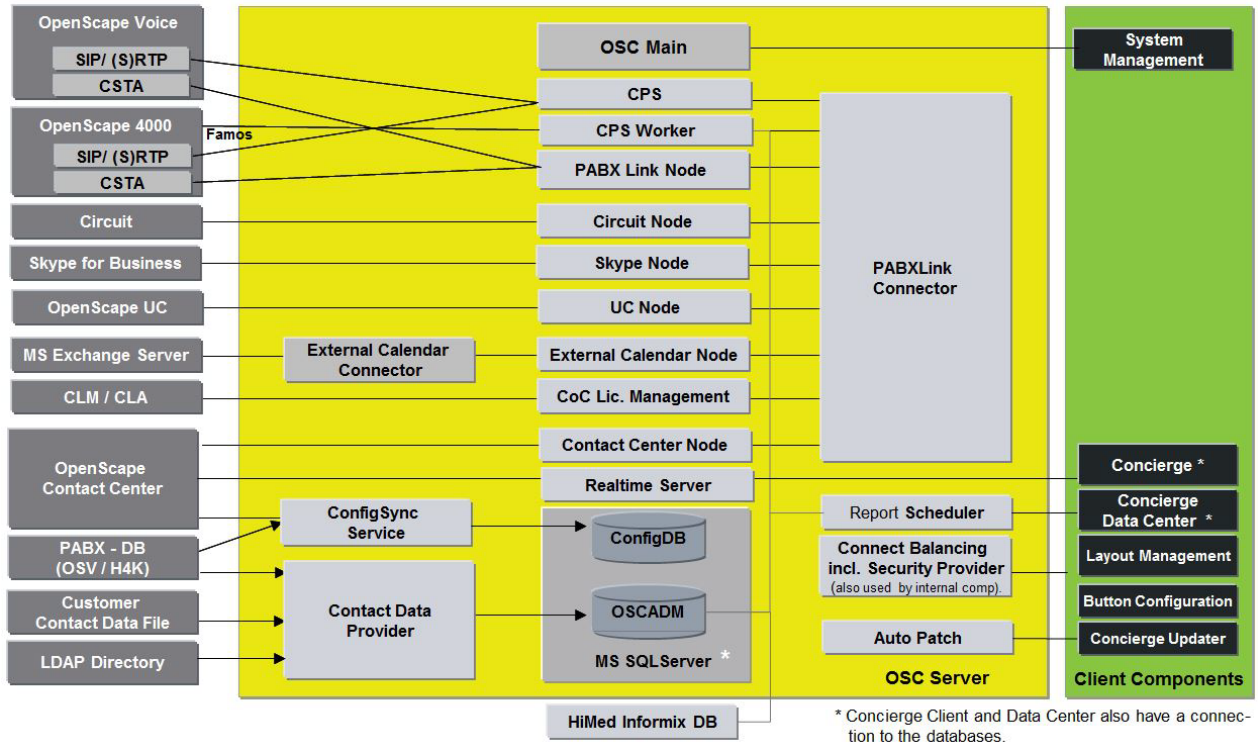
IMPORTANT:
This manual is subject to change. Before using it, make sure you have the latest version!

This manual provides an overview of the required components and configuration for **OpenScape Concierge (OSC)**.

OpenScape Concierge V4 is the successor of OpenScape Contact Center Extensions (OSCC-E) V3R1.

2.1 OpenScape Concierge components of Server and Clients

The following overviews show the essential software modules and components of OpenScape Concierge.



Description of the most important OSC Server components:

On top of the figure the service **OSC Main** is displayed. It controls all processes on the machine and can be started and stopped using Windows services; it is named "**OpenScape Concierge Service**".

The MS SQL Server Express database on the main machine, with ***OSCADM*** and ***ConfigDB*** for hosting Concierge data.

Processes called *ControlConfigDB* and *ControlOscadmDB* are responsible for creating and maintaining the databases – these are not in the figure. This database can also be swapped out on a dedicated machine.

The central instance is the **PABXLink Connector** where all other function nodes connect to and integrate with each other. PABX Link Connector is responsible for synchronizing and controlling the single components.

The **CPS (Concierge Provider Service)** is responsible for controlling the calls that are handled by the Concierge users / attendants. Without OSCC the CPS is responsible for automatic push of calls to agents / attendants (ACD).

The CPS is responsible for holding, transferring and parking calls as well as for the pager functionality. When the call is assigned to an attendant and the attendant speaks with the caller CPS is not involved, it comes back to CPS if the agent parks or pages or transfers or holds the contact.

The **CPS Worker** is a worker process of CPS and is used for additional communication needs in case:

- OSCC is used to monitor OSCC call flow
- OS4K Famos interface is used to read and set Class of Service
- HiMed is used to synchronise patient data into OSConcierge database.

Contact Data Provider (CDP) is responsible for (automatically) importing contact data for the **Electronic Telephone Book (ETB)**. Multiple sources of different types can be used for that data import.

The **Realtime Server** consists of the Realtime Server and the Realtime Node which is part of the Contact Center Node.

The **UC node** connects Concierge with **OpenScape UC** for displaying the presence status and the media state of the UC extension to the attendant.

The **Circuit node** connects Concierge with **Circuit** for displaying the presence status of the Circuit extension to the attendant.

The **Skype node** connects Concierge with **Skype for Business** for displaying the presence status of the Skype extension to the attendant.

The **Microsoft Teams** node connects Concierge with Microsoft Teams for displaying the presence status of the respective Microsoft Teams user to the attendant (using the respective contact Microsoft Teams e-mail account)."

The **External Calendar** node connects Concierge with external calendar systems to provide external calendar information of contacts in ETB to the attendant. Internal calendar information can additionally be stored in the OSCADM by Concierge.

Report Scheduler Worker is responsible to process report schedules.

2.1.1 CPS

Besides the CSTA link the **CPS (Concierge Provider Service)** is the second important connection between OSC Server and the communication platform (OS400/OSV/OSCC). CPS is a central service in the system. It is responsible for the complete handling of the calls that are in scope of Concierge as well as for the handling of announcements for callers handled by Concierge.

Calls that are parked or appended are connected to the CPS where the caller can listen to defined music. Calls that are transferred are temporarily connected to the CPS as long as the target device has not accepted the call. This allows Concierge to always keep track and control of the calls until they are connected to the target party.

In case the required person does not answer, the CPS is the instance that decides how to proceed with the call. It is no longer the ***Intercept*** settings of the communication platform that make the decisions in case the target user can not be reached.

This way the CPS is always the master of calls for the attendant console. This includes RTP streams to the CPS. Concierge defines the handling in all possible scenarios and can report on what happened in every moment.

Finally the CPS also provides a simple ACD routing of incoming calls in installations without OpenScape Contact Center.

2.1.2 OpenScape Contact Center Integration

With the optional OpenScape Contact Center integration the following services are also required:

- **Contact Center Node**
- **CPS Worker** is mainly used with OSCC and is responsible for displaying the waiting OSCC calls in the Concierge GUI. Also COS changes are handled by CPS Worker.

2.1.3 Client Applications

Concierge is available in two versions:

- Professional (full version)
- Plus (limited version)

Differences are clearly marked within this document, but the displayed figures are based on Concierge Professional – so these might differ in case you configure a Concierge Plus environment. The Administrator and User Guide are available for both versions.

These client applications are used with OpenScape Concierge:

- OpenScape **Concierge Client** (Attendant Console application)
- **Concierge Data Center** (Concierge related configuration)
- **Layout Management** (Configuration of the Concierge client layout (look).
- **Button Configuration** (Speed- and Direct dial button configuration)
- **System Management** (Main server configurations)

Remarks

The **System Management** is the general administration tool for configuring the OSC Server's base parameters, like IP addresses, port numbers, database settings and passwords as well as OSC applications settings.

2.2 Deployment

The deployment of an OSC Server can be distributed on multiple servers (which can reside at different sites). The flexible deployment options are helpful for load sharing amongst multiple servers as well as for flexibly deploying redundant or standby scenarios, depending on the customer's needs.

2.2.1 Sites

A **site** defines a location, where an OSC Server is assigned to. Finally the site corresponds to the PABX the OSC system is connected to.

One **Master Site** is configured, means the Main PABX, where the OSC Server connects to. The system also integrates with an existing OSCC system that belongs to that main PABX.

Additional **Monitored Sites** can be configured for monitoring the extensions on other communication platforms by the actual deployment, like e.g. for the Concierge's busy lamp field feature.

Further server machines can be assigned to a deployment, but only one server can be the **Main Server** in a deployment. The **Main Server** hosts the configuration of the whole deployment and runs central components like licensing and configuration synchronization processes.

2.2.2 PABX Connections

Under PABX Connections you configure the settings for the **communication platform that is associated with a site**. It does not matter if it is a main site or a monitored site.

NOTE:
Each PABX connection in a deployment matches a site.

For communication platforms with multiple exits to Central Office (CO) it is possible to configure additional local trunks/ CO exits for a given PABX connection.

In case multiple local trunks or sites are in use a database routing can be defined that allows Concierge to route calls to target extensions in multiple sites.

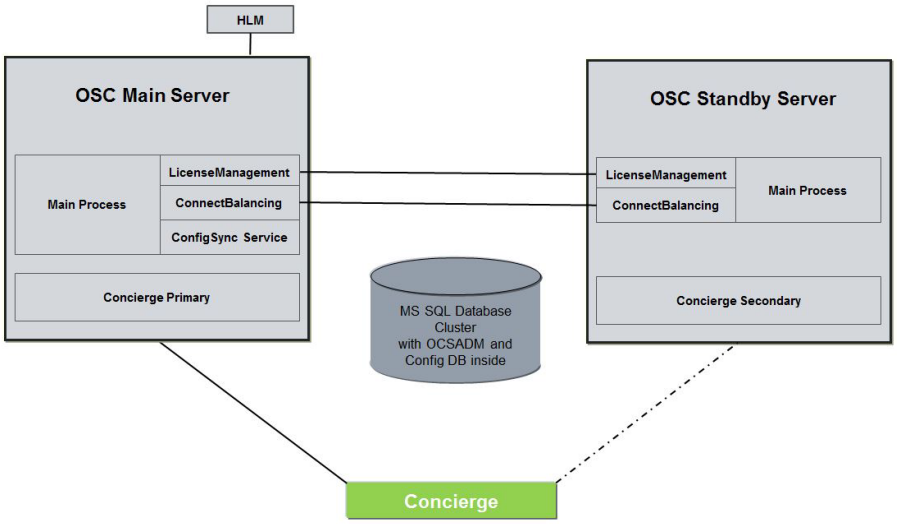
2.2.3 Contact Center Connections

The OpenScape Contact Center system that is connected to the Master Site's PABX can be assigned to the given Open Scape Concierge. The OSCC IP parameters are required.

Also an **OSCC high availability** deployment can be integrated, and then both servers are configured.

NOTE:
OSCC can only be assigned to the **Master Site**. Thus **one** Contact Center connects with **one** OSC deployment only!

2.3 Redundancy / Standby deployments



Further scenarios for standby are described later!

2.3.1 Trigger points for switch over

The Solution Level redundancy in OSC works in a hot standby mode. The respective components on Main and Standby Servers are always active and keep identical information. So Standby Server can take over the service without any interruption, if Main Server fails.

The Application Level redundancy for OSC is designed as a warm standby solution. If a defined “core component” for any redundant application fails, this is recognized by the central **OpenScape Concierge Service** and a switchover is initiated. It is foreseen, that all connections between client and the presently active server will be switched over to the secondary or respective primary server, if the secondary was active before. The switch over can take some time (depending on the environmental conditions up to some minutes).

NOTE:
There will be no automatic switch back to the Primary server after it is available again. This is designed to avoid additional connection lost on client side. A planned switch back can be forced by manual interaction.

The following situations will force a switch over to the Secondary Server:

- Primary Server down (hardware or system level)
- Network Connection lost (i.e. NIC or switch port defect)
- **OpenScape Concierge Service** Service down
- PABXLink Connector Process down
- PABXLink Node Process down, Connection to the Telephony System lost
- Contact Center Node process down
- Concierge Provider Service (no complete switchover, but reconnect to the Secondary Concierge Provider Service instance, connected to the **OpenScape Concierge Service** on the Secondary server).

The following processes are **not used as triggers** for switch over:

- ConfigSyncServer process

- CpsWorker process
- Realtime Server process
- UCNode process
- External Calendar Connection processes
- ContactDataProvider process

If such a service fails the functions provided by it will not be usable until the connection was successfully re-established, e.g. no UC states if UC service is down.

NOTE:
After an automatic switch over to the standby system it is recommended to execute a manual switch back shortly after the Primary Server is back in service to avoid
- additional communication flow between the Primary and the Secondary Server and
- client connections on both the Primary and the Secondary Server.

2.3.2 Standby installation scenarios

Two installation scenarios can be a start point for a standby/redundant environment:

Scenario 1

A new OpenScape Concierge project realization is implemented as a redundant solution. All required servers are available in advance to the installation and configuration.

Procedure

As the Standby server will be installed (see OpenScape Concierge, Server, Installation Guide) and configured (within the System Management – see from section 6 System Management) right from the beginning, all relevant processes for the Standby server will be set and started automatically after the configuration within the System Management is published.

IMPORTANT:
During configuring the applications as described in section 6.3 Section Applications – do not forget to configure redundancy. Also see “Scenario 2” under “Procedure for applications”.

Scenario 2

The Standby server has to be installed and integrated into an existing and productive standalone OSC environment.

Procedure for OSC Server

1. Start the System Management application on the Main server. It is important that it is active so the new standby server can be recognized by the Main Service.
2. Run the OSC Setup procedure for the Standby server (see OpenScape Concierge, Server, Installation Guide).
3. After the installation and the reboot of the Standby server, the OSC Main-Service starts automatically and as soon it has reached the corresponding run level the new Standby server appears in the **Control Center** tab of the System Management application on the Main Server with its base processes (ConnectBalancingServer Secondary,

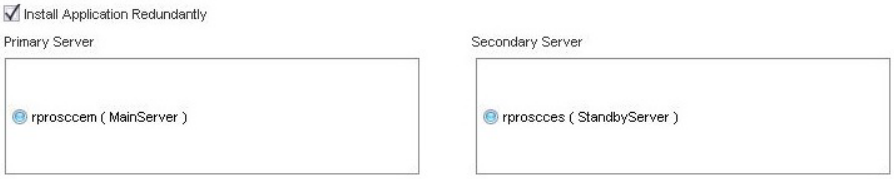
HttpServer, LicenseManagementServer Secondary, LogTranferProcess, SnmpAgent). Those processes – except SnmpAgent - should become green (with correct licenses) after a while.

4. Check in System Management the tab **Installation Designer** under **Resources / Servers**. Your Standby server should be listed here.
5. **IMPORTANT**: Acknowledge the new server by Publishing the automatically added configuration in the System Management. As the data must be written into the Main server machine's configuration file. Execute a "Publish" by pressing "**F5**" or selecting "**Action → Publish Installation Data**".

2.3.3 Configuration of the Application redundancy

After completing these steps you have a redundant OS Concierge system, but the redundancy is not yet used by any application. Follow the next steps to configure redundancy for the applications:

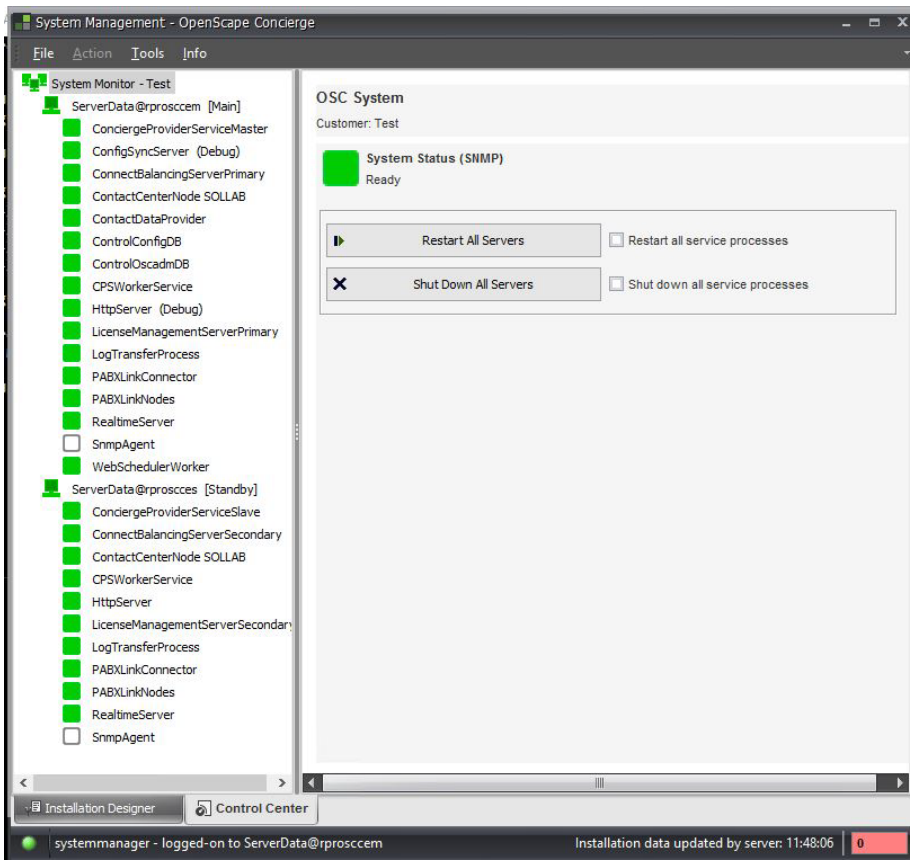
1. Configure redundancy in the System Management under **Applications → Concierge**. Mark the checkbox „Install Application Redundantly" to activate redundancy.



2. As soon as this feature is activated the **Secondary Server** field appears and lists all available secondary servers with usage type Standard. Select the appropriate server as Secondary server (Standby server) for this application.
3. Publish the configuration with "**F5**" or by selecting "**Action → Publish Installation Data**". All application relevant processes should appear in the **Control Center** tab under the selected secondary server per application.
   - ConciergeProviderServiceSlave
   - ContactCenterNode (only with OSCC)
   - CPSWorkerService (only with OSCC)
   - PABXLinkConnector
   - PABXLinkNode
   - RealtimeServer (only with OSCC).

   Depending on system configuration additional processes are possible: ExternalCalendarConnector, ExternalCalendarNode, UCNode

   The figure shows all processes that should be visible in case the standby server was configured for all above mentioned applications:



NOTE:
Please be aware, that during time periods the OSC system is running in standby mode (the clients connected to their Secondary servers) the following processes are not active and the respective features are not available on client side:
Basis: ConfigSyncServer – no synchronization between OSC ConfigDB and OSCC and/or telephony system(s) possible.
ContactDataProvider – no import for new phonebook data into the ETB possible.

3 Prerequisites check

3.1 Additional documentation

Make sure you have following up-to-date documentation at hand

- OpenScape Concierge Plus, Administrator Documentation
  or
  OpenScape Concierge Professional, Administrator Documentation
- OpenScape Concierge Plus, User Guide
  or
  OpenScape Concierge Professional, User Guide
- OpenScape Concierge Server, Installation Guide

3.2 Staff prerequisites

The manual was written for technical specialists (e.g. administrators of the OpenScape Contact Center and personnel responsible for integrating, installing and managing the software). The following prerequisites are required:

- Knowledge of OSV / OS400 / OSCC administration
- Successful OS Concierge Service Training participation

3.3 General

Before proceeding with the sections 6 System Management and 8 Basic Data Center configuration for Concierge, please check that all required configurations and settings in OSV / OpenScape 4000 / OSCC are done and the information about these settings is at your disposal.

If the settings in the communication platform are properly configured, proceed with sections 6 System Management.

If the configuration of the communication platform is required, please see the following chapters:

- For OpenScape Voice configuration refer to section 4 Switch configuration OpenScape Voice.
- For OpenScape 4000 configuration, refer to section 5 Switch configuration OpenScape 4000.

IMPORTANT:
The example configurations in this manual describe a configuration in the environment of the lab. In customer's environment other parameters are required, like e.g. different Server names, IP addresses, number ranges, prefix access codes, etc.

Only trained staff should configure and adopt the configuration to the customer's environment.

4 Switch configuration OpenScape Voice

IMPORTANT:
The configuration examples in this section describe a configuration in the environment of the lab. In customer's environment other parameters are required, like e.g. IP addresses, number ranges, prefix access codes, etc.

Only trained staff should configure the OpenScape Voice and adopt the configuration to the customer's environment.

In this section the OpenScape Voice settings required for integrating OpenScape Concierge are described for scenarios without and with OpenScape Contact Center.

4.1.1 OSV connection without OSCC

The incoming calls to the pilot numbers all route to the Concierge Provider Service (CPS) that is connected via SIP trunking.

The calls are queuing in CPS and stay there until further actions are required; the calls for the personal line of an attendant also queue in CPS.

CPS assigns the call to the attendant or the attendant picks the call.

In case the CPS is down calls are handled by fallback hunt group routing in OpenScape Voice.

4.1.2 OSV connection with OSCC integration

With OpenScape Contact Center (OSCC) the incoming calls for the attendants are routed by OSCC – also the backup routing case is handled by OSCC strategies.

Incoming calls to the personal lines of the attendants are handled as described in the scenario without OSCC. These calls are queuing in CPS and CPS assigns the call to the attendant or the attendant picks the call from the personal queue.

In the following sections the configuration of devices is described as well as the configuration of the SIP trunk and the fallback hunt group mentioned above.

4.2 Concierge Provider Service (CPS)

4.2.1 Features and functionalities

CPS

CPS is the central instance for controlling the calls that are handled by the Concierge user.

Processing Queue

Calls that are parked or on hold, calls that need to be transferred or require the paging functionality to be connected with the target person, all these calls are transmitted to the CPS and wait there for further handling. That is why this position is called the **processing queue**.

As the CPS is an internal resource of the OSC Server, Concierge is fully controlling what happens with a call and displays this information on the upper right pane to the Concierge user.

In case of a standalone installation, where no OpenScape Contact Center is in use, the CPS also queues the calls that come in via the pilot numbers and allows a simple call push (ACD) to the attendants which are assigned to the pilot number.

Transferring calls is controlled by CPS in a way that calls that are meant to be transferred to a target extension are “parked” on CPS on one channel where another channel of CPS tries to reach the target device. The connection between both only happens if the target person answers the call. Otherwise the call stays connected to CPS. The call can be controlled and handled by Concierge user (even if the Concierge user is in a call with another customer).

During the transfer process the call is visible in Concierge.

CPS acts as a media server for Concierge calls. Data Center allows to specifying different types of music / wave files that can be assigned in multiple handling scenarios, for example a personal greeting wave file can be assigned for every Concierge user that is played to the caller as well as to the attendant right before the call is connected.

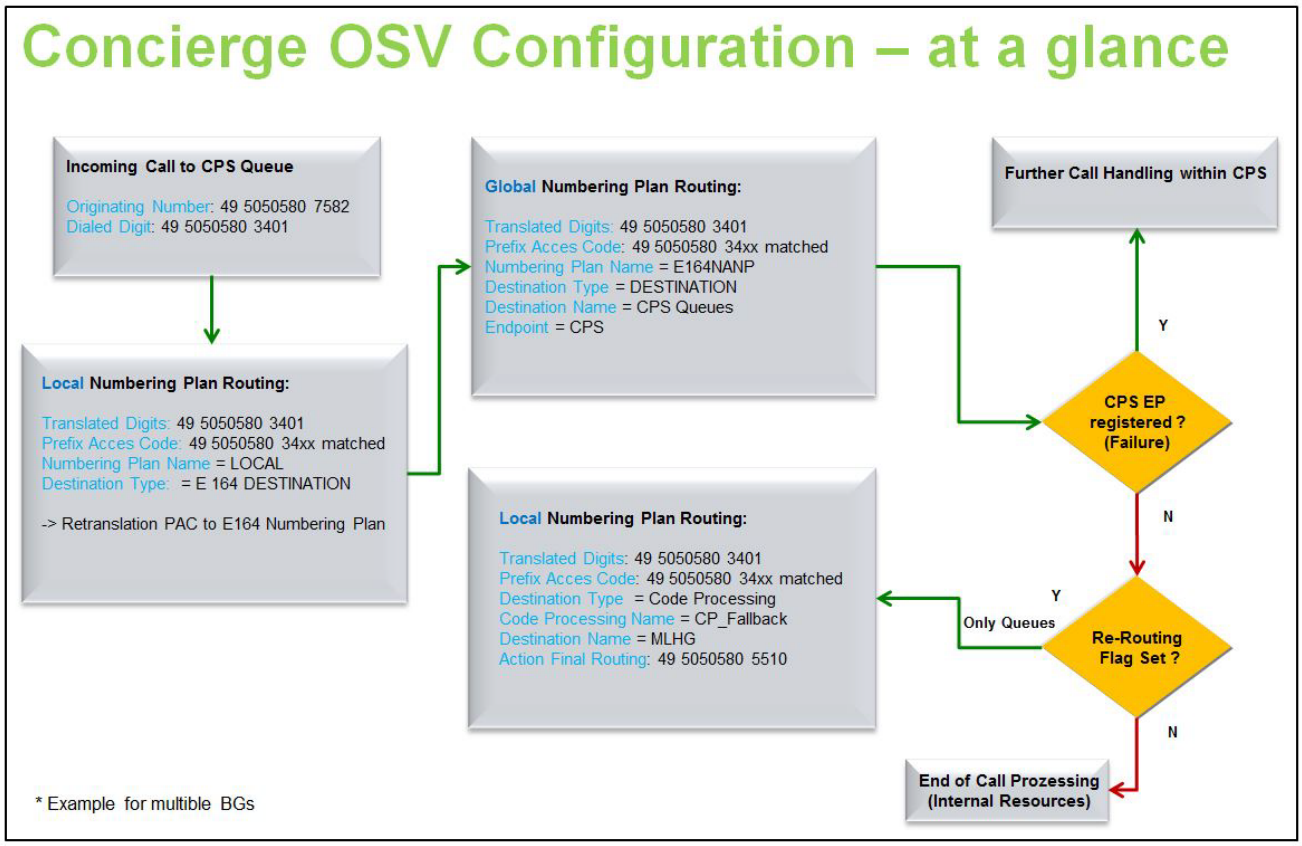
The functionality described requires the CPS to be connected via SIP trunking to the communication platform. All numbers using this trunk have to be in E164 format.

4.2.2 CPS Integration / Backup Routing

For a proper handling in case CPS fails or the SIP trunk connection is down a fallback routing is required. The calls which cannot reach CPS will fall back to hunt group routing in OSV, all Concierge users must be members in that hunt group.

Overview: Routing and fallback of pilot numbers and personal calls

Incoming calls are routed to the SIP trunk for CPS. In case CPS is down, the call is re-routed to a hunt group in the local business group.



In case of a failure the calls will not be handled by CPS; the OSV will route the calls to the local BG's routing and a code processing takes place that deletes the original pilot number and inserts the number of the fallback hunt group as destination.

With this information the call routes to BG's local hunt group for backup. The fallback routing is only activated for incoming calls (pilot numbers and personal line numbers). For the internal CPS resources the fallback routing will not take place.

4.3 Concierge user device configuration

4.3.1 Configuration pages

The following must be configured on the terminals (e.g. OpenStage) used by the Concierge users:

- Administrator Pages -> System -> Features -> Configuration -> Allow uaCSTA = enabled
- Administrator Pages -> System -> Features -> Configuration -> Server features = enabled
- Administrator Pages -> System -> Features -> Addressing -> Conference = <valid code for conference factory>
- Administrator Pages -> System -> Features -> Feature access -> Blind transfer = enabled
- Administrator Pages -> System -> Features -> Feature access -> Call forwarding = enabled
- Administrator Pages -> System -> Features -> Feature access -> Feature toggle = enabled
- Administrator Pages -> System -> Features -> Feature access -> CTI control = enabled
- Administrator Pages -> System -> Security -> System -> Use secure calls = disabled
- User Pages -> Configuration -> Incoming calls -> Handling -> Allow call waiting = disabled

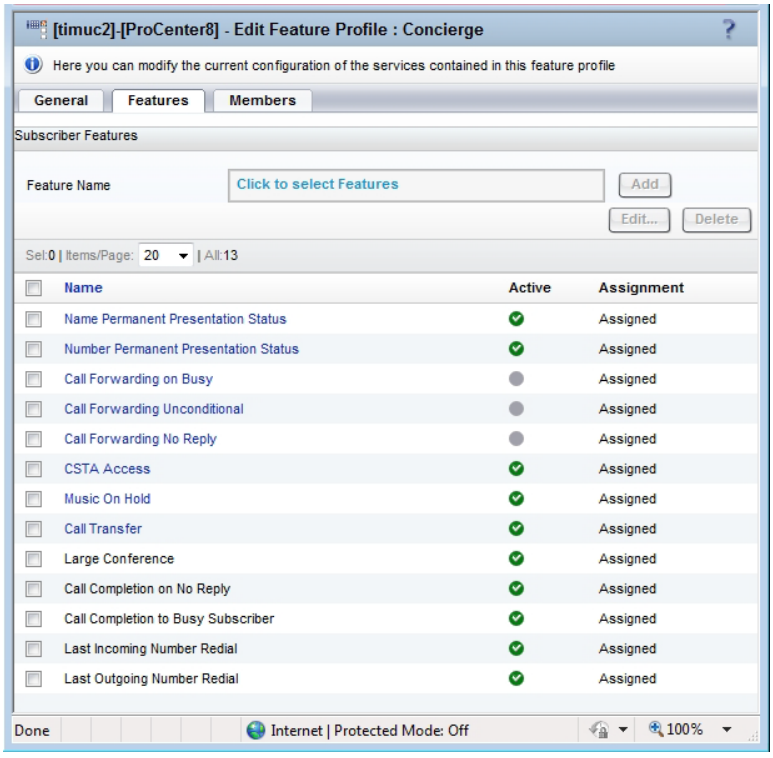
- User Pages -> Configuration -> Incoming calls -> Handling -> Allow DND = disabled
- User Pages -> Configuration -> Incoming calls -> Handling -> Allow busy when dialing = disabled
- User Pages -> Configuration -> Connected calls -> Allow call transfer = enabled
- User Pages -> Configuration -> Connected calls -> Allow music on hold = disabled
- User Pages -> Configuration -> Connected calls -> Allow conferences = enabled
- User Pages -> Configuration -> Incoming calls -> CTI calls -> Allow auto-answer = enabled

4.3.2 Concierge phone settings in OSV for CPS fallback

Concierge endpoints are members of the Fallback Hunt Group (in the example below the +4950505805520)

4.3.3 Feature profile for Concierge user devices

Configure the Feature Profile for Concierge User devices with the following parameters:



The relevant CSTA type has to be selected in the feature profile for the contacts whose status is to be monitored by OpenScape Concierge.

Submenu “Call Forwarding Unconditional”:

- Activate via: All
- Specify redirect number via: All

Submenu "Call transfer"

- Transfer Calls: All
- Disallow transfer to restricted party: No

Submenu "CSTA Access"

- CSTA Type: CSTA Over SIP

NOTE:
In case the user is handling a Concierge call, his device is busy. Direct calls for that device are forwarded by Concierge to the user's personal line number and queue in CPS for being handled by the user. Therefore the call forwarding unconditional via CSTA must be enabled.

4.3.4 Monitored devices of office users

The relevant CSTA type has to be selected in the feature profile for the contacts whose status is to be monitored by OpenScape Concierge.

Submenu "CSTA Access"

- CSTA Type: CSTA Over SIP

Submenu "Call Forwarding Unconditional":

- Activate via: All
- Specify redirect number via: All

If Concierge should be able to change/see the call forwarding entry of an office user, **server based features** must be enabled in the terminal.

For those office users that require intercept function to Concierge, the Call Forwarding feature "CFNR" and "CFB" in the Feature Profile of these users must be configured. Configure the corresponding DDI entries for **CF no reply** and **CF busy**.

4.4 Routing configuration in OSV without OSCC

4.4.1 DDI settings in OSV

All incoming calls are handled by CPS and thus have to be routed to the SIP endpoint for CPS. There are number ranges for pilot numbers / personal lines as well as ranges for the request pool and callback pool, which are used to route calls to CPS. The CPS is fully responsible for the call handling.

In case the CPS / Concierge server fails, the calls will be routed to a dedicated fall back hunt group that is used for Concierge only. All attendants' devices have to be member in that hunt group to be able to handle the calls in a fall back scenario.

4.4.2 CPS number ranges

As described above the CPS is Concierge's central service for handling calls. Without OSCC the calls to the pilot numbers are directly routed to CPS and queue there for being distributed.

The connection to CPS needs two types of number ranges:

- one for pilot numbers and personal line numbers of attendants
- one for internal CPS resources like Request pool and Callback Pool

Furthermore if CPS fails, a Fallback Hunt Group has to be defined in the OSV, where all attendant users are members.

In the following description a basic fallback configuration is displayed where all types of incoming calls route to the same hunt group in case of failure.

The fallback solution is used in case of CPS failure for the personal lines and service number (queues). These calls coming in via pilot numbers and personal line numbers are routed to the fallback hunt group.

The internal resources like callback numbers and request numbers are not in use when CPS fails. Therefore no fallback solution for those is required.

Definition of number ranges for example configuration used in this book:

Parameter	Description	Value
CPS Resources for the example in the following sections		
Pilot Numbers Start	Numbers that route to CPS used for Pilot Numbers (DDI Lookup table)	+4950505803201
Pilot Numbers End		+4950505803219
Personal Lines Start	Numbers that route to CPS used for Personal Line Numbers of Attendants	+4950505803220
Personal Lines End		+4950505803299
Loop Number	Used in Multi-CPS environment	+4950505803300
Request Numbers Start	Numbers that route to CPS used for internal tasks, like e.g. Park, Append	+4950505803301
Request Numbers End		+4950505803349
Callback Numbers Start	Numbers that route to CPS used for paging service (Park Slot Numbers)	+4950505803350
Callback Numbers End		+4950505803399
Fallback Hunt Group	Hunt Group for Calls to Pilot and Personal Line Numbers, if CPS fails	+4950505805520

NOTE:
The CPS Loop number is used in a Multi-CPS environment like e.g. when deploying a redundant Concierge Server System. In that case the CPS on the Standby server machine is frequently calling this number and expects a corresponding loop back message from the switch.
This message is only send if the CPS on the Main Server is active and running. If the call is not answered by a loop back message, the CPS on the Standby Server assumes that the CPS on the Main Server is not running and starts getting active by itself.

Please assure that the Loop number routes to the CPS endpoint in OSV.

4.4.2.1 Formula for estimating the number range of internal CPS resources

Use this formula to calculate the range of the internal resources:

Range of request numbers: 8 plus number of agents

NOTE:
During the transfer from the client to the processing queue a request no. is used. When the call reaches the CPS (arrived in the processing queue) the request no. is usable (free) again.

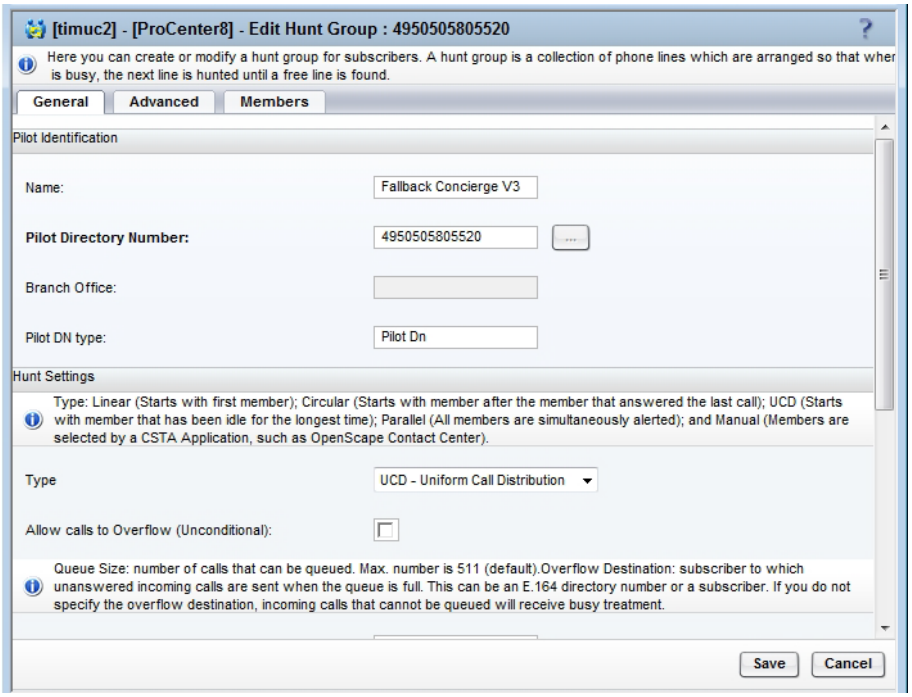
The request range does not limit the count of calls in the processing queue.

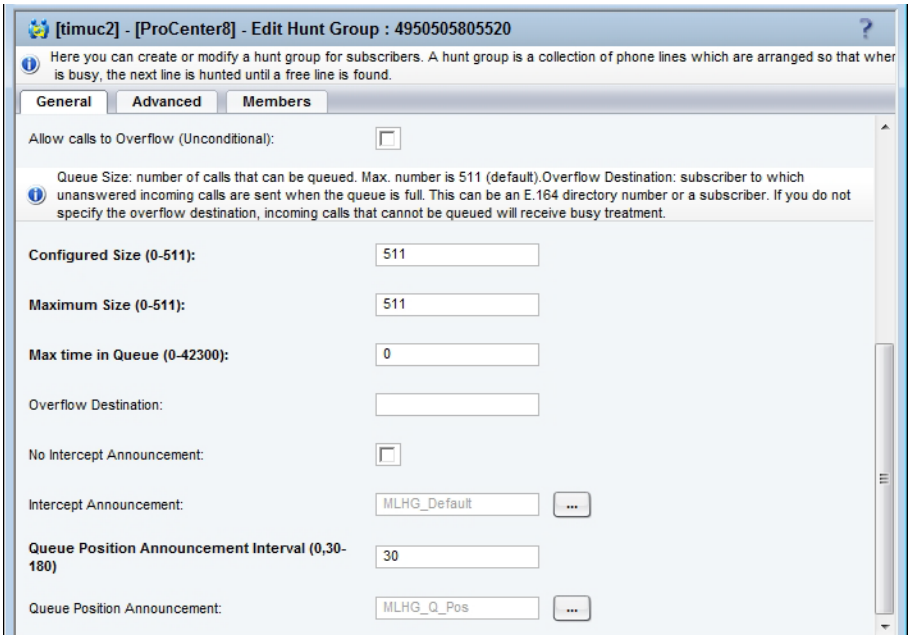
Range of callback numbers: 3 plus the maximum number of calls that shall be parked for the paging functionality

4.4.3 Fallback Hunt Group

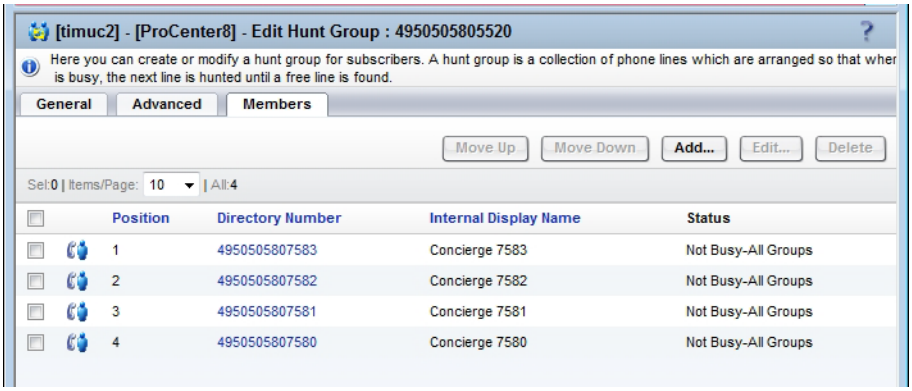
Business Group

1. Create the fallback hunt group **(e.g. +4950505805520) with hunt type "**UCD**" and name it "**Fallback Concierge V3**".**
2. The users, profile only members and hunt groups need to be configured in the appropriate Business Group.
3. Create a profile only subscriber (e.g. +4950505805520)
4. Create a Hunt Group based on this profile only subscriber

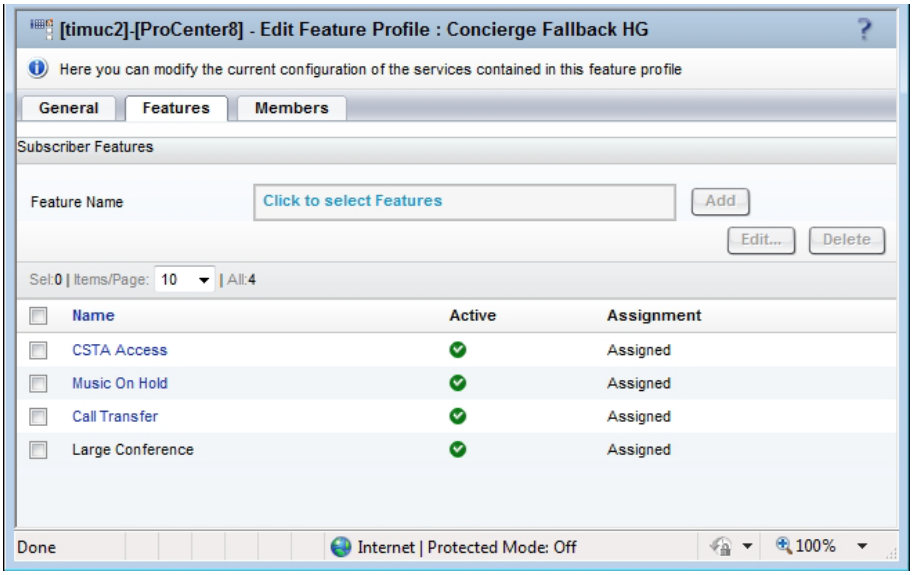




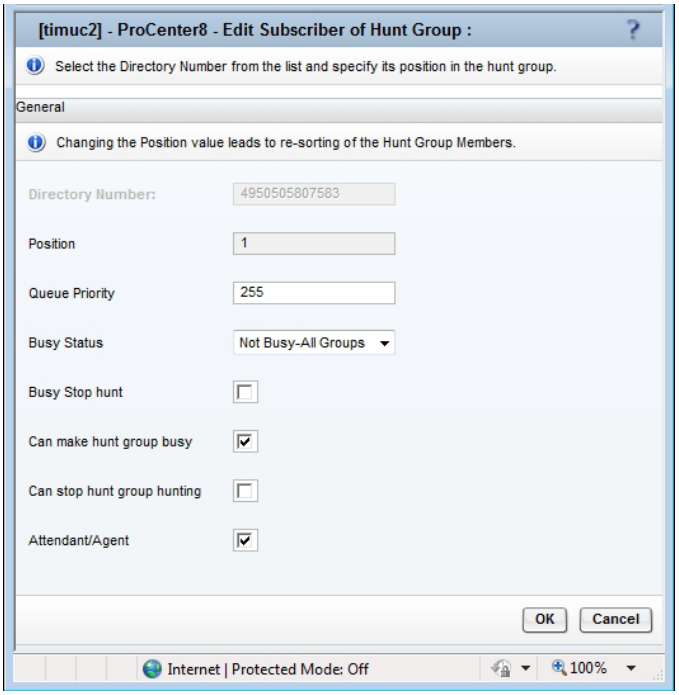
5. Add all Concierge members (phones) to this HG



6. Verify that the number of the hunt group can be dialed and the members can be reached.
7. For the hunt group pilot number's extension the following parameters have to be configured in the feature profile:



8. In the selected members, the options **"**Can make hunt group busy**"** and **"**Attendant / Agent**"** have to be activated. More details can be found in the OpenScape Voice Configuration Manual.



4.4.4 Routing Configuration for SIP endpoint CPS in a single BG environment

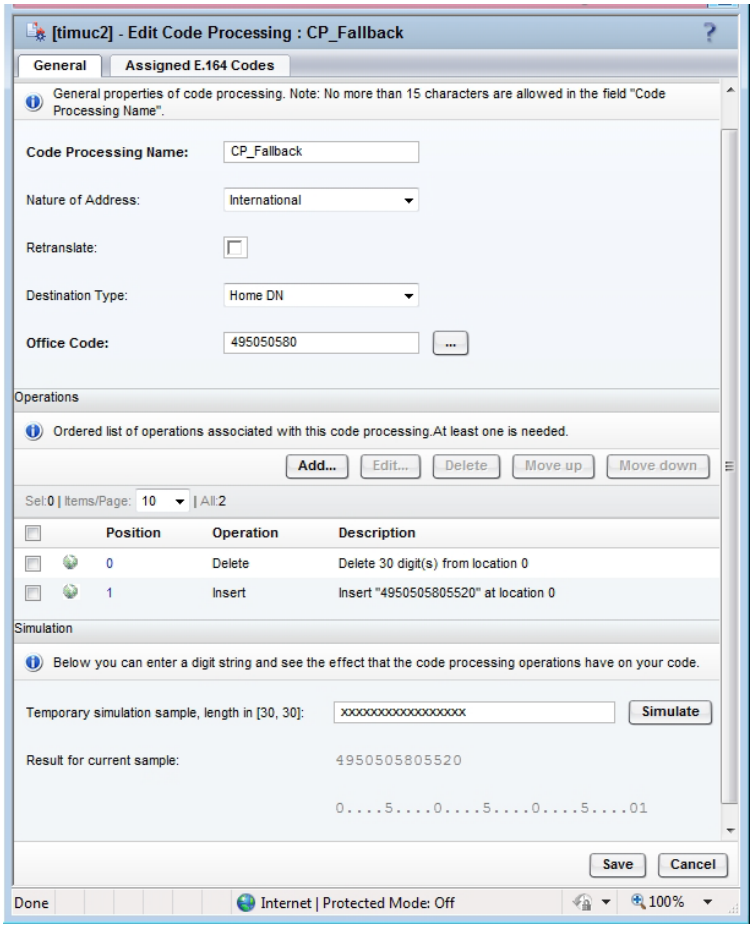
If you have just a single BG you will need a **central numbering plan** (not common numbering plan). CDC generates a headquarter named “Site1” per default. So the name “NP_Site1” is used as **central numbering plan** for all examples below.

For **fallback** – means if the CPS cannot be reached anymore – a **code processing** is required in the global numbering plan that deletes the pilot numbers to CPS and replaces these with the fallback hunt group pilot number.

NOTE:
The internal resources do not fall back to the hunt group!
(If CPS is down Concierge will not use internal resources anymore)

Global Translation and Routing

1. Create a **Code Processing "CP_Fallback"** with the following operations: **NoA**= international; **Destination type**= Home DN; **Office Code** of the used BG
2. **Delete** 30 digit(s) from location 0
3. **Insert** "<Number of Hunt Group>" (e.g. 4950505805520) at location 0



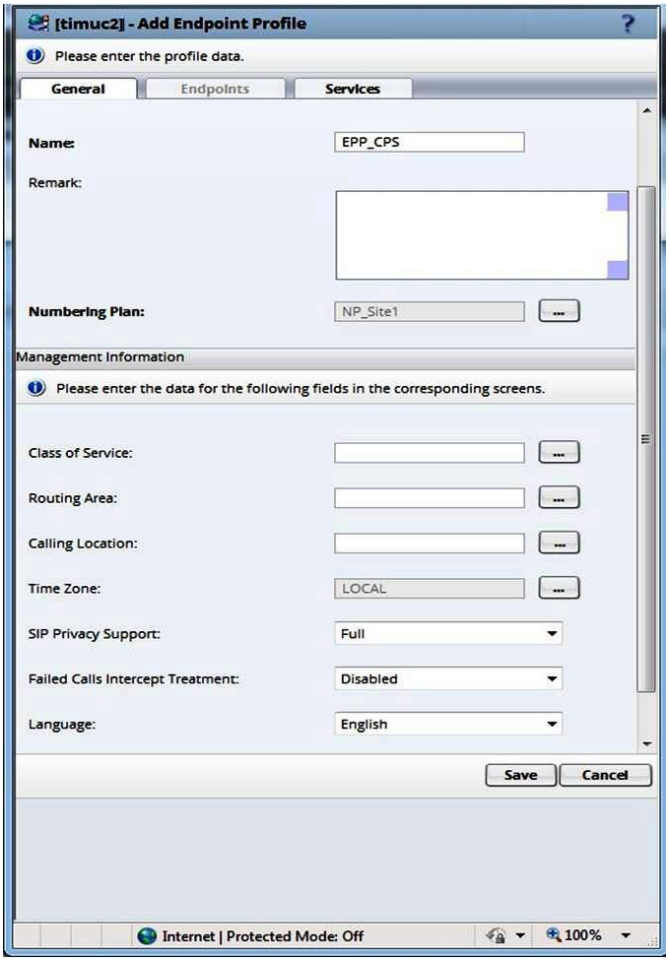
NOTE:
Pilot number dialed is deleted and replaced by the fallback hunt group number.

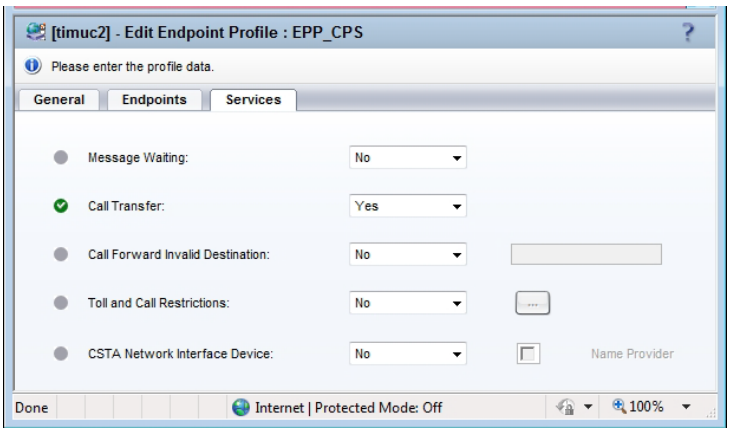
NOTE:
If you want to separate the fallback destinations for each site, you have to generate one fallback hunt group for each site and create a Code Processing for each site.

4. Create an **Endpoint Profile** "EPP_CPS" with **SIP privacy support** set to "full" and service "Call Transfer" in the **central numbering plan** (e.g. NP_Site1) of the BG.

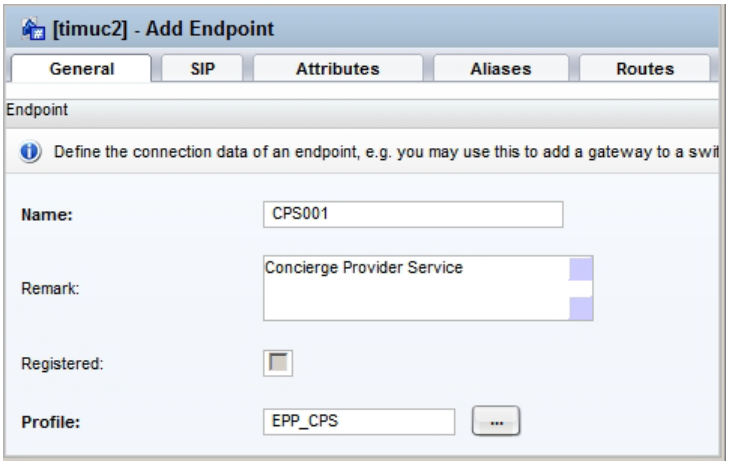
NOTE:
Up from OSCC-E V3R1 outgoing Invites have the SIP header “X-Siemens-CDR” included. This enables OSV to use different numbering plans for routing decisions depending on the initiating Concierge working place. The numbering plan associated with the Concierge working place will be used for outgoing calls - not the numbering plan of the CPS-endpoint anymore. The dialed number can be in the same format as if it was dialed directly from the Concierge‘s associated handset.

If OpenScape Voice receives a SIP INVITE or REFER request containing the X-Siemens-CDR header field with the charge parameter then charge number will be stored as the billing number in the CDR. In addition the number plan, rate area, and code/toll restriction services associated with this charge number will also be used to process the call.

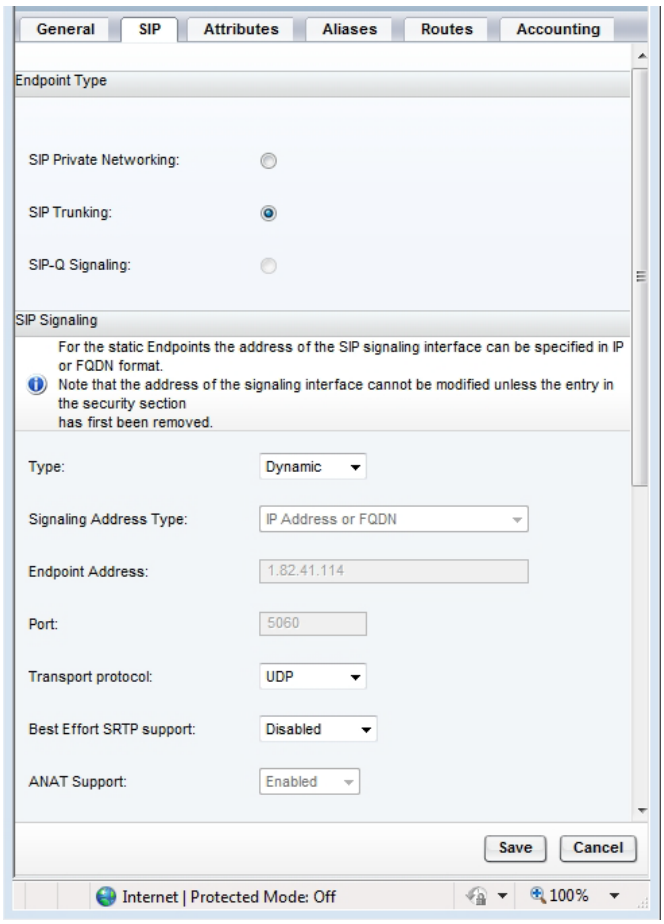




5. Create an Endpoint **named "CPS001" using this profile.**



6. On tab SIP choose "**SIP Trunking**", **type**: "Dynamic", **transport protocol**: "UDP" and **best effort SRTP support**: "Disabled".
   Up from OSV V8: disable the ICE Support and set the Outgoing Call Supervision Timer to 32000ms.



7. On tab **Attributes** check "Supports SIP UPDATE Method for Display Updates", "UPDATE for Confirmed Dialogs Supported", "Accept Billing Number", "Allow Sending of Insecure Referred-By Header", "Send International Numbers in Global Number Format (GNF)","Rerouting Forwarded Calls", "Enhanced Subscriber Rerouting" and "Enable Session Timer".

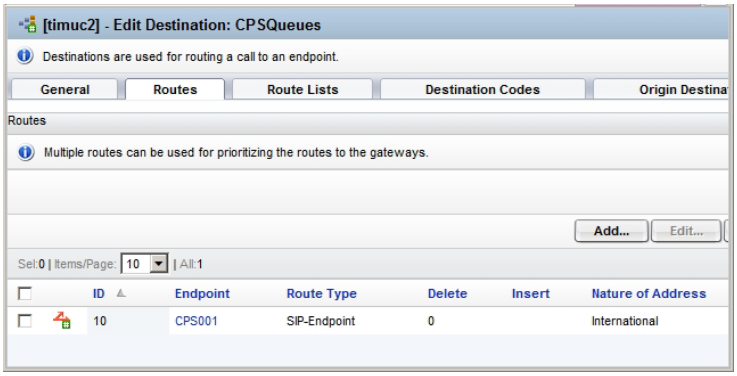
8. On tab **Aliases** add the alias "**CPS1**" and the **IP address** of the CPS Server. (Add also the IP of the second CPS Server, if redundancy is used).

NOTE:
Add the IP Addresses to the Realms within "Administration – Signaling Management – Digest Authentication", if your security policy requires it.

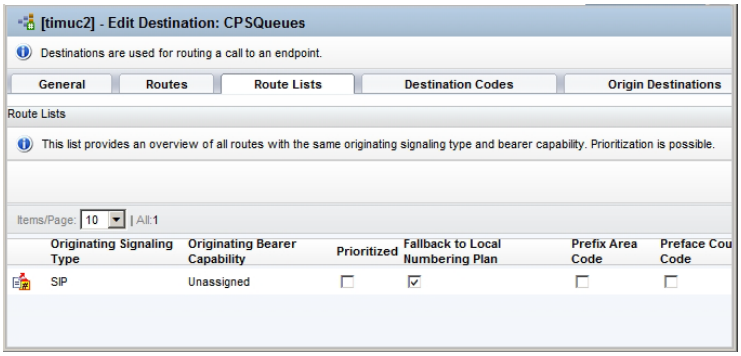
NOTE regarding Routing:
It is important to make sure that all phones (Concierge and Office) and Gateways are able to reach all numbers defined above.

9. Create the Destination "**CPSQueues**" for **Pilot numbers** and **personal lines** in the common numbering plan (NP_Common) of your BG.

10. Add a route to endpoint "**CPS001**" using **Modification Type** “Number Manipulation” and **Nature of Address** “International”

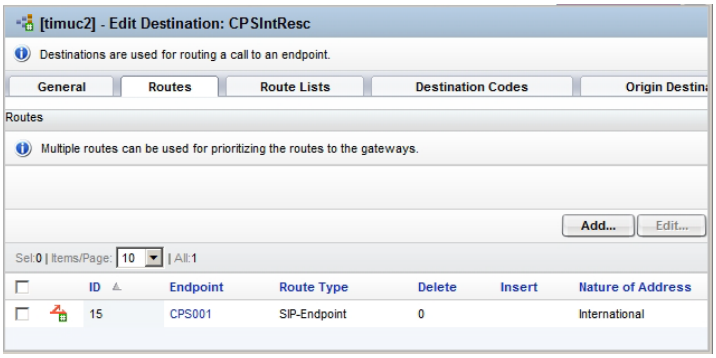


11. On tab Route Lists check "**Fallback to Local Numbering Plan**"

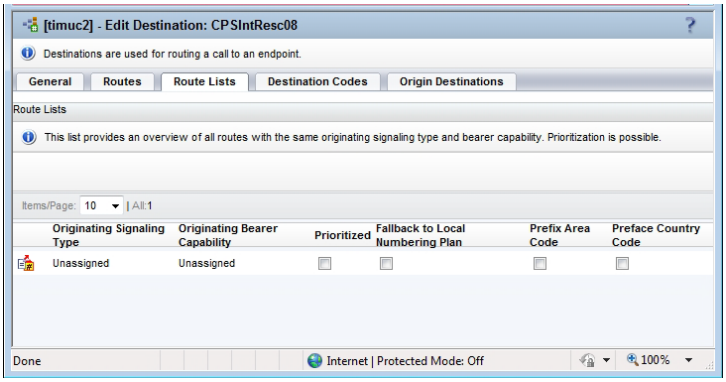


12. Create the Destination **"CPSintResc"** in the common numbering plan (NP_Common) of your BG.

13. Add the route to endpoint "**CPS001**" using **Modification Type** **“**Number Manipulation**”** and **Nature of Address** **“**International**”**



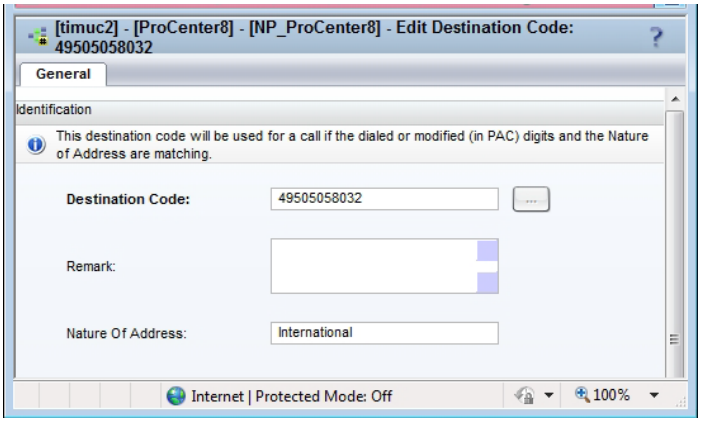
14. On tab Route Lists **DO NOT** check "Fallback to Local Numbering Plan"

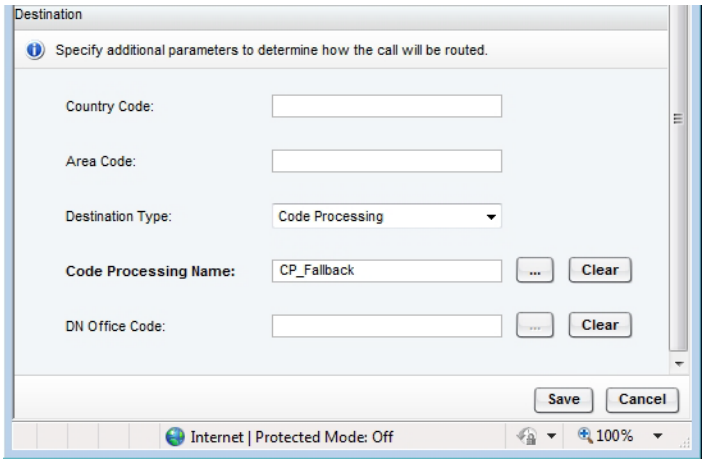


In the BG's numbering plan **destination codes** and **prefix access codes** have to be defined for the queues' pilot numbers as well as for the personal line numbers.

Pilot numbers and personal line numbers must fall back to the hunt group in case of CPS failure. Therefore these will route to **the code processing** in the global numbering plan configured above.

15. **Create a destination code** in the numbering plan of the customer (e.g. NP_Site1) for the queues' pilot numbers dialed in international format (e.g. 49505058032xx) with **Destination Type** "Code Processing" and **Code Processing Name** "CP_Fallback", **NoA**=International. Create a second destination code in the same way with **NoA**=unknown.





16. **Create a destination code** in the common numbering plan "NP_Common" for the queues (e.g. 49505058032xx) with nature of address "international", destination type "Destination" and destination name "CPSQueues".

17. **Create a destination code** in the common numbering plan "NP_Common" for the internal CPS resources (e.g. 49505058033xx) with nature of address "international", destination type "Destination" and destination name " CPSintResc ".

18. Create a **prefix access code** "+" in the common numbering plan "NP_Common" with nature of address "international", Min Length = "1", Max Length = "30", Prefix Type = "On-Network Access Code", Digit Position = "1". This enables CPS to reach all internal and external destinations. Hint: This prefix access code should be already created by CDC.

NOTE:
Edit the Feature Profile of your public network endpoint (default: “EPP_FPRVC_Site1”) and enable the service “Call Forward Invalid Destination”. Enter a pilot number which is named “invalid destination” in the DDI Lookup (datacenter).

4.4.5 Routing Configuration for SIP endpoint CPS in a multiple BG environment

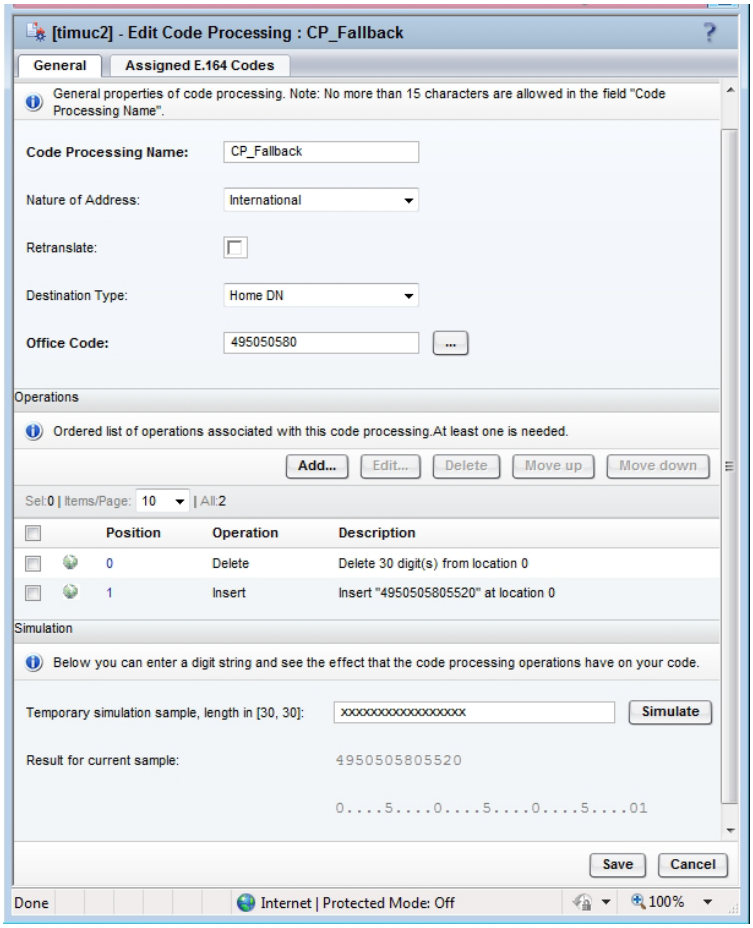
If you have multiple BGs and want to have just one Concierge instance, all calls must be route via the Global Translation and Routing.

For **fallback** – means if the CPS cannot be reached anymore – a **code processing** is required in the global numbering plan that deletes the pilot numbers to CPS and replaces these with the fallback hunt group pilot number.

NOTE:
The internal resources do not fall back to the hunt group!
(If CPS is down Concierge will not use internal resources anymore)

Global Translation and Routing

1. Create a **Code Processing "CP_Fallback"** with the following operations: **NoA**= international; **Destination type**= Home DN; **Office Code** of the used BG
2. **Delete** 30 digit(s) from location 0
3. **Insert** "<Number of Hunt Group>" (e.g. 4950505805520) at location 0

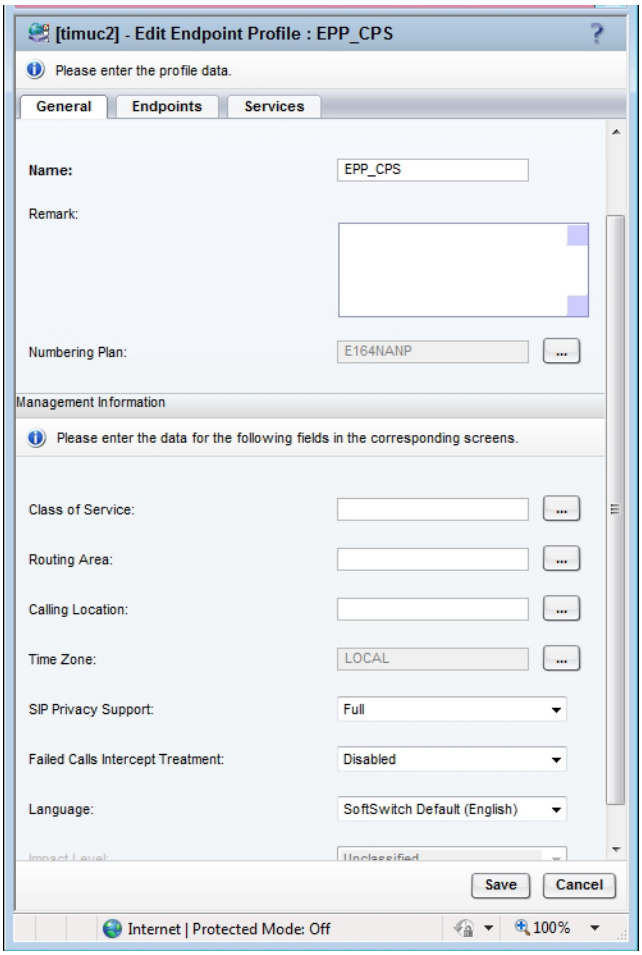


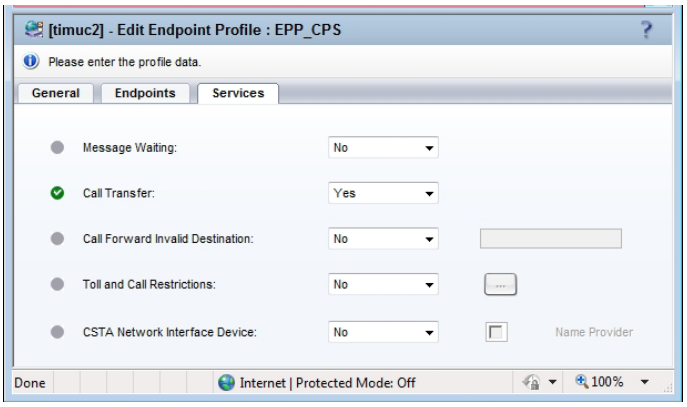
NOTE:
Pilot number dialed is deleted and replaced by the fallback hunt group number.

4. Create an **Endpoint Profile** "EPP_CPS" with **SIP privacy support** set to "full" and **Service** "Call Transfer" in the - **central numbering plan** (e.g. NP_Site1) of the BG.

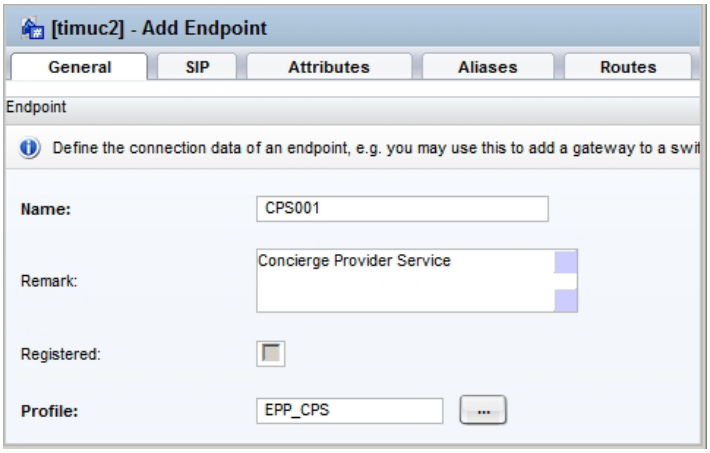
NOTE:
Up from OSCC-E V3R1 outgoing Invites have the SIP header “X-Siemens-CDR” included. This enables OSV to use different numbering plans for routing decisions depending on the initiating Concierge working place. The numbering plan associated with the Concierge working place will be used for outgoing calls - not the numbering plan of the CPS-endpoint anymore. The dialed number can be in the same format as if it was dialed directly from the Concierge‘s associated handset.

If OpenScape Voice receives a SIP INVITE or REFER request containing the X-Siemens-CDR header field with the charge parameter then charge number will be stored as the billing number in the CDR. In addition the number plan, rate area, and code/toll restriction services associated with this charge number will also be used to process the call.

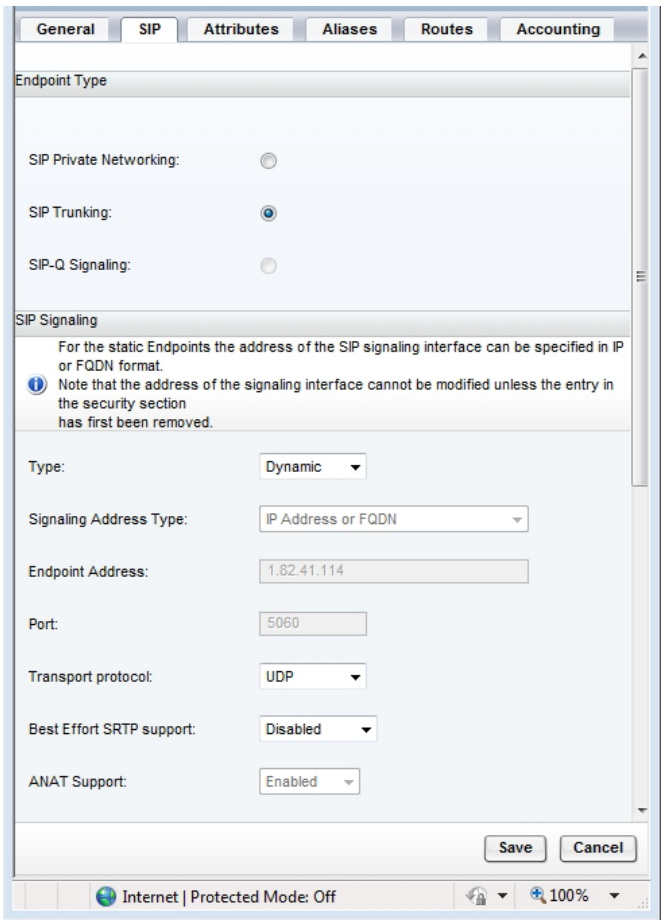




5. Create an Endpoint **named "CPS001" using this profile** in the Global Translation and Routing.

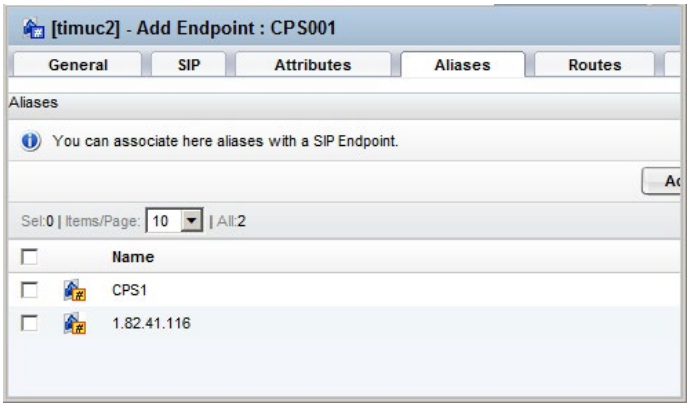


6. On tab SIP choose "**SIP Trunking**", **type**: "Dynamic", **transport protocol**: "UDP" and **best effort SRTP support**: "Disabled".
   Up from OSV V8: disable the ICE Support and set the Outgoing Call Supervision Timer to 32000ms.



7. On tab **Attributes** check "Supports SIP UPDATE Method for Display Updates", "UPDATE for Confirmed Dialogs Supported", "Accept Billing Number",, "Allow Sending of Insecure Referred-By Header", "Send International Numbers in Global Number Format (GNF)","Rerouting Forwarded Calls", "Enhanced Subscriber Rerouting" and "Enable Session Timer".
   To allow CPS to see a change of a connected call, the RTP parameter “Srx/Main/UpdateDisplaysForExternalCalls” must be set to **RtpTrue**.

8. On tab **Aliases** add the alias "**CPS1**" and the **IP address** of the CPS Server. (Add also the IP of the second CPS Server, if redundancy is used).

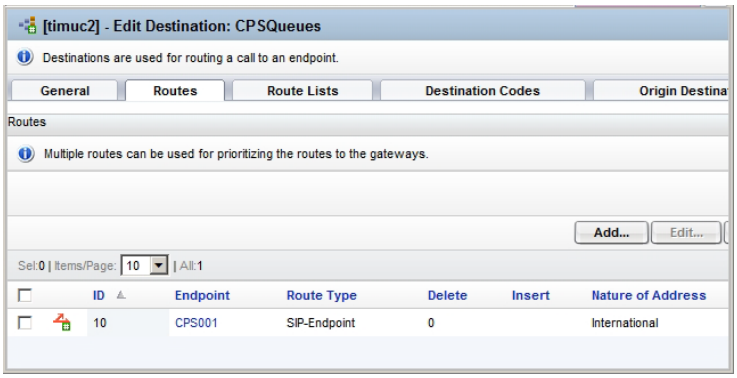


NOTE:
Add the IP Addresses to the Realms within "Administration – Signaling Management – Digest Authentication", if your security policy requires it.

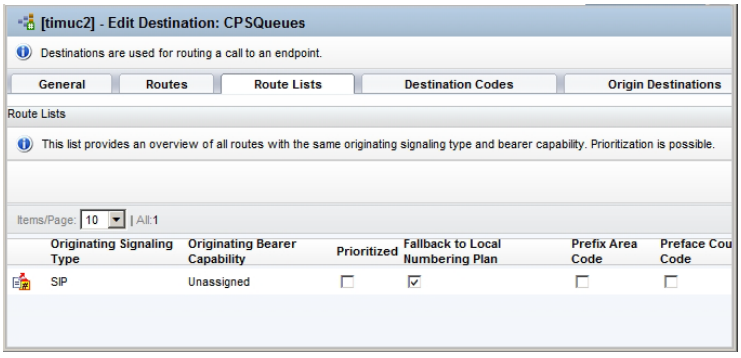
NOTE regarding Routing:
It is important to make sure that all phones (Concierge and Office) and Gateways are able to reach all numbers defined above.

9. Create the Destination "**CPSQueues**" for **Pilot numbers** and **personal lines**:

10. Add a route to endpoint "**CPS001**" using **Modification Type** “Number Manipulation” and **Nature of Address** “International”

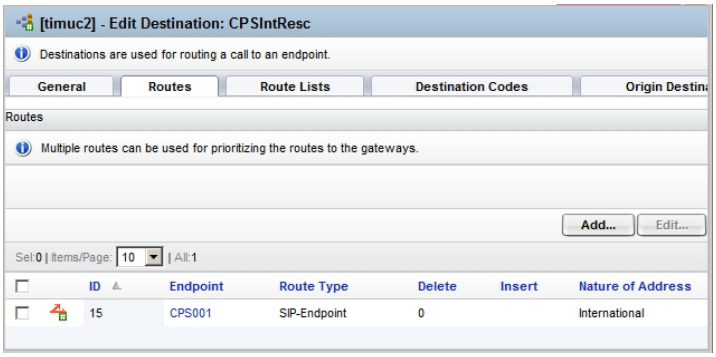


11. On tab Route Lists check "**Fallback to Local Numbering Plan**"

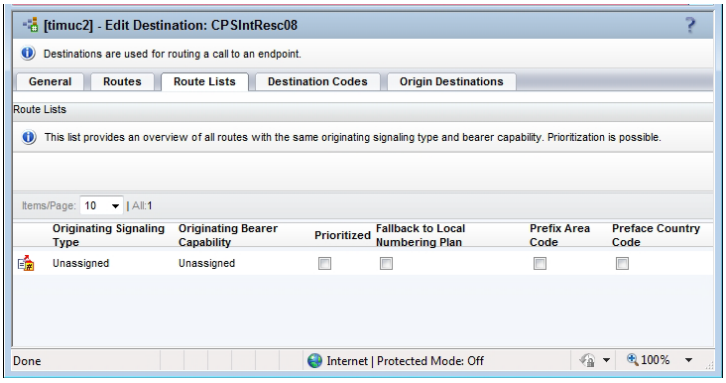


12. Create the Destination **"CPSintResc"**

13. Add the route to endpoint "**CPS001**" using **Modification Type “**Number Manipulation**”** and **Nature of Address “**International**”**



14. On tab Route Lists **DO NOT** check "Fallback to Local Numbering Plan"



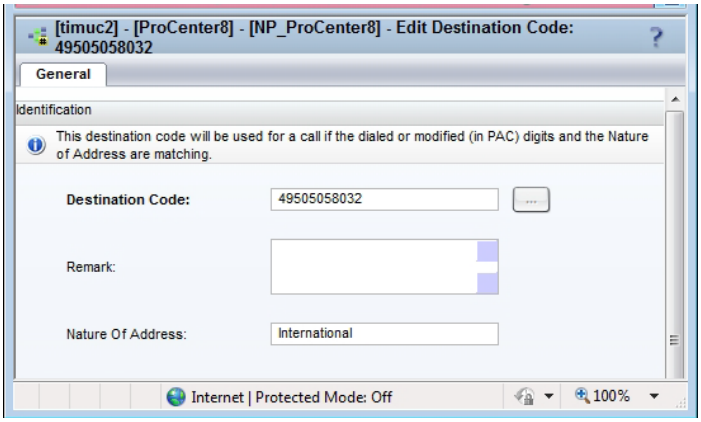
4.4.5.1 Codes in BGs numbering plan

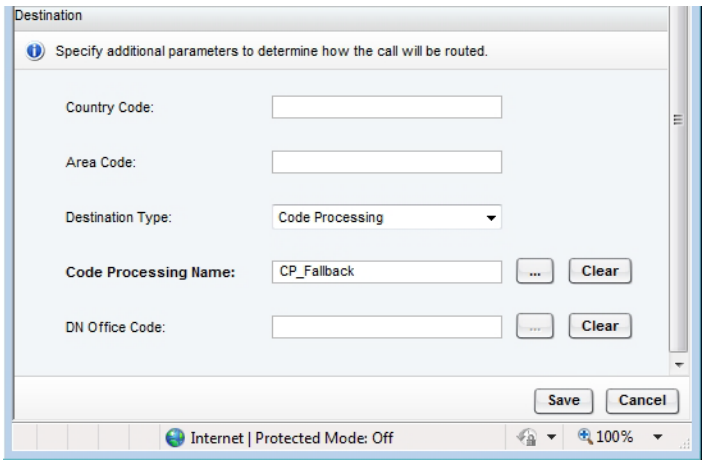
In the BG's numbering plan **destination codes** and **prefix access codes** have to be defined for the queues' pilot numbers as well as for the personal line numbers.

Pilot numbers and personal line numbers must fall back to the hunt group in case of CPS failure. Therefore these will route to **the code processing** in the global numbering plan configured above.

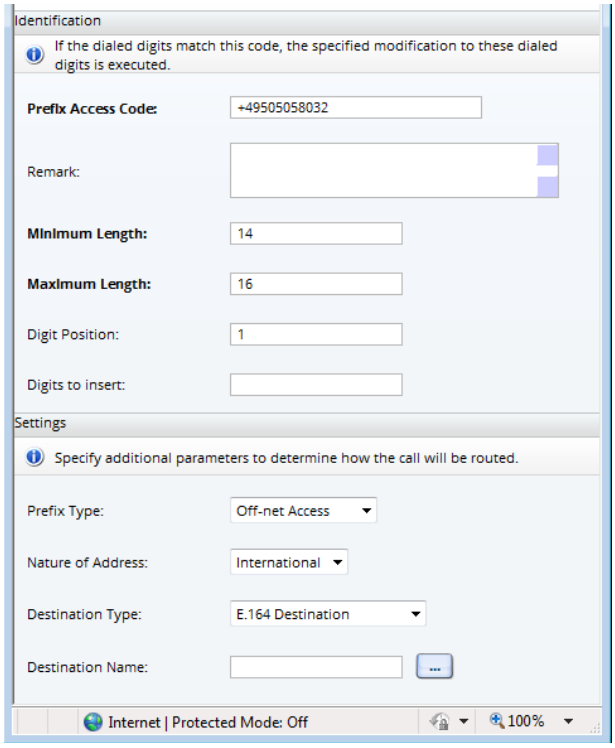
Business Group

1. **Create a destination code** for the queues' pilot numbers (e.g. 49505058032xx) with **Destination Type** "Code Processing" and **Code Processing Name** "CP_Fallback", **NoA**=International.

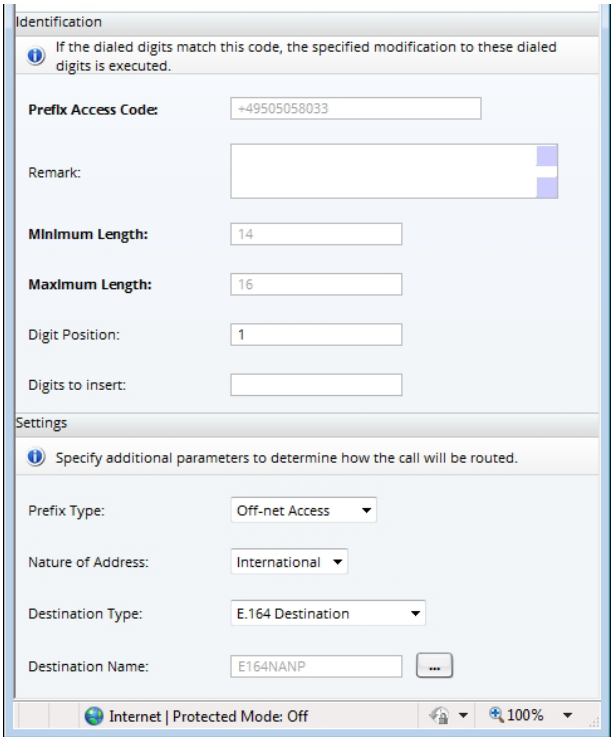




2. Create a **prefix access code for the queues** (e.g. **+**49505058032 or shorter, depending on your numbering plan) with **digit position "**1", **prefix type** "Off-net Access", **nature of address** "international" and **destination type** "E.164 Destination".



3. Create a **prefix access code for the internal CPS resources** (e.g. **+**49505058033 or shorter, depending on your numbering plan) with **digit position** "1"**, prefix type** "Off-net Access", **nature of address** "international" and **destination type** "E.164 Destination".

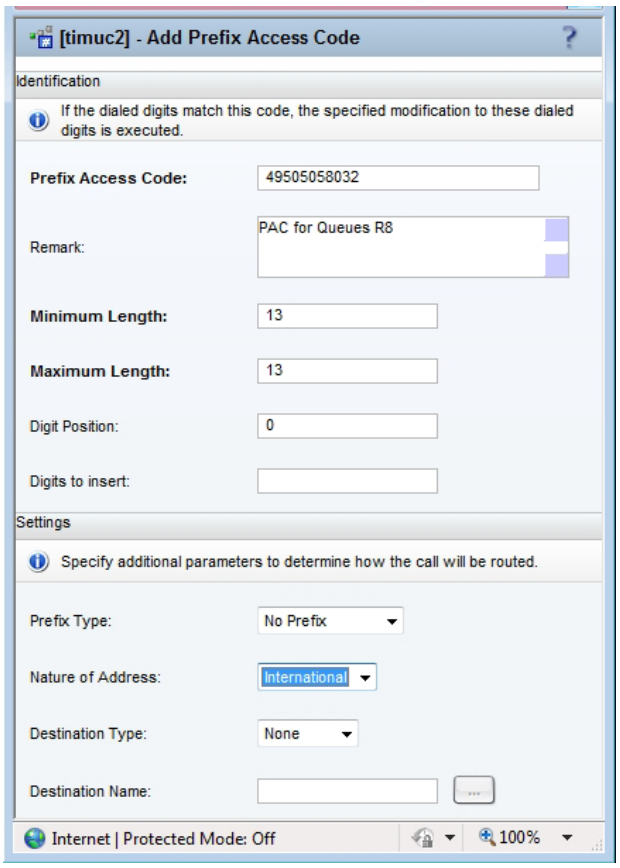


4.4.5.2 Codes in global numbering plan

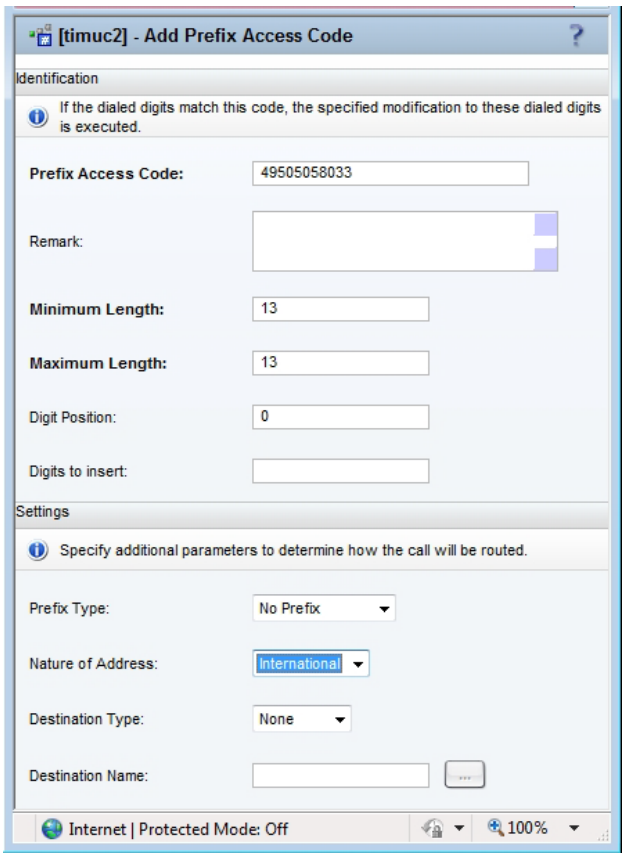
Prefix Access codes and E164 codes are configured in the global numbering plan for both, the internal resources as well as for the pilot numbers:

Global Translation and Routing

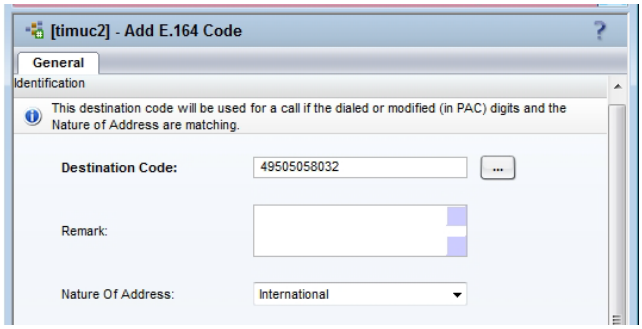
1. Create a **prefix access code for the queues** (e.g. 49505058032 or shorter, depending on your numbering plan) with prefix type "**No Prefix**", nature of address "**international**" and destination type "**none**".

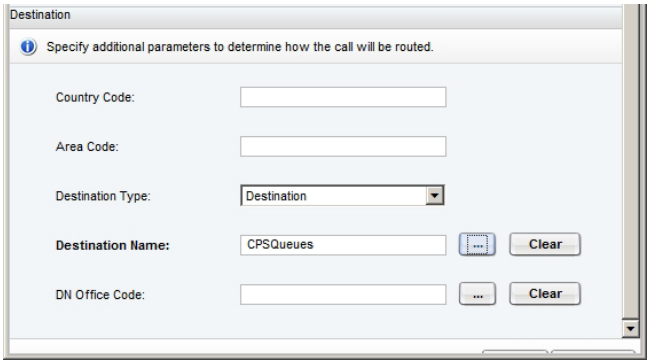


2. Create a **prefix access code** for the **internal CPS resources** (e.g. 49505058033 or shorter, depending on your numbering plan) with prefix type "**No Prefix**", nature of address "**international**" and destination type "**none**".

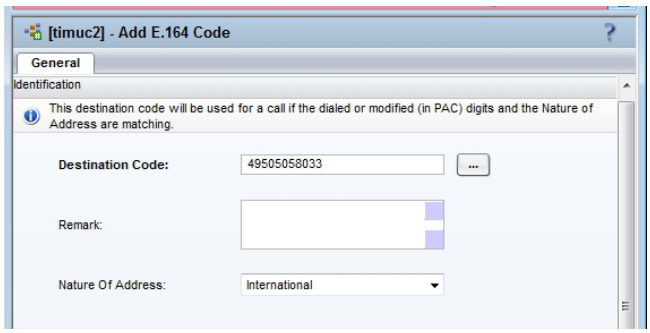


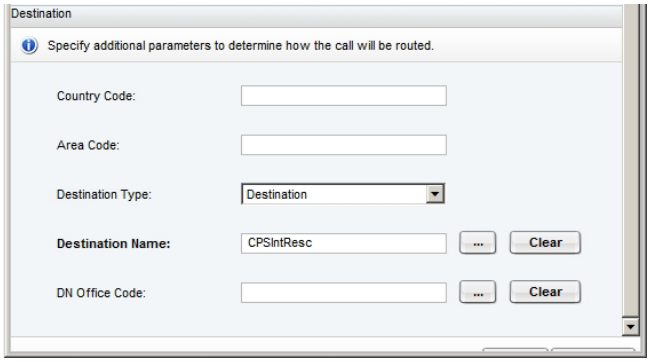
3. Create an **E164 Code for the queues** (e.g. 49505058032) with nature of address "**international**", destination type "**Destination**" and destination name "**CPSQueues**".





4. Create an **E164 Code** for the **internal CPS resources** (e.g. 49505058033) with nature of address "**international**", destination type "**Destination**" and destination name "**CPSintResc**".





NOTE:
Edit the Feature Profile of your public network endpoint (default: “EPP_FPRVC_Site1”) and enable the service “Call Forward Invalid Destination”. Enter a pilot number which is named “invalid destination” in the DDI Lookup (datacenter).

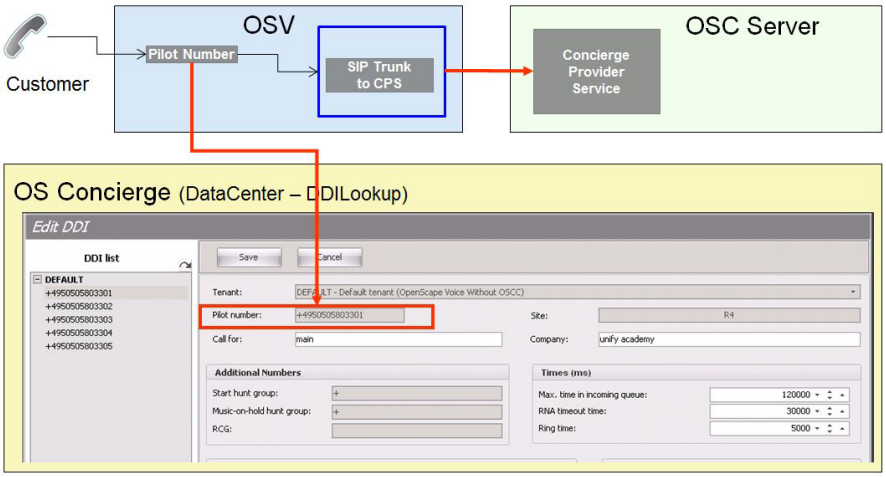
4.4.5.3 Enable routing of calls from CPS in global numbering plan

NOTE:
It is important to make sure that CPS is able to reach all phones (Concierge and Office) and it is able to make external calls (via Gateways).

Therefore in the global numbering plan it is necessary to create one or multiple destinations to external Gateways.

4.4.6 DDI Lookup entry example for OSV without OSCC

This example gives an overview of configuration of service numbers (pilot numbers) in OSV without OpenScape Contact Center:
Pilot numbers route the incoming calls to the SIP trunk of CPS. The CPS is then fully responsible for handling / distributing the call.



The picture displays the pilot number routings for Concierge in OSV without OpenScape Contact Center. The pilot number is one number out of the range of numbers that route to the CPS running on the OSC Server / Concierge Server and fall back to the fall back hunt group if CPS is down.

In case of a Concierge Server failure the **fallback hunting group** in OSV is responsible for call handling. This fall back configuration is used for service number calls and also for agent's Personal Line calls

This configuration is used for all kinds of service calls handled by Concierge; e.g. Main and Internal lines. Additional service numbers can be created.

NOTE:
For detailed information on Data Center configuration, see appropriate OSC Concierge, Administrator documentation

---

4.5 Routing configuration in OSV with OSCC

The configuration is nearly the same as “without OSCC integration”, the difference is that instead of a pool of pilot numbers and personal line numbers here only the personal line numbers are used.

4.5.1 Definition of numbers and number ranges

With OSCC the CPS connection uses two number ranges:

One for the **personal line numbers** of the attendants and one for internal CPS resources like Request pool and Callback Pool.

Furthermore if CPS fails, a fallback Hunt Group has to be defined in the OSV, where all attendant users are members. The fallback solution is used in case of CPS failure for the personal lines.

These calls coming in via the personal line numbers are routed to that fallback hunt group. The **internal resources** like callback numbers and request numbers will not be used in case CPS fails. Therefore no fallback for these is required.

NOTE:
In the scenario with OSCC all queues are handled by OSCC except the personal lines. They are queuing in CPS.

Define number ranges:

Parameter	Description	Value
CPS Resources for the example in the following sections		
Personal Lines Start	Numbers that route to CPS used for Personal Line Numbers of attendants	+4950505803200
Personal Lines End		+4950505803299
Loop Number	Used in Multi-CPS environment	+4950505803300
Request Numbers Start	Numbers that route to CPS used for internal tasks, like e.g. Park, Append	+4950505803301
Request Numbers End		+4950505803349
Callback Numbers Start	Numbers that route to CPS used for paging service (Park Slot Numbers)	+4950505803350
Callback Numbers End		+4950505803399
Fallback Hunt Group	Hunt Group for Calls to Pilot and Personal Line Numbers, if CPS fails	+4950505805520

NOTE:
The CPS Loop number is used in a Multi-CPS environment like e.g. when deploying a redundant Concierge Server System. In that case the CPS on the Standby server machine is frequently calling this number and expects a corresponding loop back message from the switch.
This message is only send if the CPS on the Main Server is active and running. If the call is not answered by a loop back message, the CPS on the Standby Server assumes that the CPS on the Main Server is not running and starts getting active by itself.

Please assure that the Loop number routes to the CPS endpoint in OSV.

4.5.2 Two fallback scenarios to be considered

OSCC is down: the normal fallback mechanism for OSCC is used, the hunt groups switch from manual to UCD.

Only the OSCC queues are affected – the personal lines are not.

CPS is down: the OSCC queues are not affected; the calls are still routed by OSCC.

Calls to personal lines cannot reach the CPS (CPS is not registered anymore) so these calls use the fallback mechanism to the fallback hunt group.

4.5.3 Settings in OSV

Please refer to the sections 4.4.3 Fallback Hunt Group, 4.4.4 Routing Configuration for SIP endpoint CPS in a single BG environment, 4.4.5 Routing Configuration for SIP endpoint CPS in a multiple BG environment.

All these settings are necessary additionally to the configuration described in the OSCC documentation.

NOTE:
The example configuration describes a configuration in the environment of the lab. In customer's environment other parameters are required, like e.g. different IP addresses, number ranges, prefix access codes, etc.
Only trained staff should configure the OpenScape Voice and adopt the configuration to the customer's environment.

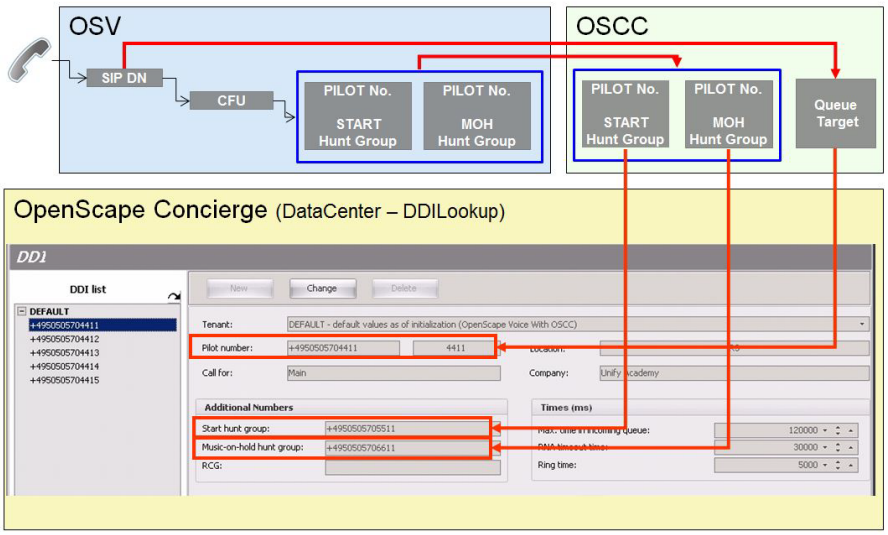
4.5.4 DDI Lookup entry example for OSV with OSCC

This example gives an overview of configuration of service numbers (pilot numbers) in OSV with OpenScape Contact Center:

When integrating with OpenScape Contact Center, a new Service number (DDI or Pilot Number) has to be configured in OpenScape Voice. For a correct handling through OSCC, it has to be configured ***in OSCC's Telephony Center*** together with the corresponding *Hunt Groups* (Initial HG and MoH HG) and finally set in the *DDI Lookup list* of Data Center.

The figures illustrate the settings in OSV with its corresponding settings in OSCC that are reflected in the DDI Lookup table fields for Concierge.

The first figure shows the configuration of a service number in OSV, OpenScape Contact Center's Telephony Center and Concierge DataCenter.



To enable OSCC to monitor the incoming call, three values are required:

1. the **Pilot number** that forwards the call
2. the **Start hunt group** (*Initial HG*) and
3. the **Music-on-hold hunt group** *(MoH HG)*

All of them have to be configured in the DDI Lookup in Concierge Data Center and the *Pilot number* is configured as *Queue Target* in OSCC Telephony Center.

Principally there is only one type of service number configuration for Concierge. It depends on customer's requirements, which types of service numbers are required, e.g. "Internal Intercept" or "Reception".

NOTE:
For detailed information on Data Center configuration, see appropriate OSC Concierge, Administrator documentation

4.5.5 Concierge user devices

All Concierge user devices must be member in the Fallback hunt group!

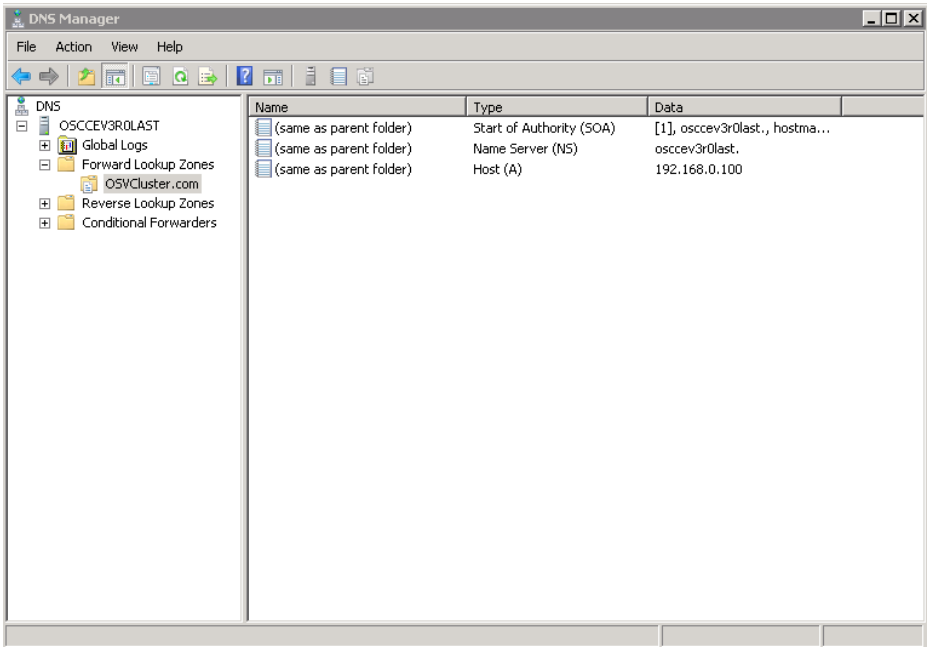
This HG is only used for the ***personal lines of each Concierge*** working places – it has nothing to do with the OpenScape Contact Center fallback mechanisms for the normal service numbers / queues.

The personal lines are queuing in CPS.

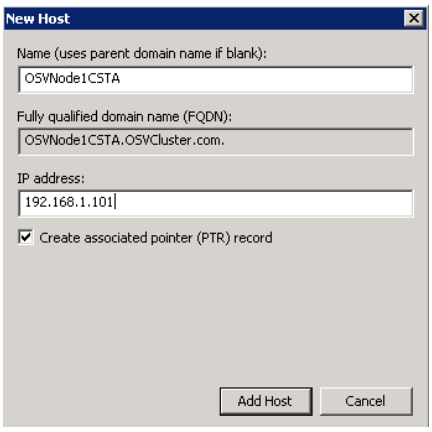
4.6 Configuration Microsoft DNS for geo-separated OSV deployment

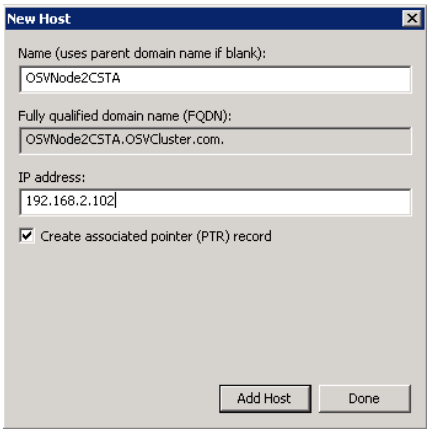
4.6.1 DNS-SRV Configuration for CSTA

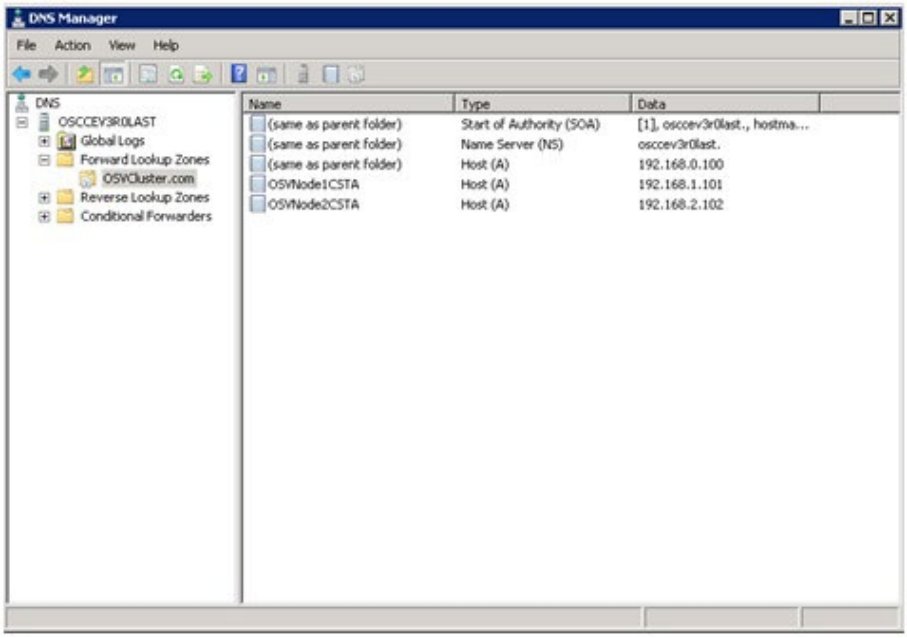
Start the DNS Management console via **Start -> Administrative Tool -> DNS** and create a new **Forward Lookup Zone** e.g. ***OSVCluster.com***.



Make a new Host entry for the DNS IP-Address and two new Host entries for the CSTA of both OSV Nodes with right click on Zone OSVCluster.com then select **New Host (A).**



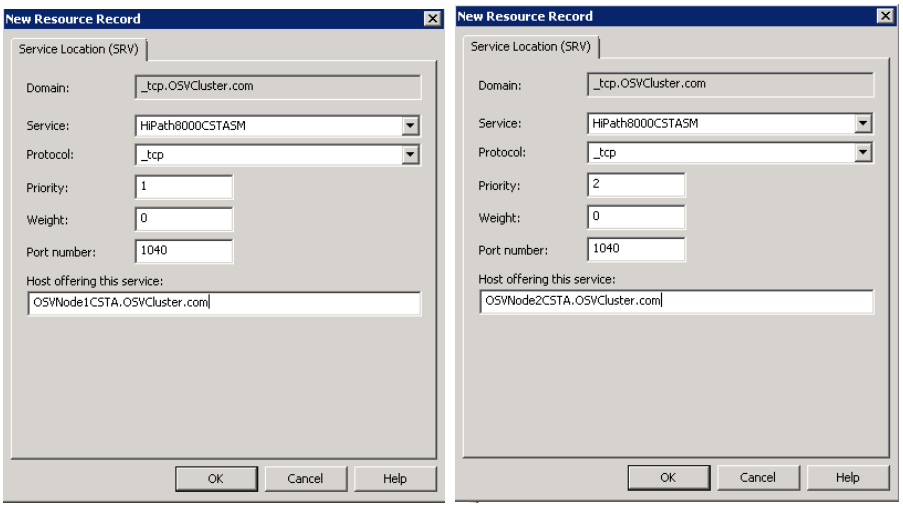


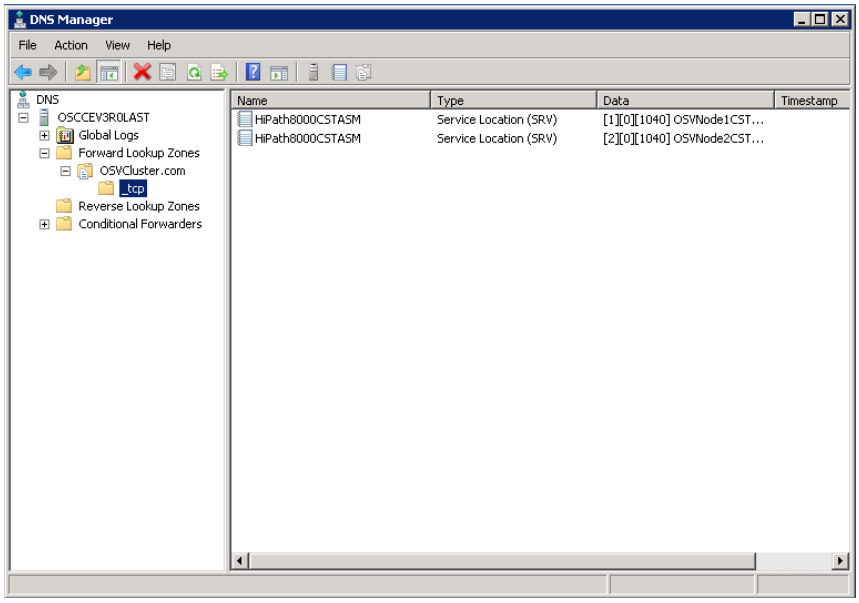


Create a new DNS Domain Name entry for the Zone with right click on Zone **OSVCluster.com** then select **New Domain**. The Name must be _tcp!

Create two new SRV Resource Records for both OSV Nodes with right click on Zone **OSVCluster.com** then select **Other New Records**. Select **Service Location (SRV)** in the List box of the **Resource Record Type** Window.

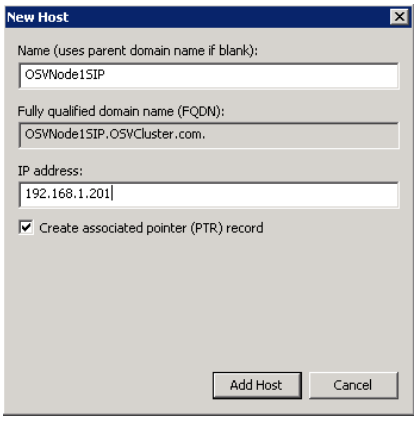
NOTE:
It's important to use different priorities for the OSV Nodes.



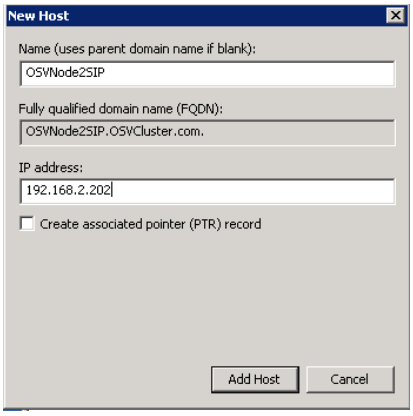


4.6.2 DNS-SRV Configuration for SIP

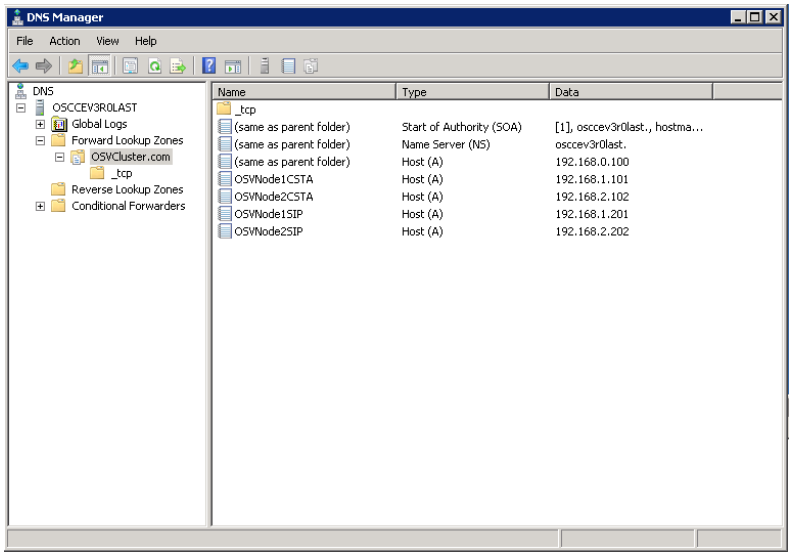
Make two new Host entries for the SIP interfaces of both OSV Nodes with right click on Zone OSVCluster.com then select **New Host (A).**



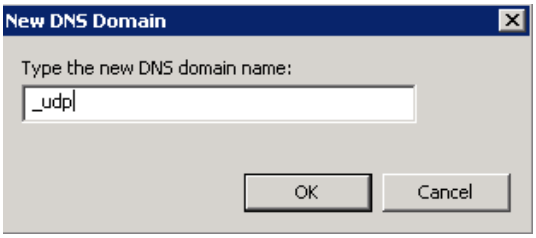
1



2

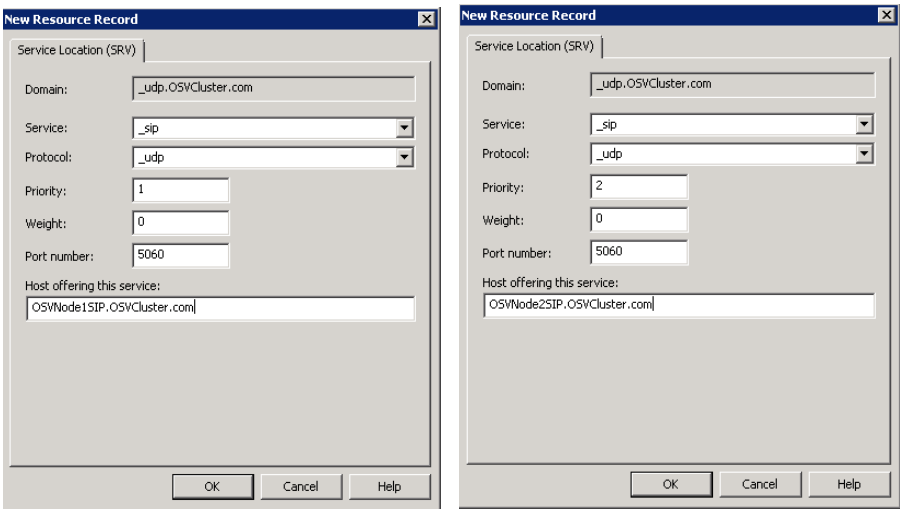


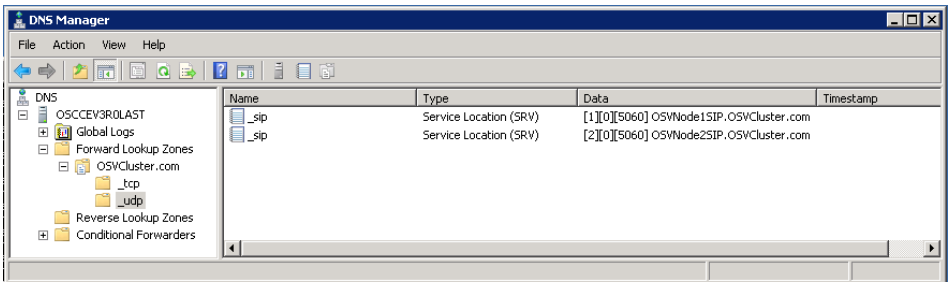
Create a new DNS Domain Name entry for the Zone with right click on Zone **OSVCluster.com** then select **New Domain**. The Name must be _udp!



Create two new SRV Resource Records for both OSV Nodes with right click on Zone **OSVCluster.com** then select **Other New Records**. Select **Service Location (SRV)** in the List box of the **Resource Record Type** Window. The Service must be named "_sip"

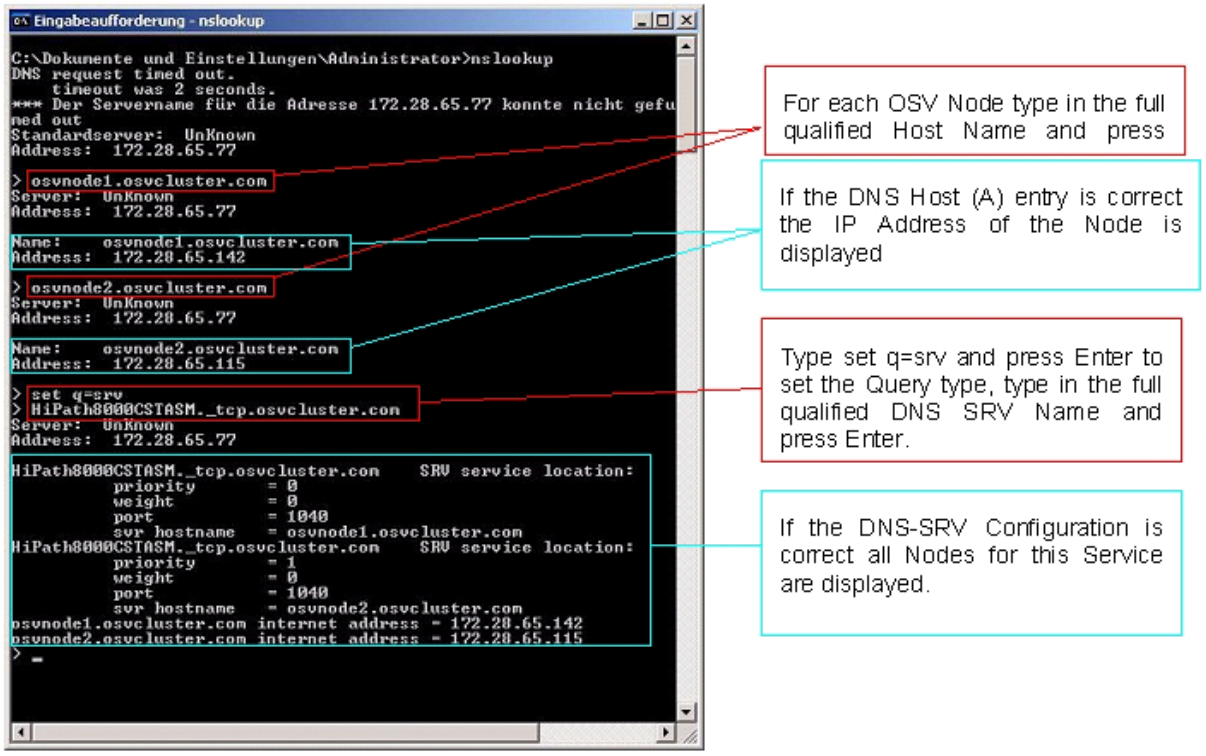
NOTE:
It's important to use different priorities for the OSV Nodes.





4.6.3 Checking the DNS-SRV configuration on Integration Server

1. Open a Command Prompt window via **Start > Run** and **cmd**. Please enter ***nslookup*** and press ENTER.



2. Do the check for Service "HiPath8000CSTASM" (example above) and "_sip".

5 Switch configuration OpenScape 4000

IMPORTANT:
The configuration examples in this section describe a configuration in the environment of the lab. In customer's environment other parameters are required, like e.g. IP addresses, number ranges, prefix access codes, etc.

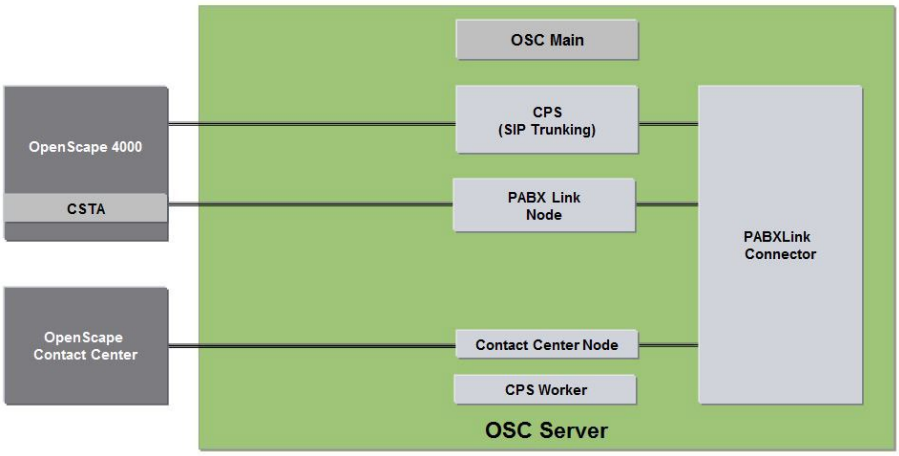
Only trained staff should configure the OpenScape 4000 and adopt the configuration to the customer's environment.

In this section the OpenScape 4000 settings required for integrating OpenScape Concierge are described for scenarios without and with OpenScape Contact Center.

The settings in OpenScape 4000 and OSCC are described from the perspective of OpenScape Concierge.

The **OSC server** is installed in parallel to the existing infrastructure and **has its own CSTA application link to the OS 4000**; the CSTA link that is established by the **PABX Link Node.**

5.1 General information



As visible the Concierge System has two connections to the OpenScape 4000: the CSTA link that is established by the **PABX Link Node** and the CPS that is connected as a SIP Endpoint in OpenScape 4000 and requires a SIP trunking configuration.

5.1.1 OpenScape 4000 CSTA link connection

The CSTA link connection requires a CSTA application using a CSTA Adaptor in OpenScape 4000; perform the following steps in the OpenScape 4000 Assistant:

1. Check if an existing OSC Adaptor allows creating an additional CSTA application.
2. Add a new Connectivity Adaptor, if no existing Adaptor can be used; Select the new Connectivity Adaptor and modify PBX Link Number and Subapplication Number for the new connection.

3. Create a new CSTA application corresponding to the parameters set for the PABX Link Node in System Management.
4. Restart the Connectivity Adaptor.
5. Check the Status of the new CSTA Adaptor.

5.1.2 Configuration for restricted numbers

NOTE:
If the presentation of users is restricted please proceed as follows

Run the **AMO SBCSU** to configure the presentation indicator. The presentation indicator is normally configured as unrestricted (**SSTNO=NO**).

However, if the Calling Line Identification Restriction (CLIR) setting on the user's extension is configured as "presentation restricted", you must configure the presentation indicator as restricted (**SSTNO=YES**).

In this case, you must **add a parameter to each instance of the CA4000.cfg** file where PABXLinkConnector is connected to.

NOTE:
This also needs to be done if the ZAND/ACD parameter SUPAGTNU(UNAGTNU) is set to **yes**.

Set the restricted value to **ignore**.

• PRESENTATION_RESTRICTED=ignore

5.1.3 OpenScape 4000 connection without OSCC

The incoming calls to the *pilot numbers* all route to the Concierge Provider Service (CPS) that is connected via SIP trunking.

The calls are queuing in CPS and stay there until further actions are required; the calls for the *personal line* of an attendant also queue in CPS.

CPS assigns the call to the attendant or the attendant picks the call.

In case the *CPS breaks down* calls are handled by fallback routing in OpenScape 4000 that is initiated through LCR, means if the CPS cannot be reached the call can route to a hunt group for example.

5.1.4 OpenScape 4000 connection with OSCC integration

With OpenScape Contact Center (OSCC) the incoming calls for the attendants are routed by OSCC – also the backup routing case is handled by OSCC strategies.

Incoming calls to the personal lines of the attendants are handled as described in the scenario without OSCC. These calls are queuing in CPS and CPS assigns the call to the attendant or the attendant picks the call from the personal queue.

In the following sections the configuration of devices is described as well as the configuration of the SIP trunk and the fallback LCR-Routing mentioned above.

5.2 Concierge Provider Service (CPS)

5.2.1 Features and functionalities

CPS

CPS is the central instance for controlling the calls that are handled by the Concierge user.

Processing Queue

Calls that are parked or on hold, calls that need to be transferred or require the paging functionality to be connected with the target person, all these calls are transmitted to the CPS and wait there for further handling. That is why this position is called the **processing queue**.

As the CPS is an internal resource of the OSC Server, Concierge is fully controlling what happens with a call and displays this information on the upper right pane to the Concierge user.

In case of a standalone installation, where no OpenScape Contact Center is in use, the CPS also queues the calls that come in via the pilot numbers and allows a simple call push (ACD) to the attendants which are assigned to the pilot number.

Transferring calls is controlled by CPS in a way that calls that are meant to be transferred to a target extension are “parked” on CPS on one channel where another channel of CPS tries to reach the target device.

The connection between both only happens if the target person answers the call. Otherwise the call stays connected to CPS. The call can be controlled and handled by Concierge user (even if the Concierge user is in a call with another customer).

During the transfer process the call is visible in Concierge.

CPS acts as a media server for Concierge calls. Data Center allows to specifying different types of music / wave files that can be assigned in multiple handling scenarios, for example a personal greeting wave file can be assigned for every Concierge user that is played to the caller as well as to the attendant right before the call is connected.

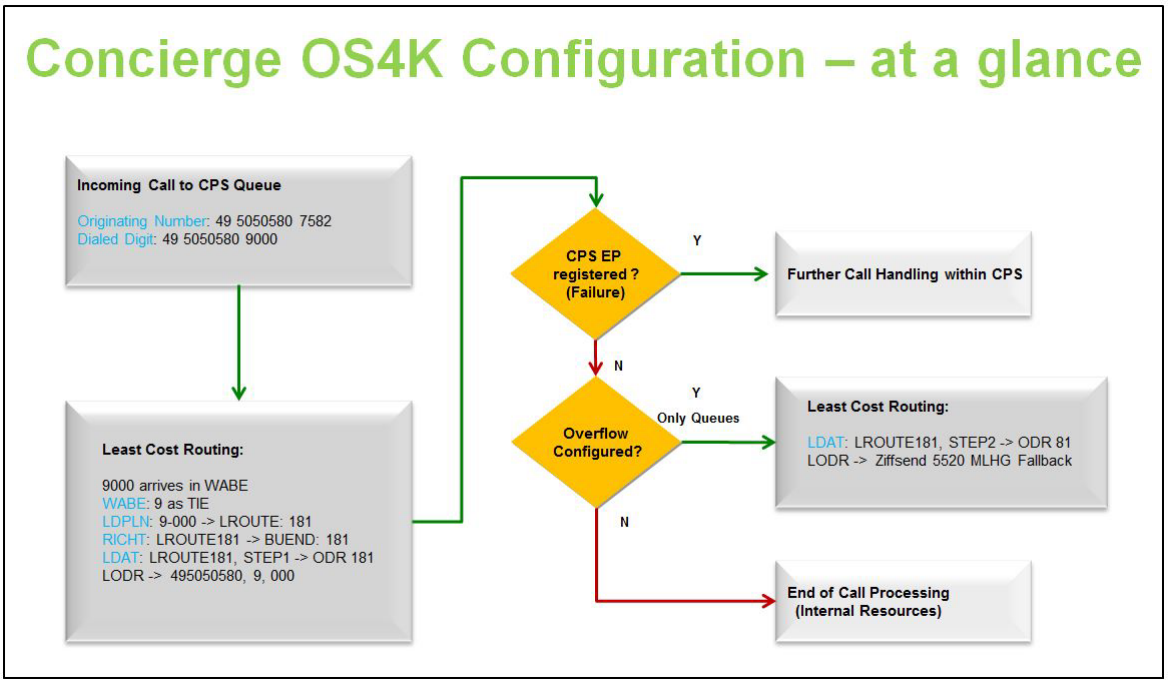
The functionality described requires the *CPS to be connected via SIP trunking to the communication platform*. All numbers using this trunk have to be in E164 format.

5.2.2 CPS Integration / Backup Routing

For a proper handling in case CPS fails or the SIP trunk connection is down a fallback routing is required. The calls which cannot reach CPS will fall back to hunt group routing in OpenScape 4000, all Concierge users must be members in that hunt group.

Overview: Routing and fallback of pilot numbers and personal calls

Incoming calls are routed to the SIP trunk for CPS. In case CPS is down, the call is re-routed to a hunt group by the LCR Routing.



In case of a failure the calls will not be handled by CPS, the OpenScape 4000 will route the calls by an overflow configuration in the AMO LDAT of the direction to the CPS. Here the calls will be routed by an internal rerouting over the AMO LODR to a destination that should be a MLHG

The fallback routing is only activated for incoming calls (pilot numbers and personal line numbers). For the *internal CPS resources* the fallback routing will not take place.

5.3 Concierge user device configuration

NOTE:
Concierge does not support UFIP extensions. Some features (i.e. pickup) will not work properly when using UFIP extensions as a Concierge extension.

5.3.1 Concierge device

Example Configuration

ADD-SBCSU:STNO=<STNO>,OPT=OPTI,CONN=DIR,PEN=1-1-1-0,DVCFIG=OPTIP500,TSI=1,COS1=33,COS2=33,LCOSV1=9,LCOSV2=1,LCOSD1=9,LCOSD2=1,DPLN=0,ITR=0,SSTNO=N,COSX=0,SPDI=0,IDCR=N,REP=2,STD=57,SECR=N,INS=Y,ALARMNO=0,RCBKB=N,RCBKNA=N,DSSTNA=N,DSSTNB=Y,DIGNODIS=N,CBKBMAX=5,HEADSET=N,HSKEY=NORMAL,CBKNAMB=Y,TEXTSEL=GERMAN,HMUSIC=0,CALLOG=ALL,COMGRP=0,DNIDSP=Y;

5.3.2 Concierge phone settings in OS4000 for CPS fallback

Concierge extensions are members of the Fallback Hunt Group
(in the example below the Number **5520** is used for that Hunt Group)

5.4 Routing configuration in OpenScape 4000 without OSCC

5.4.1 CPS number ranges

As described above the CPS is Concierge's central service for handling calls. Without OSCC the calls to the pilot numbers are directly routed to CPS and queue there for being distributed.

The connection to CPS needs two types of number ranges:

- one for *pilot numbers and personal line numbers* of attendants (Queues)
- one for *CPS internal resources* like Request pool and Callback Pool

Furthermore if CPS fails, a Fallback Hunt Group has to be defined in the OpenScape 4000, where all attendant users are members.

In the following description a basic fallback configuration is displayed where all types of incoming calls route to the same hunt group in case of failure.

The fallback solution is used in case of CPS failure for the personal lines and service number (queues). These calls coming in via pilot numbers and personal line numbers are routed to the fallback hunt group.

The *internal resources* like callback numbers and request numbers are not in use when CPS fails. Therefore no fallback solution for those is required.

Definition of number ranges for example configuration used in this book:

Parameter	Description	Value
CPS Resources for the example in the following sections		
Pilot Numbers Start	Numbers that route to CPS used for Pilot Numbers (DDI Lookup table)	+495050580-9000
Pilot Numbers End		+495050580-9009
Personal Lines Start	Numbers that route to CPS used for Personal Line Numbers of Attendants	+495050580-9200
Personal Lines End		+495050580-9209
Loop Number	Used in Multi-CPS environment	+495050580-9300
Request Numbers Start	Numbers that route to CPS used for internal tasks, like e.g. Park, Append, etc.	+495050580-9301
Request Numbers End		+495050580-9349
Callback Numbers Start	Numbers that route to CPS used for paging service (Park Slot Numbers)	+495050580-9350
Callback Numbers End		+495050580-9399
Fallback Hunt Group	Hunt Group for Calls to Pilot and Personal Line Numbers, if CPS fails	+495050580-5520

NOTE:
The CPS Loop number is used in a Multi-CPS environment like e.g. when deploying a redundant Concierge Server System. In that case the CPS on the Standby server machine is frequently calling this number and expects a corresponding loop back message from the switch.
This message is only send if the CPS on the Main Server is active and running. If the call is not answered by a loop back message, the CPS on the Standby Server assumes that the CPS on the Main Server is not running and starts getting active by itself.

Please assure that the Loop number routes to the CPS endpoint in OSV.

5.4.1.1 Formula for estimating the number range of internal CPS resources

Use this formula to calculate the range of the internal resources:

Range of request numbers: 8 plus number of agents

NOTE:
During the transfer from the client to the processing queue a request no. is used. When the call reaches the CPS (arrived in the processing queue) the request no. is usable (free) again.

The request range does not limit the count of calls in the processing queue.

Range of callback numbers: 3 plus the maximum number of calls that shall be parked for the paging functionality

5.4.2 Fallback Hunt Group

1. Add a Number in the WABE as type “Hunt”. Configure a Hunt Group and add all Concierge extensions.

Example Configuration

ADD-WABE:CD=5520,DAR=HUNT;

*ADD-SA:TYPE=VCE,CD=**5520**,STNO=<STNO>,STYPE=CYC,NAME="**FALLBACK**";*

5.4.3 Configuration of the SIP Endpoint for CPS

2. Add a STMI Board to the Switch.

Example Configuration

ADD-BFDAT:FCTBLK=3,FUNCTION=HG3550,BRDBCHL=BCHL60&BCHL120;

CHANGE-BFDAT:CONFIG=CONT,FCTBLK=3,FUNCTION=HG3550,LINECNT=2,UNITS=3;

CHANGE-BFDAT:CONFIG=OK,FCTBLK=3,ANSW=YES;

ADD-BCSU:MTYPE=IPGW,LTG=1,LTU=1,SLOT=5,PARTNO="Q2324-X500",FCTID=1,FCTBLK=3,BCHL3550=60;

3. Configure the IP Address (1.82.11.80) and Default Gateway (1.82.11.254) of the Board

Example Configuration

*ADD-CGWB:LTU=1,SLOT=5,SMODE=NORMAL,IPADR=**1.82.11.80**,NETMASK=255.255.255.0,DEFRT=**1.82.11.254**,TRPRSIP=60;*

4. Configure the registration of CPS SIP-Endpoint (1.82.11.114). Because of the special SIP Trunk-Profile in the WBM a registration as **internal and external** Gateway must be configured.

Example Configuration

CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=5,TYPE=LEGKDATA,GWNO=281,GWDIRNO=281,REGEXTGK=NO;

*ADD-GKREG:GWNO=181,GWATTR=EXTGW&REGGW&HG3550V2&SIP,GWIPADDR=**1.82.11.114**,GWDIRNO=9,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="CPS SIP",SECLEVEL=TRADITIO;*

ADD-GKREG:GWNO=281,GWATTR=INTGW&HG3550V2&SIP,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="CPS SIP";

RES-BSSU:PEN,,1,5;

NOTE:
In case of the special Registration of the CPS, a Trunk Profile must be used in the WBM and a GKREG configuration for external Gateway must be done, target address is the primary server. The Gateway Directory Number (GWDIRNO) in the AMO CGWB (LEGKDATA) and GKREG (EXTGW) is free of use, but both numbers must be different.

---

5. Configure the trunk and B-Channels (here 30)

Example Configuration

ADD-BUEND:TGRP=181,NAME="CPS",NO=60;

ADDCOT:COTNO=181,PAR=PRI&RCL&ANS&KNOR&CEBC&CBBN&CBFN&BSHT&BLOC&LWNC&ATRS&ROPT&NLCR&TSCS&TRSC&DFNN&NLRD&NITO&BCNE&NOFT&NTON;

CHANGE-COT:COTNO=181,COTTYPE=COTADD,DEV=S2CONN,INFO="181: CPS";

ADD-COP:31,,TA,TA;

CHANGE-COP:31,COPADD,,,,S2CONN,"31: S0/2 QUER LOKN";

ADD-COSSU:,2,,,,,,,,"";

CHA-COSSU:COS,2,TA&TNOTCR&TTT;

CHA-COSSU:COS,2,,TA&TNOTCR&TTT;

CHA-COSSU:COS,2,,,TA&TNOTCR&TTT;

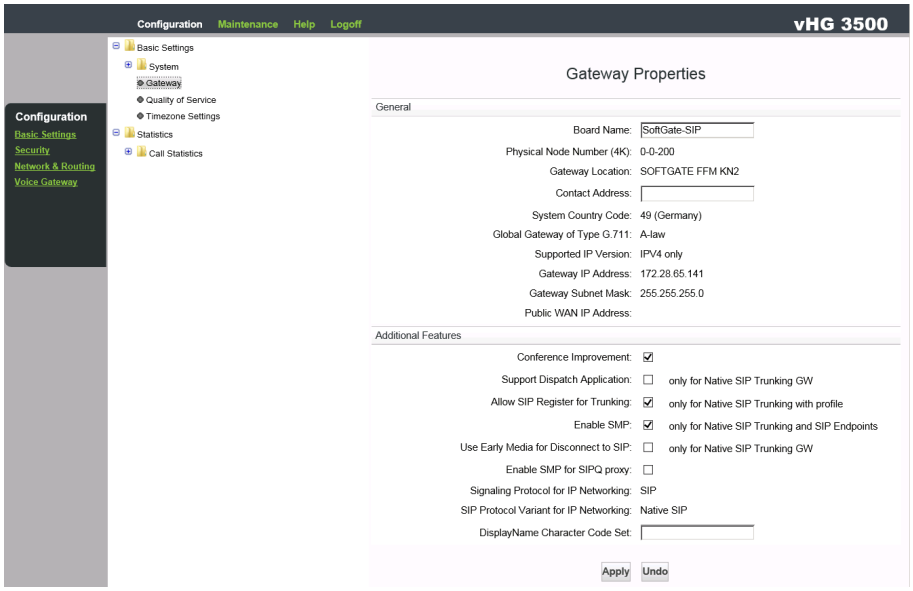
ADD-TDCSU:OPT=NEW,PEN=<Board

Location>,COTNO=181,COPNO=31,DPLN=0,ITR=0,COS=2,LCOSV=9,LCOSD=9,CCT="CPS",DESTNO=0,PROTVAR=ECMAV2,SEGMENT=8,NNO=1-1-181,FWDX=10,CLASSMRK=EC&G711&G729AOPT,TGRP=181,DEV=HG3550IP,BCHAN=1&&30,BCNEG=N,BCGR=1;

5.4.4 Configuration of the WebBasedManagement (WBM)

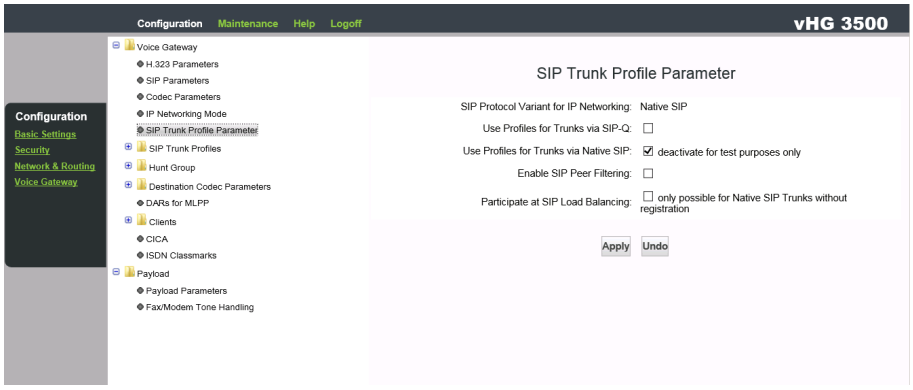
1. Connect the Board to the LAN and open the WBM

Under Basics Settings \ Gateway



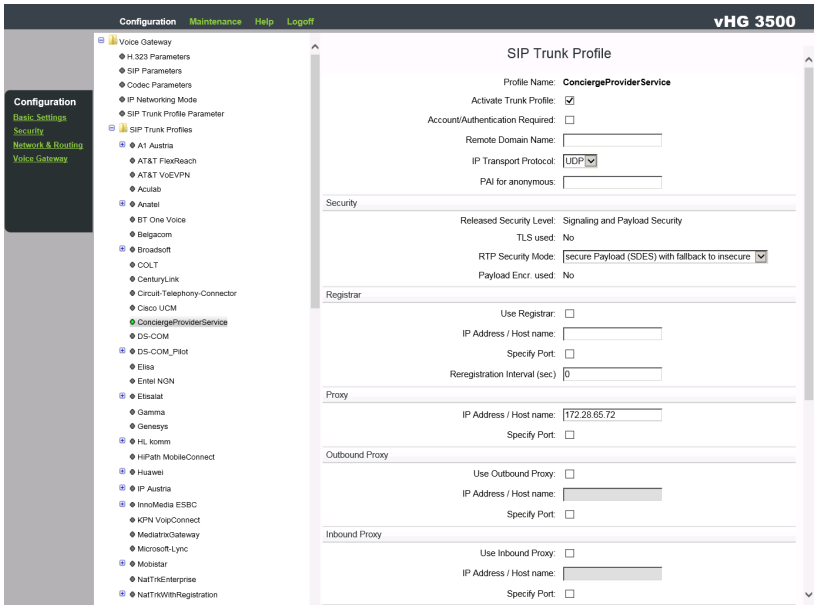
2. Set the following parameter:
   - Support Dispatch Applications: No
   - Allow SIP Register for Trunking: Yes
   - Use Early Media for Disconnect to SIP: No

Under Voice Gateway \ SIP-Trunk Profile Parameter



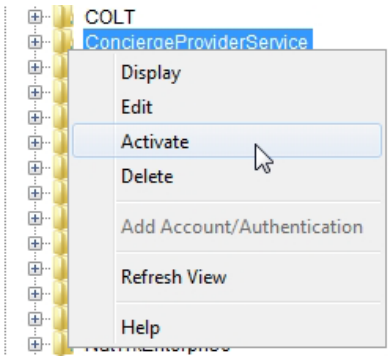
3. Set Use Profiles for Trunks via Native SIP: Yes

Under Voice Gateway \ SIP-Trunk-Profile

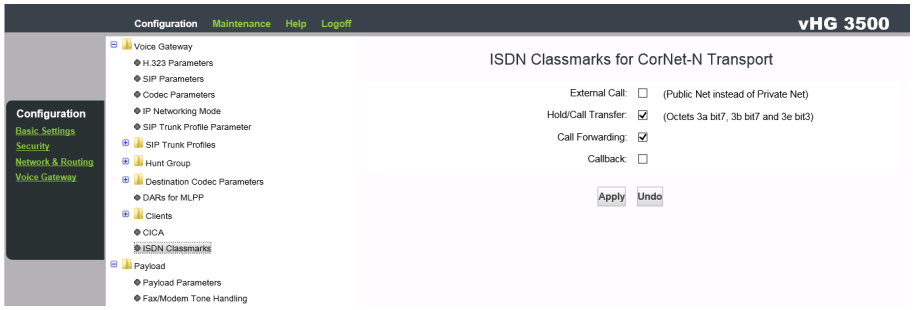


4. Select the *ConciergeProviderService* profile.
5. Set the following parameter:
   - SIP Transport Protocol: UDP
     Under Proxy:
   - IP Address / Host Name: <CPS Server IP-Address>
     Under Inbound Proxy:
   - Use Inbound Proxy: No, only with Standby Configuration
   - IP Address/Host Name: <Standby CPS Server IP-Address>

6. Activate the profile subsequently!



Under Voice Gateway \ ISDN Classmarks



7. Set the following parameter:
   - External Call: No
   - Hold/Call Transfer: Yes
   - Call Forwarding: Yes

8. Save the configuration and restart the HG.

NOTE:
IF the **diagnosis** is activated for the STMI and special diagnosis settings are configured, it can happen that the Concierge / CPS reacts very slowly when calls are transferred..

5.4.5 Configuration of the CPS number ranges

1. Configure the LCR

NOTE:
The example configuration describes a configuration in the environment of the lab. In customer's environment other parameters are required, like e.g. different IP addresses, number ranges, prefix access codes, etc. **Only trained staff should configure and adopt the configuration to the customer's environment.**

Example Configuration

ADD-WABE:CD=9,DAR=TIE,CHECK=N;

ADD-LODR:ODR=181,CMD=OUTPULSE,DGTS=495050580;

ADD-LODR:ODR=181,CMD=ECHO,FIELD=1;

ADD-LODR:ODR=181,CMD=ECHO,FIELD=2;

ADD-LODR:ODR=181,CMD=NPI,NPI=ISDN,TON=INTERNAT;

ADD-LODR:ODR=181,CMD=END;

ADD-LODR:ODR=181,INFO="CPS";

ADD-RICHT:MODE=LRTENEW,LRTE=181,LSVC=ALL,NAME="CPS",TGRP=181,DNNO=1-1-181,ROUTOPT=YES,DTMFCNV=SUFDIAL,DTMFDISP=DIGITS,DTMFTEXT="MFV-WAHL",INFO="CPS";

ADD-LDAT:LROUTE=181,LSVC=ALL,LVAL=1,TGRP=181,ODR=181,LAUTH=1,CARRIER=1,ZONE=EMPTY,GW1=181-0;

NOTE:
All Numbers from and to CPS must be sent in Type International.

2. Configure the Fallback Routing

Example Configuration

ADD-LODR:ODR=81,CMD=OUTPULSE,DGTS=5520;

ADD-LODR:ODR=81,CMD=END;

ADD-LDAT:LROUTE=181,LSVC=ALL,LVAL=2,ODR=81,LAUTH=1,CARRIER=1,ZONE=EMPTY,LATTR=RERTEINT;

3. Configure Pilot Numbers

Example Configuration

Main '0' as -9000 in DDI Lookup

ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=9-000,LROUTE=181,LAUTH=1,PINDP=N;

ADD-WABE:CD=0,CPS=6,DAR=ATNDDID,CHECK=N;

ADD-NAVAR:NOPTNO=1,TYPE=CASEXT,CD=9000;

ADD-VFGR:ATNDGR=0,QUEMODE=DQ,NOPT1=1,OPT=1,CQMAX=5,AUTNS=OFF,SDIST=NO,CASMCF=YES,ANSYN=NO,WC=5,COD=OFF,INIGHTPR=NO;

ADD-VFGKZ:TYPE=ATNDGR,CD=0,CPS=6,ATNDGR=0;

ADD-ACTDA:TYPE=ATNDGR,ATNDGR=0,NOPT=1,ACT=ACT;

Internal '-9001' in DDI Lookup

ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=9-001,DPLN=5,LROUTE=181,LAUTH=1,PINDP=N;

NOTE:
If Intercept is needed, the parameter for corresponding intercept reason needs to be added in the COT of the trunks(see "Feature Usage Example Documentation of OpenScape 4000). All calls will be intercepted to the linked VF-Group. **All calls which are forwarded (redirection party included) to a DDI Lookup are shown in Concierge as Intercept calls.**

Intercept '-9009' in DDI Lookup

ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=9-009,LROUTE=181,LAUTH=1,PINDP=N;

ADD-NAVAR:NOPTNO=2,TYPE=CASEXT,CD=9009;

ADD-VFGR:ATNDGR=1,QUEMODE=DQ,NOPT2=2,OPT=2,CQMAX=5,ITDEST=0&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15,AUTNS=OFF,SDIST=NO,CASMCF=YES,ANSYN=NO,WC=5,COD=OFF,INIGHTPR=NO;

ADD-ACTDA:TYPE=ATNDGR,ATNDGR=1,NOPT=2,ACT=ACT;

Personal Line -9200 in DDI Lookup

ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=9-200,DPLN=5,PROFIDX=181,LAUTH=1,PINDP=N;

NOTE:
If the amount of VF-Groups is not sufficient or calls to an extension must be routed directly to CPS a networking with closed numbering can be used.

Example for 985101-0 as corresponding VNRNU 985101 to Accesscode 49 89 7007-0

ADD-WABE:CD=0181,DAR=NETRTE,CHECK=N;

ADD-WABE:CD=985101,DAR=OWNNODE,CHECK=N;

ADD-WABE:CD=0,DPLN=0,CPS=6,DAR=STN,CHECK=N;

ADD-LODR:ODR=171,CMD=OUTPULSE,DGTS=498970070;

ADD-LODR:ODR=171,CMD=NPI,NPI=ISDN,TON=INTERNAT;

ADD-LODR:ODR=171,CMD=END;

ADD-LODR:ODR=171,INFO="CPS CLOSEDNUMBERING";

ADD-RICHT:MODE=CD,LRTE=171,CD=0181,CPS=0,SVC=VCE&DTE,NAME="CLOSED-NUMBERING",TGRP1=181,DESTNO=181,DNNO=1-1-181,REROUT=NO,PDNNO=181,CHARCON=NEUTRAL,NOPRCFWD=NO,CLNAMEDL=NO;

ADD-LDAT:LROUTE=171,LSVC=ALL,LVAL=1,TGRP=181,ODR=171,LAUTH=1,CARRIER=1,ZONE=EMPTY,LATTR=NONE,VCCYC=4,GW1=181-0;

CHANGE-WABE:CD=9851010,DESTNO=181;

5.4.6 Configuration of the CPS Resources

4. Configure CPS Resources

Example Configuration

Loop-, Request- and Callback Numbers

ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP=9-xxx,DPLN=5,PROFIDX=181,LAUTH=1,PINDP=N;

NOTE:
Only use '–xxx' in LDPLN if the Number length of the Resources Numbers is the same. If the length is different, configure each Number individually.

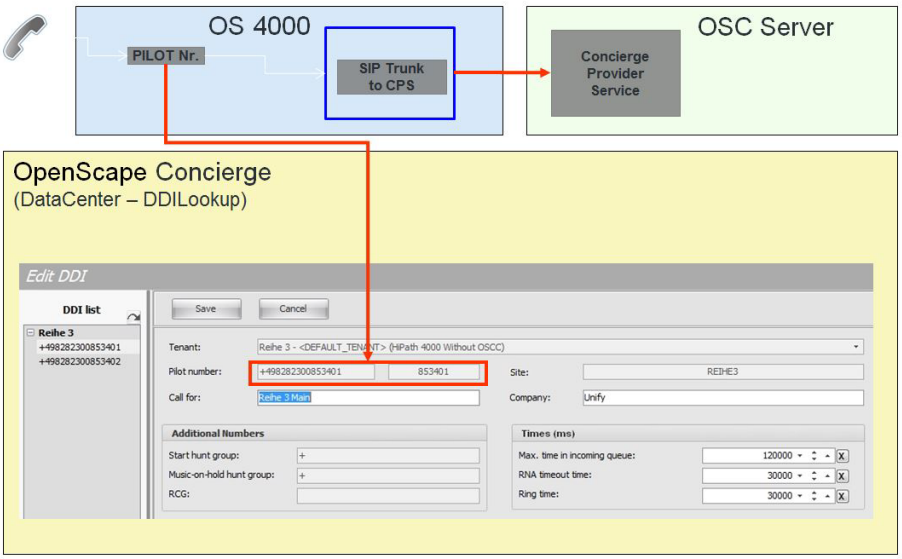
5.4.7 DDI settings in OpenScape 4000

All incoming calls are handled by CPS and thus have to be routed to the SIP endpoint for CPS. There are number ranges for pilot numbers / personal lines as well as ranges for the request pool and callback pool, which are used to route calls to CPS. The CPS is fully responsible for the call handling.

In case the CPS / Concierge server fails, the calls will be routed to a dedicated fall back hunt group that is used for Concierge only. All attendants' devices have to be member in that hunt group to be able to handle the calls in a fall back scenario.

5.4.8 DDI Lookup entry example for OS4000 without OSCC

The following figure shows the relations between the pilot number in OpenScape 4000 that routes the call to the CPS and the required entries in the DDI Lookup in Concierge Data Center.



We see the configuration of a pilot number in Data Center using Concierge without OpenScape Contact Center integration.

The pilot number must be a number that routes to CPS as described above. At least one service number has to be configured. Optionally additional service numbers can be used, depending on the customer's needs, like e.g. one for main, internal, Intercept or CF that allow Concierge creating meaningful statistics.

These queues with their corresponding pilot number need to be configured in Concierge Data Center for Concierge being able to monitor the incoming calls.

NOTE:
For detailed information on Data Center configuration, see appropriate OpenScape Concierge, Administrator documentation.

5.5 Routing configuration in OpenScape 4000 with OSCC

The configuration is nearly the same as "without OSCC integration", the difference is that instead of a pool of pilot numbers and personal line numbers here only the personal line numbers are used.

5.5.1 Definition of numbers and number ranges

With OSCC the CPS connection uses two number ranges:

One for the **personal line numbers** of the attendants and one for internal CPS resources like Request pool and Callback Pool.

Furthermore if CPS fails, a fallback Hunt Group has to be defined in the OpenScape 4000, where all attendant users are members. The fallback solution is used in case of CPS failure for the personal lines.

These calls coming in via the personal line numbers are routed to that fallback hunt group. The **internal resources** like callback numbers and request numbers will not be used in case CPS fails. Therefore no fallback for these is required.

NOTE:
In the scenario with OSCC all queues are handled by OSCC except the personal lines. They are queuing in CPS.

Define number ranges:

Parameter	Description	Value
CPS Resources for the example in the following sections		
Personal Lines Start	Numbers that route to CPS used for Personal Line Numbers of attendants	+495050580-9200
Personal Lines End		+495050580-9299
Loop Number	Used in Multi-CPS environment	+495050580-9300
Request Numbers Start	Numbers that route to CPS used for internal tasks, like e.g. Park, Append	+495050580-9301
Request Numbers End		+495050580-9349
Callback Numbers Start	Numbers that route to CPS used for paging service (Park Slot Numbers)	+495050580-9350
Callback Numbers End		+495050580-9399
Fallback Hunt Group	Hunt Group for Calls to Pilot and Personal Line Numbers, if CPS fails	+4950505805520

5.5.2 Two fallback scenarios to be considered

OSCC is down: the normal fallback mechanism for OSCC is used, the hunt groups switch from manual to UCD.

Only the OSCC queues are affected – the personal lines are not.

CPS is down: the OSCC queues are not affected; the calls are still routed by OSCC.

Calls to personal lines cannot reach the CPS (CPS is not registered anymore) so these calls use the fallback mechanism to the fallback hunt group.

5.5.3 Settings in OpenScape 4000

For the configuration of the OpenScape 4000 please refer to the sections 5.4 Routing configuration in OpenScape 4000 without OSCC.

NOTE:
The example configuration describes a configuration in the environment of the lab. In customer's environment other parameters are required, like e.g. different IP addresses, number ranges, prefix access codes, etc.
Only trained staff should configure the OpenScape 4000 and adopt the configuration to the customer's environment.

5.5.4 DDI Lookup entry example for OS4000 with OSCC

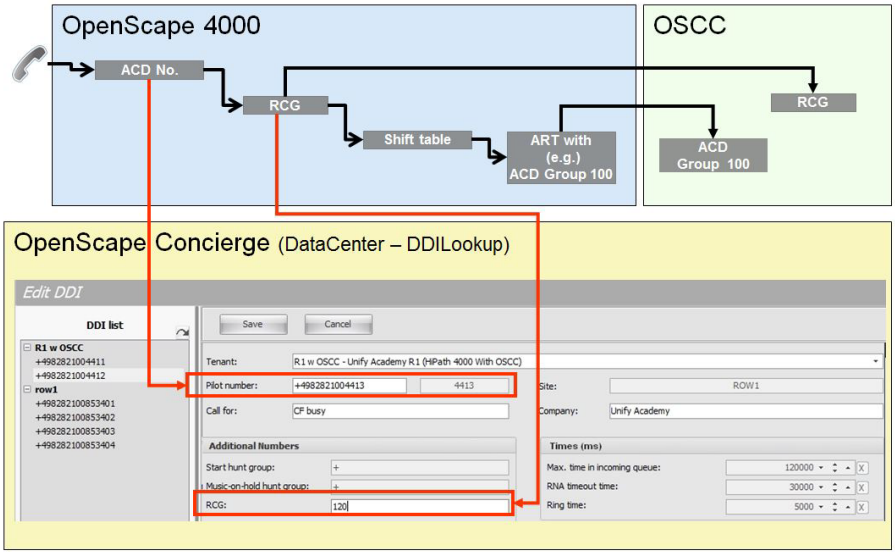
The following shows the relations between the pilot number in OS 4000, the entries in OSCC and the required entries in the DDI Lookup in Concierge Data Center.

With OpenScape 4000 the integrated ACD routing is the base for the integration with OpenScape Contact Center.

Incoming calls pass an ***RCG***, which is an instance that needs to be monitored in order to get information about an incoming call.

Therefore two items in the OpenScape 4000 must be known for a given service number, the ***service number*** itself and the ***RCG*** it is passing.

The figures illustrate the settings in OpenScape 4000 with its corresponding settings in OSCC that are reflected in the DDI Lookup table fields for Concierge.



A service number which is dialed by the customer is routed over the RCG to the ACD-Routing table and is then monitored by OSCC.

The Pilot number must be an ACD number that routes via the internal ACD routing of the OpenScape 4000 to an empty ACD group.

Principally at least one service number has to be configured as described.

Optionally additional service numbers can be configured, depending on the customer's requirements, like e.g. one for main, internal, CF busy and/or CF no reply which allows Concierge to create meaningful statistics.

NOTE:
For detailed information on Data Center configuration, see appropriate OpenScape Concierge, Administrator documentation.

5.6 Trunk Monitoring for OpenScape 4000

After setting up the PABXLink Node for OpenScape without OSCC you have to enter the settings for OS4K Trunk Monitoring in the OpenScape Concierge DataCenter. For a detailed description refer to section 8.9 System data / OS4K Trunk monitoring table (with OS 4000 only).

5.7 CPS Trunk Monitoring for OpenScape 4000

After setting up the PABXLink Node for OpenScape without OSCC you have to enter the settings for OS4K CPS Trunk Monitoring in the OpenScape Concierge DataCenter. For a detailed description refer to section 8.10 System data / CPS Trunk Monitoring.

5.8 Malicious Call Identification

OS4000:

To allow the Concierge Client to trace an incoming call add the parameter “Manual Call Trace in ISDN” to the class of service of the Concierge extension. Also add a key code for the Dial analyst result “Trace”. For further questions refer to the OS4000 service manual.

Example Configuration

CHANGE-COSSU:TYPE=COS,COS=xx,AVCE=MTRACE;

ADD-WABE:CD=*17,DAR=TRACE,CHECK=N;

Concierge Data Center:

Enable this feature in Concierge Data Center under **System data** / **Client configuration** / **Layout**.

For details see OpenScape Concierge, Administrator Documentation

5.9 Busy Override

OS4000:

To allow the Concierge Client to override a busy extension add the parameter “knocking override” to the attributes of the Concierge extension. Also add a key code for the dial analyst result “knocking/camp-on override”. For further questions refer to the OS4000 service manual.

Example Configuration

CHANGE-SDAT:STNO=xxxx,TYPE=ATTRIBUT,AATTR=KNOVR;

ADD-WABE:CD=*19,DAR=KNOVR,CHECK=N;

Concierge Data Center:

Enable this feature in Concierge Data Center under **System data** / **Client configuration** / **Layout**.

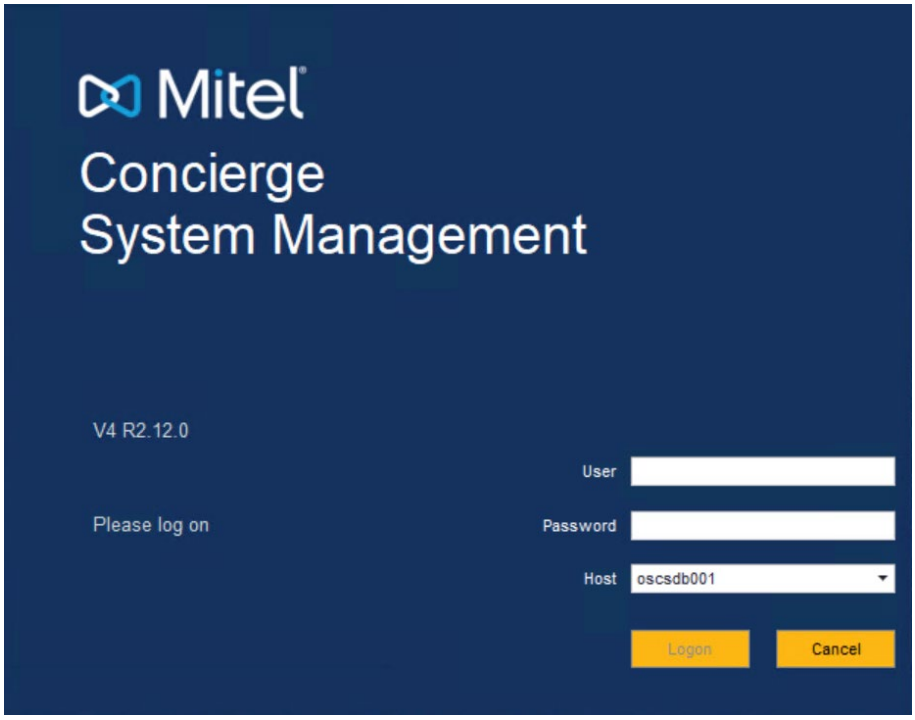
For details see OpenScape Concierge, Administrator Documentation

6 System Management

After the installation has finished and prerequisites are fulfilled, start **System Management** (via programs or shortcut on the desktop) and log on with the ***systemmanager*** account (user: “systemmanager”, password: “manager”).

Connect System Management application to the Main Server machine in your infrastructure:

Verify the server from the dropdown list of field **Target** and log on.



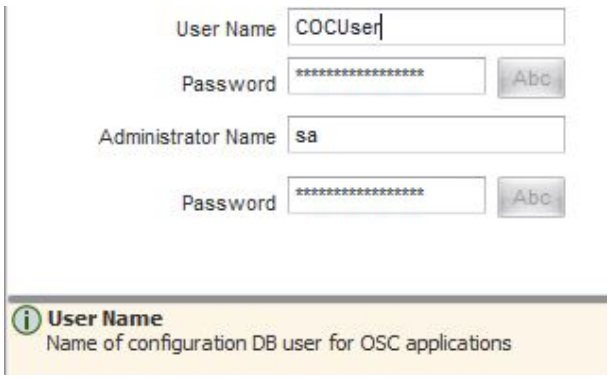
The System Management window opens. On the bottom line the green icon shows that the connection to the server is up and that you are logged on to Server data of the machine with the *systemmanager* or *manager* account.

NOTE:
Generally the System Management is configured from top to bottom. Open each section and configure the settings that are required for deployment. Leave out settings that are not used.

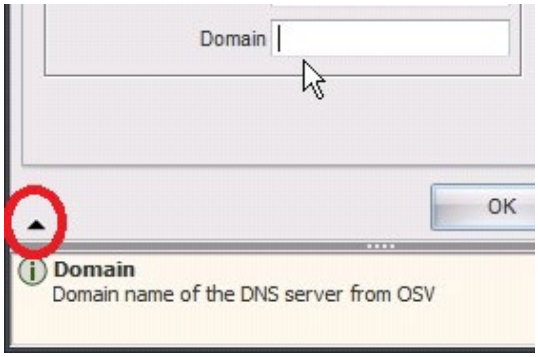
By “publishing” the configuration finally, the settings are transferred to the server database.

Help text

Each window has a help text for each field. Click into the field and the help text appears in the information section.



In separate windows the information section appears by clicking on the arrow:

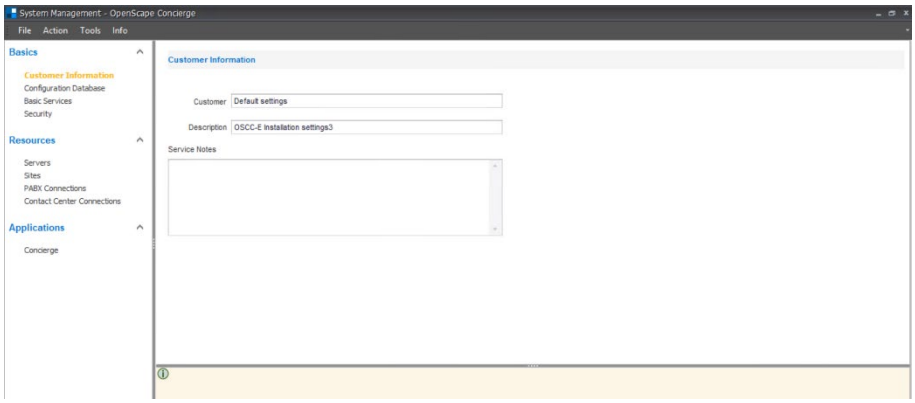


6.1 Section “Basics”

System Management opens with the tab *Installation Designer* section *Basics* and displays **Customer Information**.

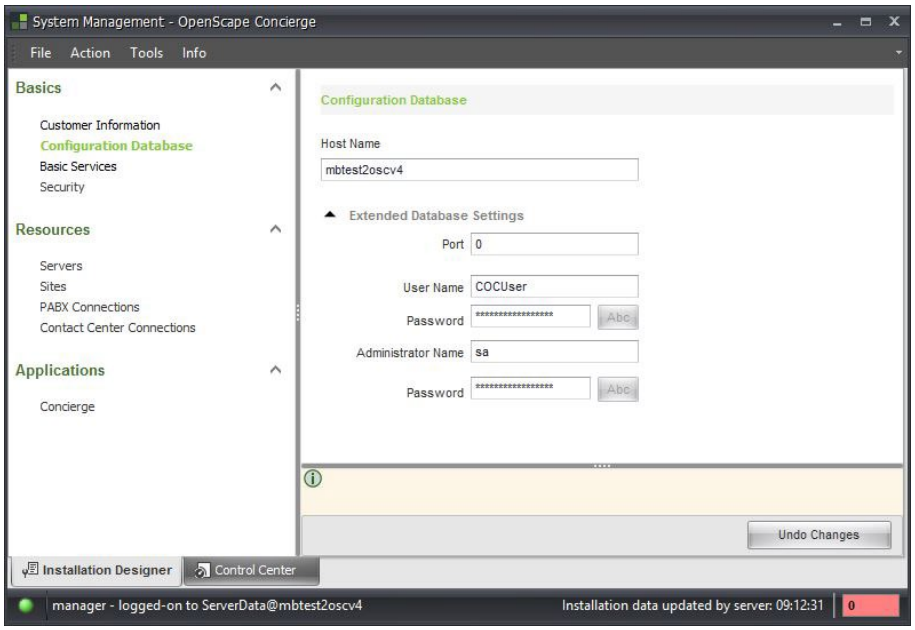
6.1.1 Customer Information

Enter **Customer’s** name and a **description** as well as information that are relevant for this project under **Service Notes**.



6.1.2 Configuration Database

Move to **Configuration Database**. By default the application displays the main server’s name as **Host name** for the internally used MS SQL Express database.



External database server connection

In case an external database is used, replace the OSC Server’s host name by the external MS SQL Server’s **host name** and **port number.** A **user account** and an **administrator account** are required.

The **User account** is used for the application to log during operational hours, the **Administrator account** is required for creation of the user accounts and databases during the first implementation process (or for patching) on that machine.

That means that the A**dministrator account needs the SA rights** on the database.

By default the Port is set to 0. This is the default value for connecting to a standalone database server. In this mode the communication ports will then be assigned dynamically.

In case an external MS SQL server cluster is in use, ask the database administrator for the port to connect to the ***Listener***

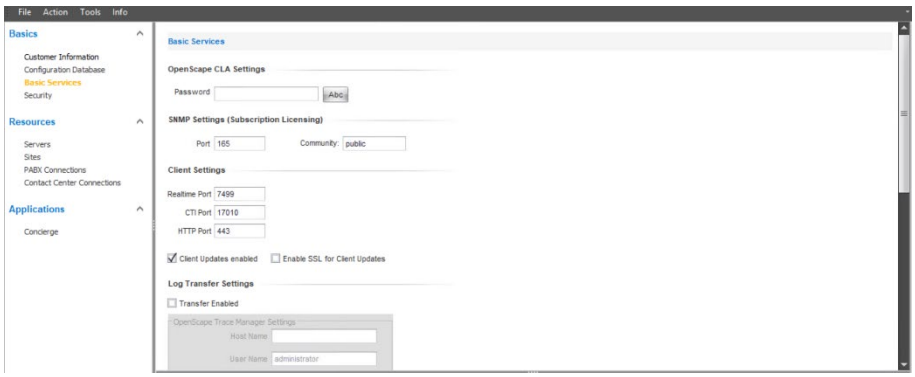
NOTE:
The services *ControlConfigDB* and *ControlOscadmDB* running on the OSC Server create and maintain the required tables and users on the database server(s) using the Administrator account.

A description of how an external database is connected directly after installation is described in the OpenScape Concierge Server Setup, Installation Guide.

For moving configuration data from one database Server to another, please see section 7.2 External SQL-Server for ConfigDB / OSCADM

6.1.3 Basic Services

NOTE:
Do not change the default values if no other or additional settings are required.



Basic OSC settings are entered for:

- OpenScape CLA
- SNMP (for Subscription Licensing – see next section)
- Client
- Log Transfer (for OpenScape Trace Manager)
- SNMP Agent
  OSC is supporting SNMP to see System state messages (so called Traps) in a **Management System** (e.g. OpenScape Fault Management). It is necessary to know the **version of SNMP** the customer is using. For SNMP V1 or V2, configure the target IP address only.

With SNMP Version 3 a user is required, a password and the protocol type with its parameters (provided by customer).
This way the SNMP Management system logs on to OSC to receive the system status of the machines.
When configuring Authentication and Privacy for SNMP V3 the combination of MD5 and TripleDES is NOT Allowed and not supported.
The Community String has to be the same as the one in SNMP Managementsystem.

NOTE:
The **MIB** (Management Information Base) contains the values and properties of „Managed Objects“, which can be monitored by a Management System. In an OSC perspective „Managed objects“ are Server processes like the Contact Center Node or PABX Link Connector.

The provided **MIBs** have to be imported on the customer’s SNMP Management System. The required MIBs (OSC-TRAP-MIB and SEN-ROOT-MIB can be found in ***Unify IFMDB***. Please ask your Unify contact for more information.

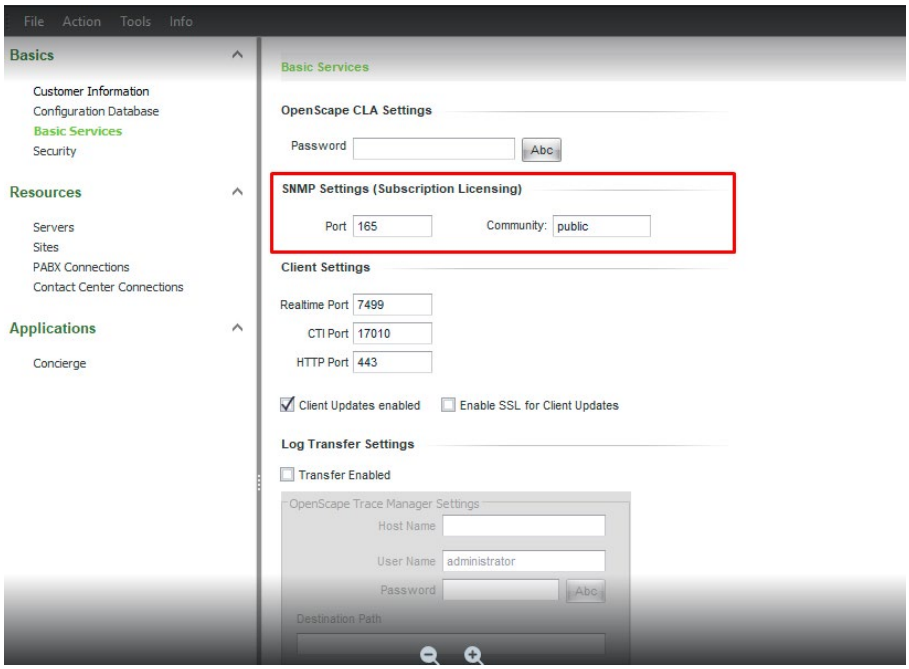
- Backup stores the backup both local databases (OSCAdm and configDB) and the System Management configuration (OscceService.Installation.xml) – see also section 7 Maintenance.

6.1.3.1 Software Subscription Licensing (SSL)

For Concierge the Software Subscription Licensing can be used. In order to use this option follow the configuration described below otherwise skip this chapter.

Configuration in System Management

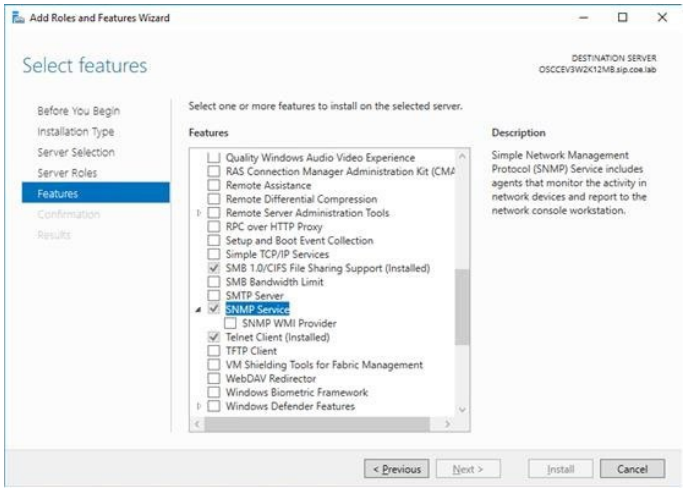
The configuration for Software Subscription Licensing within OSC is already done for you. In System Management under **Basic Services** the only visible options are the Port number and the Community, under **SNMP Settings (subscription Licensing):**



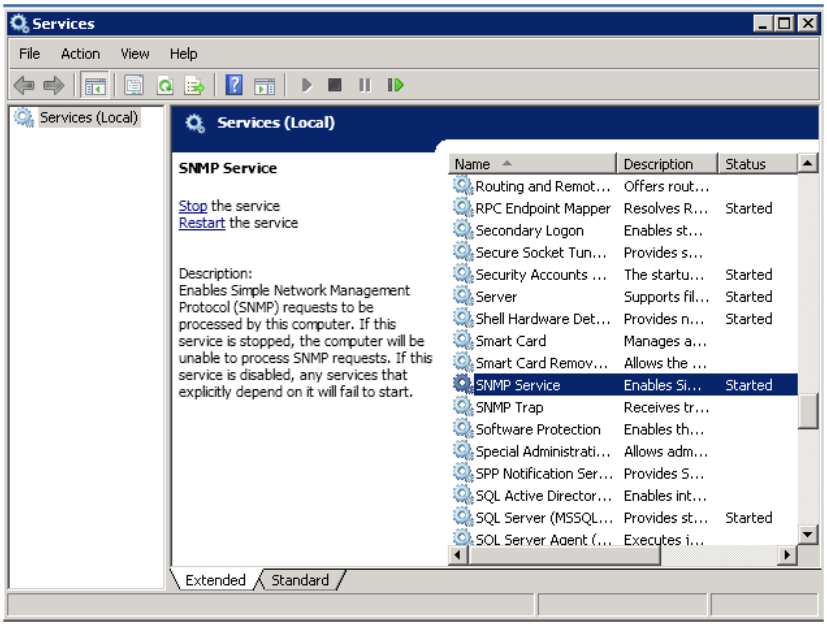
Only change Port 165 in case it cannot be used.

Configuration on OSC Server

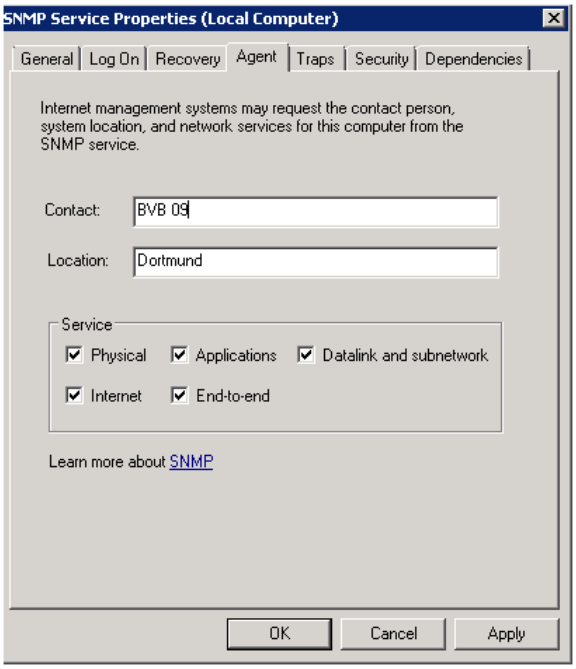
1. Install and activate the SNMP feature in Server manager.



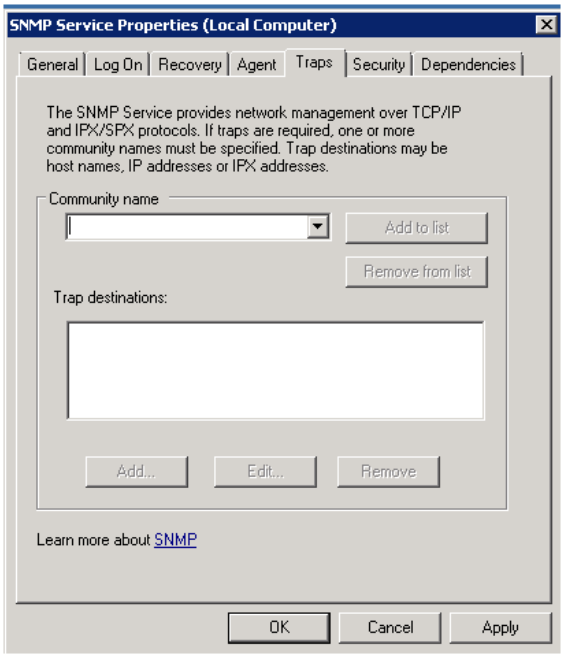
2. Under **Services** select the SNMP Service and double-click it.



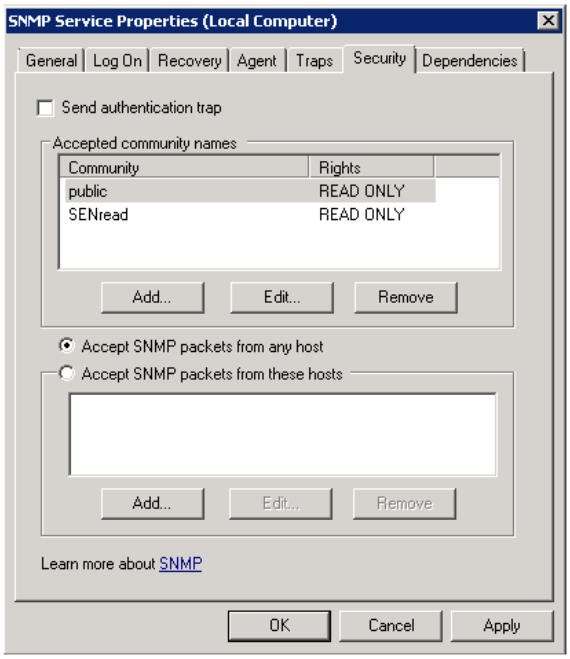
3. Select the **Agent** tab and tick all parameters under Service:



4. The **Traps** tab can remain empty:

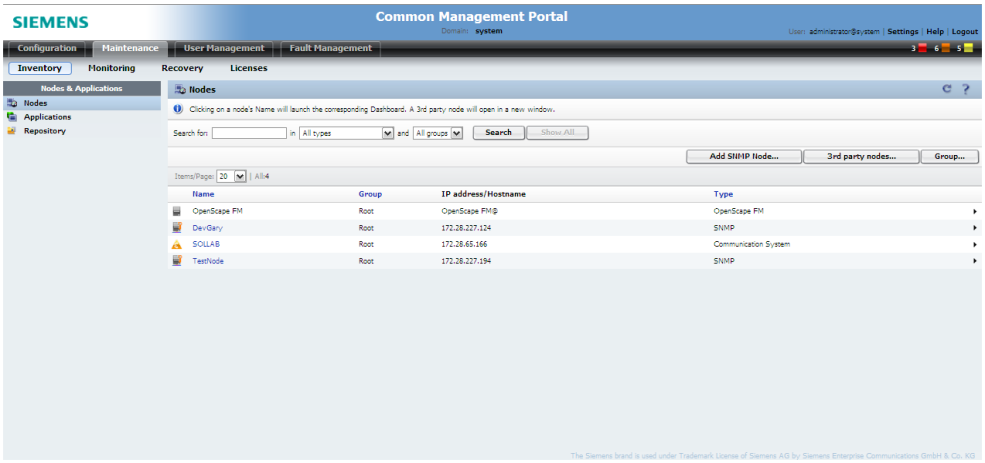


5. Select the **Security** tab. Add a community name (has to match with entry in OSV - in this example: SENRead) with the rights **Read Only**.
   Accept SNMP packets from any host has to be activated. In case you choose to select **Accept SNMP packets from these hosts** you have to add the OSV.

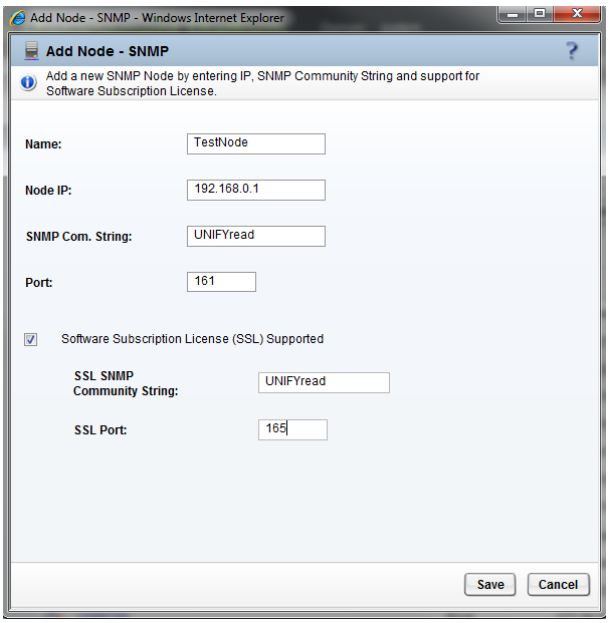


Configuration in OSV

1. In OSV Common Management Portal go to **Maintenance** \ **Inventory** \ **Nodes** and click on **Add SNMP Node…**



2. Enter the node parameters:

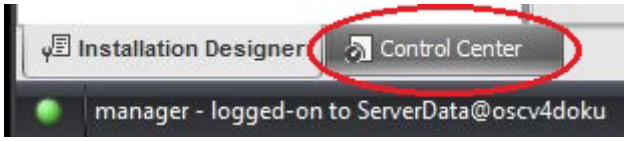


3. The Community String depends on the OSV configuration and type of installation. The administrator who prepared this machine should know the port and community string.

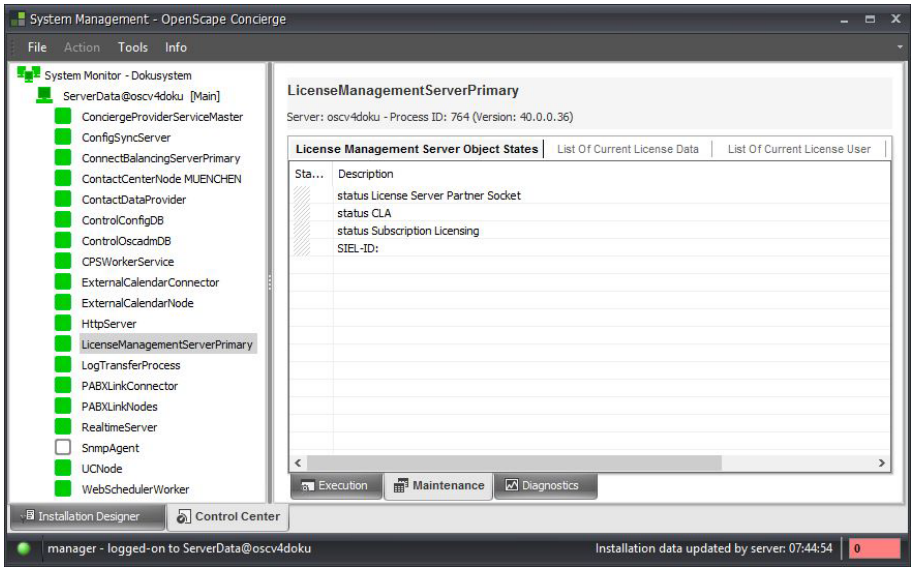
6.1.3.2 License Management

The License Management Realtime Viewer of OSCC-E versions former to V3 is integrated in the System Management application on the OSC Server.

1. In **System Management** go to the **Control Center** by selecting the following tab:



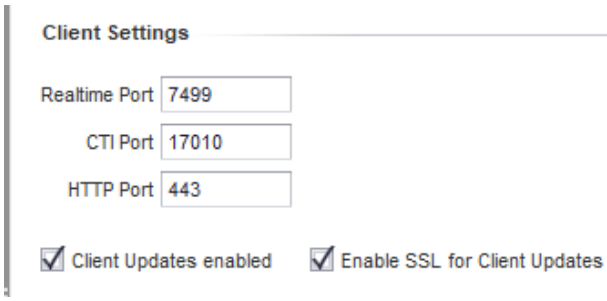
2. Select the LicenseManagementServer
3. Change to the Maintenance tab.



Here you find the tabs:

- License Management Server Object States
- List of current License Data
- List of current License User

6.1.3.3 Client Settings



For automatic Concierge client updates, it's possible to secure the connections through of HTTPS, just check the option "Enable SSL for Client Updates".

NOTE:
The Concierge opens a HTTPS webserver port 443 to be used with 3rd party or customized web applications. To avoid conflicts with other applications, this port could be changed through OpenScape Concierge System Management application -> Basic Settings -> Client Settings.

NOTE:
The secure feature will only work if there is a certificate applied in the Security section.
See section 6.1.4 – Security.

6.1.4 Security

For details on Security and on how to exchange the Standard Certificate for a Customer Certificate, refer to the OpenScape Solution Set V10, Certificate Management and Transport Layer Security (TLS), Administrator Documentation in the Subsection 3.21 OpenScape Concierge.

6.1.4.1 How to exchange the standard certificate for a customer certificate

In case you decided to exchange the standard certificate for a customer certificate, please follow this procedure:

Procedure

1. Use the bottom **Load from Store…** or **Load from File…** depending on where you load the certificate from.
2. Choose the certificate you want to use.
3. Enter the Certificate's Password and confirm your entry by **OK**.
4. Confirm the next message with **Yes** to replace the certificate.

5. After you have changed the security settings, you have to publish the changes by pressing **F5** or selecting **Action** / **Publish Installation Data**

IMPORTANT NOTE:
After publishing new security settings, all OSC services including all service processes must be restarted!

6.2 Section “Resources”

Under Resources *create and assign all hardware components* of the deployment. All servers that are included in the OpenScape Concierge architecture are “registered” here and their task in the system environment is assigned, for example the standby server for a redundant installation can be configured.

6.2.1 Servers

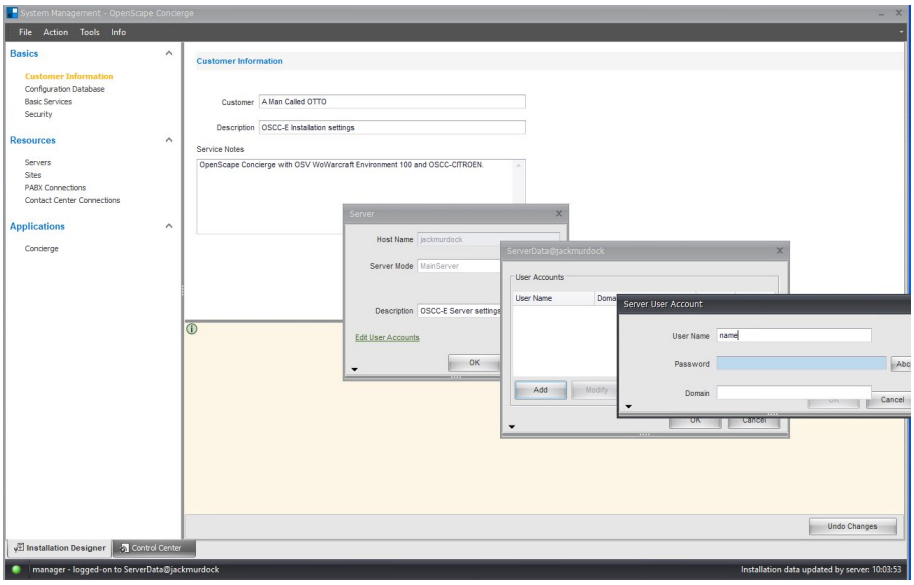
Under **Servers** all installed servers (Main and Standby server) are automatically displayed as soon as they are correctly installed.

- Main and Standby server have the Usage Type Standard

In case you perform an offline configuration, meaning that you pre-configure an OpenScape Concierge environment with System Management without being connected to it, you register the Main server and if needed, the *Standby* server. Assign the **Server Mode** in the deployment. Choose the **Usage Type** for the server from the dropdown list and write down a short **description**.

Modify User Accounts

In case you need further Windows User Accounts, you can define them here. Enter the requested values and confirm your entries with **OK**. Also see section 6.2.3 PABX Connections / Run PABXnode Process under Separate User Account.



6.2.2 Sites

The **Master Site** describes the active site/ location where this OSC Server deployment is assigned to its main communication platform.

NOTE:
There can only be one master site!

Add a new site by pressing the **Add** button and enter a **Site ID**, a description and choose the corresponding servers out of the list of available servers.

The checkmark on the right that indicates whether the site is in use or not and will be set automatically if a PABX connection is configured.

Additional sites can be configured for monitoring the corresponding communication platforms with the present deployment. These can be defined under **Monitoring sites**.

NOTE:
Concierge users only connect to the Master Site's communication platform but are able to monitor extensions from additional (monitored) sites!

6.2.3 PABX Connections

Under **PABX Connections** configure the settings for the communication platform integrated.

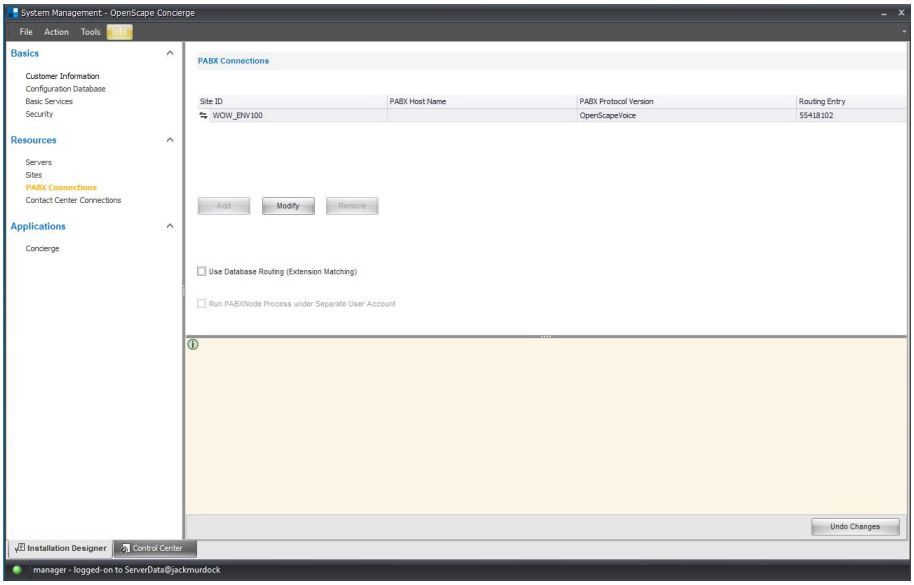
Use Database Routing (Extension Matching)

See detailed information under section 6.2.3.3 Synchronization.

Run PABXnode Process under Separate User Account

Enable this option if more than about 10 sites are used for PABX connections a separate user account for the PABXNode process can help prevent resource shortage.

In case this option is enabled, the system searches for an unused User Account which can be configured under Servers / Add or Modify / Edit User Accounts – see section 6.2.1 Servers for details on User Accounts.



Connections

Use the **Add** button to configure a new PABX connection or the **Modify** to read or modify your entries for the PABX connection.

6.2.3.1 General

NOTE:
The number of PABX connections corresponds to the number of sites. Thus one PABX is assigned to one site.

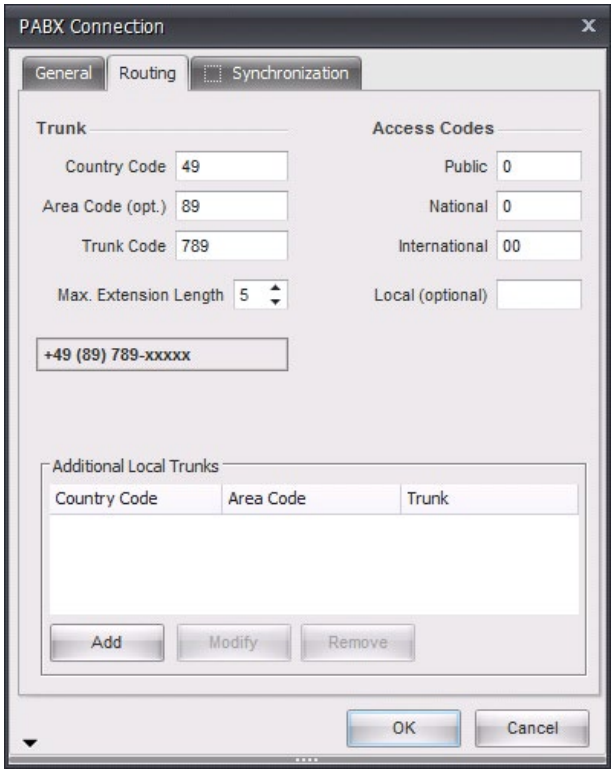
1. Select the Site ID.
2. Choose the type of communication platform from the dropdown list **PABX Model** and add further connection data, like **PABX Host Name** and **PABX Port** and **Node Listener Port** number.

   NOTE:
   For Integration with OpenScape 4000 in any of the supported versions, please choose the **PABX Model** HiPath 4000.

3. In case OSC is connected to OSV, enter the information under OSV Node.

HINT:
Use the help text under the arrow  at the lower left side of the window in case you are in doubt.

6.2.3.2 Routing



1. Configure Routing Data entries for **Trunk**. Enter digits for **Country Code**, **Area Code** (opt.) and **Trunk Code** without leading zeros and/or other special characters. Also enter the **Maximum Extension Length** for all trunks of this PABX.
2. Configure **Access Codes** for
   - **Public**
     Outside line access code to dial a public number.
   - **Access Code National**
     National Prefix which is mostly ‘0’. To resolve a national telephone number, a combination of Access Code Public and Access Code National is used, e.g.:
     Access Code Public = **0**
     Access Code National = **0**
     → Phone Number ***00****8970070* is identified as a *National Phone Number*
   - **Access Code International**
     International Prefix which is mostly ‘00’. To resolve an international telephone number, a c*ombination of Access Code Public and Access Code International* is used, e.g.:
     Access Code Public = **0**
     Access Code international = **00**
     → Phone Number ***000****498970070* is identified as an *International Phone Number*
   - **Access Code Local (opt.)**
     Outside line access code only for special scenarios

NOTE:
In case above access codes are not used in the country, amend the SystemManagement.ini accordingly – see section 6.8.1 Application settings.

3. Additional Local Trunks
   If the communication platform supports multiple exits to COs, you can add additional local trunks by pressing the **Add** button in the **Additional Local Trunks** field.

6.2.3.3 Synchronization

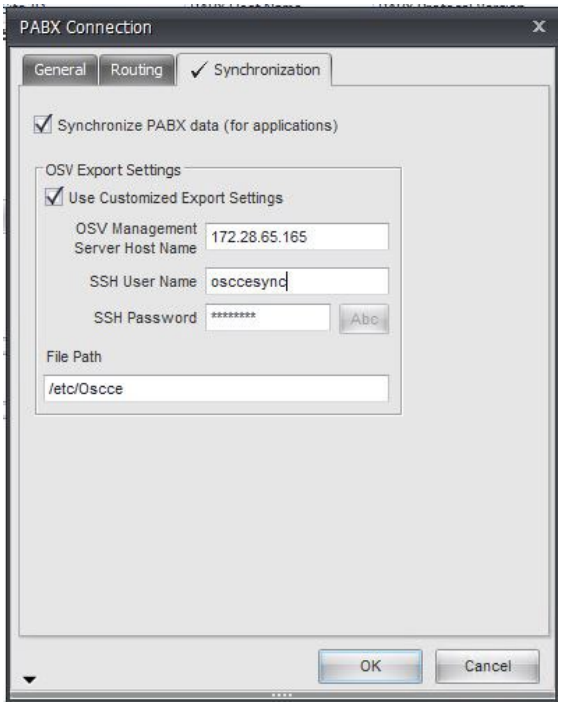
For the synchronization of extensions set the checkmark **Synchronize PABX data (for applications).** This allows connecting to the PABX and storing the extension data in the PABX-User-Table in the ConfigDB, as described in the following section.

In case **Additional local trunks** or **multiple sites** are used, a ***database routing*** can be defined that controls routing of calls to different target extensions in multiple sites.

Set the checkmark **Use Database Routing (Extension Matching)** in the main ***PABX Connections*** window if that is needed!

In case this option is checked a new area, for accessing the PABX has to be configured in the PABX Connection window.

Hint for Private Numbering:
In case you want to configure private numbering, please refer to appropriate OpenScape Concierge, Administrator Documentation.



OSV

In the field **OSV Export settings** configure the OpenScape Voice IP address and ensure that the “installExportForOsc.*sh*” script was successfully implemented on the OSV.

OSV Data Export for synchronizing PABX Extensions (also for CDP)

For the OSV data export procedure which can be used to import OSV user data via CDP into Concierge, a script is available that modifies OSV settings correspondingly.

NOTE:
The same script is used for accessing the OSV for CDP as described in OpenScape Concierge, Administrator Documentation.

The script is available on the installation DVD. The procedure is as follows

1. Bring shell script from DVD to OSV
   for OSV => V9:
   `(.\Tools\OSVExport\installExportForOscAndOsvV9.sh)`.
   If using FTP, **do NOT** use Binary mode, but Text mode.
2. Run the script using the **root** account:
   - The script creates a Cron Job that creates the MP2File
   - The script creates a path where the MP2File is created
   - The script creates a user that can access the OSV and download the MP2File.

The user credentials to log on to the OSV for downloading the MP2 file are:
User: **osccesync** and Password for OSV => V9: *always open the script with a viewer and check current password.*

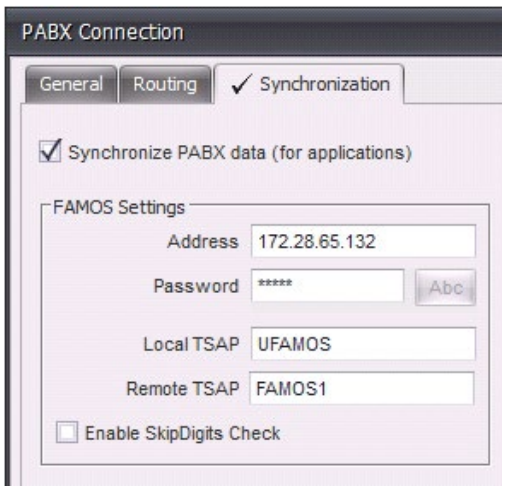
Important Note:
Whenever an update of OSV is performed, the procedure has to be done again!

You have to adjust the password in System Management under PABX Connections

Make sure that the OSV's host key (rsa2 key fingerprint) is cached in the registry of the OSC Server. This can be done by once logging on to the OSV using PuTTY from the OSC Server.

OpenScape 4000

Configure the IP address and connection for FAMOS access.



When using the standard configuration with Local TSAP = UFAMOS and Remote TSAP=FAMOS1 the PABX extensions are automatically synchronized.

For testing the OS4000 access for Configuration Synchronization please use the **FAMOS Tester** from the `\Tools` folder on the Installation DVD!

In case you want to individually configure the synchronization, you can follow this example:

OS4K synchronizing PABX Extensions Example.

Start Comwin and connect to the OS4K.

Configure the connection with the AMO CPTP

ADD-
CPTP:TYPE=DPCON,NO=50,DPPROC="FAMOS",IPNO="192.0.2.25";

ADD-
CPTP:TYPE=APPL,NO=50,EMSAPPL="FAMOS",DPPROC="FAMOS",DPAPPL="FAMOS",MSGBASED=YES,LOCPORT=102,FARPORT=5011,LOCTSAP="SRC",FARTSAP="DST";

Configure the password with the AMO PASSW

ADD-PASSW:TYPE=PSWD,PWN="HICOM",PWC=5;

NOTE:
The values in the example configuration must be adjusted to the customer‘s environment.

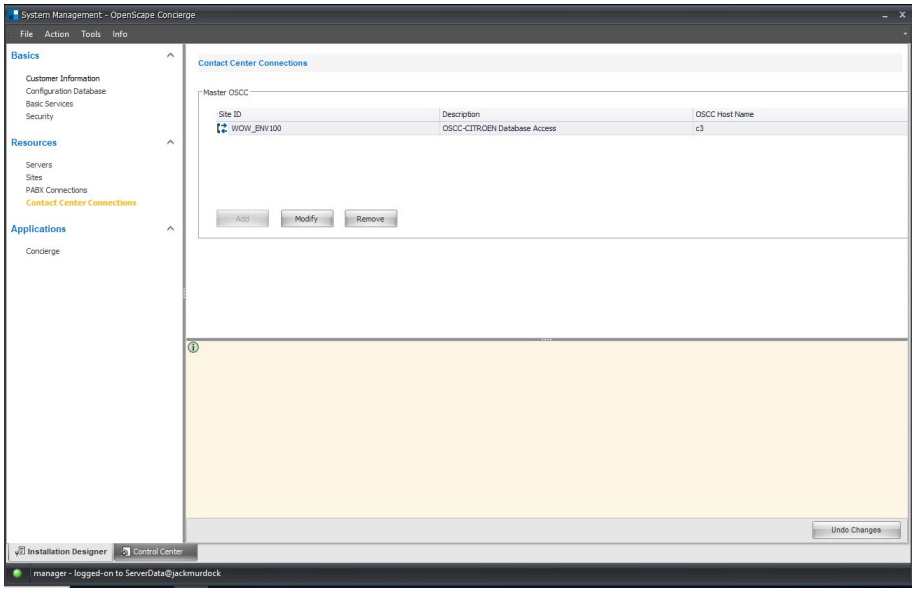
6.2.3.4 Geo-separated OSV

In case the OpenScape Voice has a **geo-separated** deployment, the pane OpenScape Voice is required.

A DNS service must be available. For the configuration of the necessary DNS services please refer to the settings in section 4.6 Configuration Microsoft DNS for geo-separated OSV deployment.

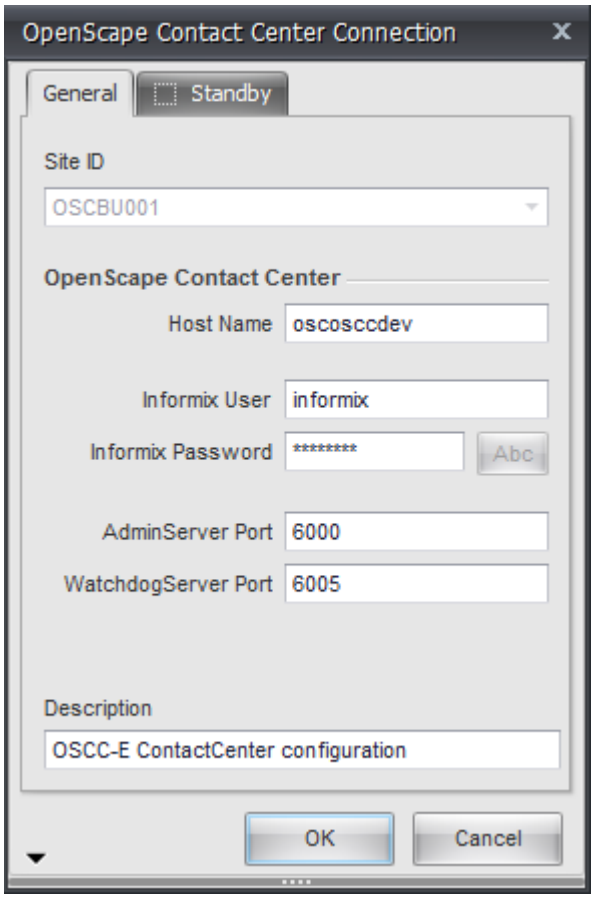
6.2.4 Contact Center Connections (Professional only)

→ Skip Contact Center settings if not integrated!



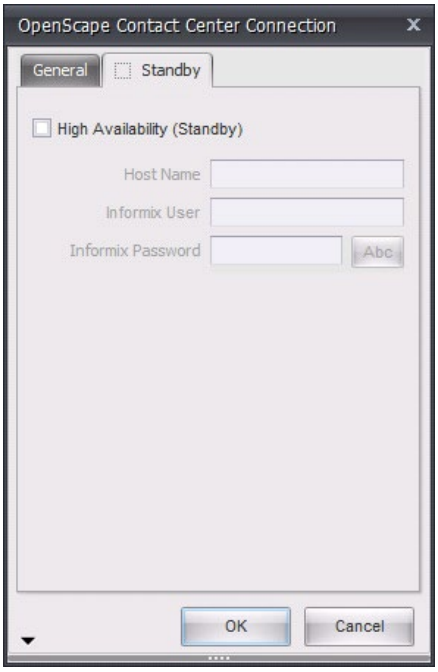
Master OSCC

Register the OpenScape Contact Center connection by pressing the **Add** button. A window opens to specify the **OSCC server name** and the **informix user** credentials for database access.



NOTE:
OpenScape Contact Center can only be assigned to the Master Site. Thus **one** Contact Center connects with **one** OpenScape Concierge deployment only!

In case an OSCC high availability deployment is used, the standby server connection has to be defined as well. Assign this OSCC system to your master site!



6.2.4.1 Settings in OpenScape Contact Center

For the OpenScape Concierge client applications working as agent application with the full agent feature set (like e.g. the post processing features) it is necessary to assign the Client Desktop access permission to the corresponding users/ agents in OSCC.

Procedure:

Logon to the **OpenScape Contact Center Manager** application; under **Users** in the **Admin Center** open the corresponding user settings. On the **General tab** under Application choose the ***Agent*** for the **Client Desktop** access.

NOTE:
Please be sure that the **Default Business Unit of OSCC** is not deleted in the Contact Center database. Renaming of that BU is okay, but if it is no more available, the Contact Center Node will not start successfully.

Check IP V6 and Firewall settings on the Contact Center Server in case the Contact Center Node does not start successfully.

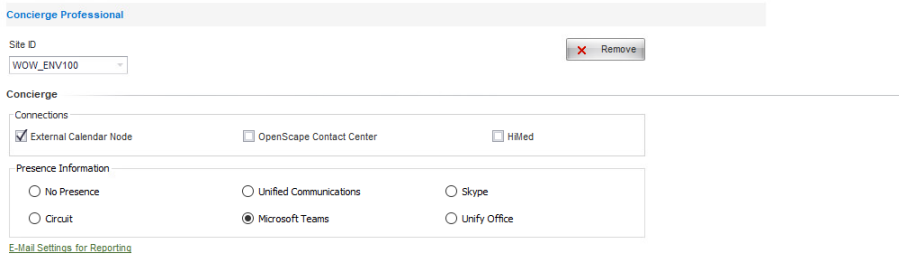
6.3 Section Applications

Concierge is available in two versions:

- Professional (full version)
- Plus (limited version)

Differences are clearly marked within this document (the images are based on Concierge Professional – so these might differ in case of a Concierge Plus environment). Further documentation (Administrator and User Guide) are strictly separated. Please make sure you continue with the correct documents after configuration – see section 9 Further procedure.

In the upper part of the Applications/Concierge window, activate the Concierge attendant console by choosing the **Site ID** previously configured under Resources/Sites.



Additional options can be activated, like **Presence information** from system integration (e.g. UC, Circuit, Skype or Microsoft Teams Node), **HiMed, External Calendar Node** (Professional only) and integration with an **OSCC** (Professional only).

For sending out reports via email, the **E-Mail Settings for Reporting** can be opened and configured by clicking the hyperlink.

The **Remove** button can be used to remove the whole Concierge settings in one. In case you clicked on this button by mistake, use the button **Undo Changes**.

6.3.1.1 Install Application redundantly (Professional only)

As soon as a Standby Server is configured the field **Install Application Redundantly** and the **Secondary Server** field appears and lists all available secondary servers with usage type Standard. Activate the field **Install Application Redundantly** and select the appropriate server as Secondary server (Standby server) for this application.

Also see section 2.3.2 Standby installation scenarios

6.3.1.2 Database Settings (MSSQL)

By default the application displays the main server's name as **Host name** for the internally used MS SQL Express database.

Extended Database Settings (Professional only):

You have the option to use an external database server for the contact data in the Electronic Telephone Book (ETB)

In case an external database shall be used, enter the Host Name of the external Server and extend the window by clicking on the arrow next to **Extended Database Settings**.

By default the Port number is set to 0. This is the default value for connecting to a *standalone database server*. In this mode the communication ports will then be assigned dynamically.

In case an external MS SQL server cluster is in use, ask the database administrator for the port to connect to the ***Listener***.

The **User account** (default: OSCADM) is used for the application to log during operational hours, the **SA User account** is required for creation of the user accounts and databases during the first implementation process (or for patching) on that machine. The SA User account thus needs the **SA rights** on the database.

Note:
The services *ControlConfigDB* and *ControlOscadmDB* running on the OSCC-E Server create and maintain the required tables and users on the database server(s) using the Administrator / SA user account.

A description of how an external database is connected directly after installation is described in the OSC Server Setup, Installation Guide.

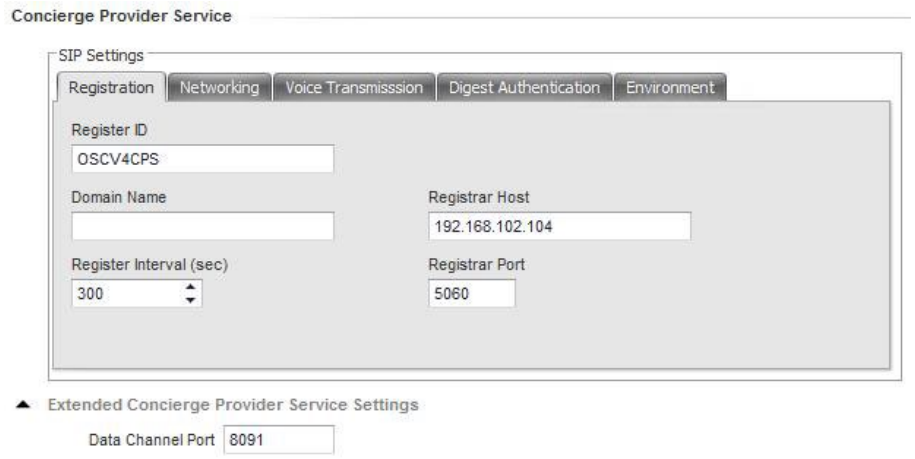
For moving configuration data from one database Server to another, please see section 7.2 External SQL-Server for ConfigDB / OSCADM.

6.3.1.3 Concierge Provider Service (CPS)

This pane displays the Concierge settings for the CPS and the communication platform (PABX). Enter the required registration information and network data from the PABX as well as CPS' own parameter for the endpoint configuration in PABX and security options (TLS and SRTP).

IMPORTANT NOTE:
The System Management offers a functionality to set the Concierge Provider Service to “config mode“.
This mode was introduced to provide a possibility to configure the OpenScape Concierge system without having a working SIP Trunk on OSV or OS4K. If the “config mode“ has been activated for configuration, the Concierge Provider Service needs to be restarted to end the config mode.
Attention: The entry “ConfigMode initiated” under ConciergeProviderServiceMaster/Messages might be deleted on a System Management refresh -> therefore it might not be visible, that the CPS is in ConfigMode!

It is not allowed to use this config mode on a system which is in normal operation!



In order to configure the CPS follow the help text in System Management, which appears at the bottom of the window when clicking on the field.

Some additional information:

The **Register Id** must match the value Alias in the endpoint configuration in OSV (please care about case sensitivity of the Alias name!), see section 4.4.4 Routing Configuration for SIP endpoint CPS. For OpenScape 4000 this field is not used.

The minimum value for the **Register interval** is 300.

For the **Registrar port** leave the default value 5060.

NOTE:
OpenScape Voice deactivates a SIP endpoint that registers in intervals shorter than 300 seconds. It is recommended to set the Register interval to 305 seconds.

Under **Registrar Host** enter the corresponding IP address of the Registrar for the CPS (with OSV this is usually the OSV IP address, for OpenScape 4000 use the IP address of the STMI card for CPS)

NOTE:
Using a Domain Name (e.g. in case of geo-separated OSV deployments) will cause CPS resolving the OSV registrar via DNS-SRV. Be sure just to enter the Domain Name itself (e.g. OSVCluster.com) and not the full DNS zone (like _sip._udp.OSVCluster.com).

For more details regarding the DNS-SRV configuration refer to section 4.6 Configuration Microsoft DNS for geo-separated OSV deployment.

Leave the default values for the **Default Registrar Port**, **Rtp Start Port** and **Rtp Port Count**. Configure the Loop number as defined above in the checklist. (Enter the Loop number including the '+' in front of the country code!)

NOTE:
The RTP ports are a continuous range of port that starts with the **RTP Start Port** value and ends up with that value increased by the **RTP Port Count**. It is important that the whole range of these ports must not be used by any other application, even if that is just a single port!

→Please ensure that none of these ports is used by any other application.

Under **Available Channels** enter the number of channels that are available on the SIP trunk to CPS. The maximum amount of channels is:

- 120 with OpenScape 4000 (STMI)
- 250 with OSV (increase the default value of 120 if required)

NOTE:
- If 90% of the "processing channels" are allocated the attendant gets an Alert Window
- If 100% of the "processing channels" are allocated the overload configuration will take over as configured under Miscellaneous in the DDI lookup table entries.

Overload settings only apply for processing channels, not for operational channels! They apply for both types of PABX, OpenScape Voice and OpenScape 4000

The **Channel Ratio** defines the ratio of channels used for "operational call handling by the attendant" compared to channels which are used for "call processing by CPS".

Operational call handling means the act of enqueueing and dequeueing of calls to or from the CPS. This is a short time usage of the channel initiated by the attendant. 2 operational channels are fix reserved for security reason to remain in operable mode.

Processing Channels are used for accepting the incoming calls and enqueueing and keeping them in the pilot number queue, the personal line queue or parking queue, provided by CPS. Those channels are also used for the paging functionality.

Channel calculation:

Example: 10 channels – ratio slider is set to 3; thus 2 channels are fixed reserved for operational handling, these are not part of the calculation.

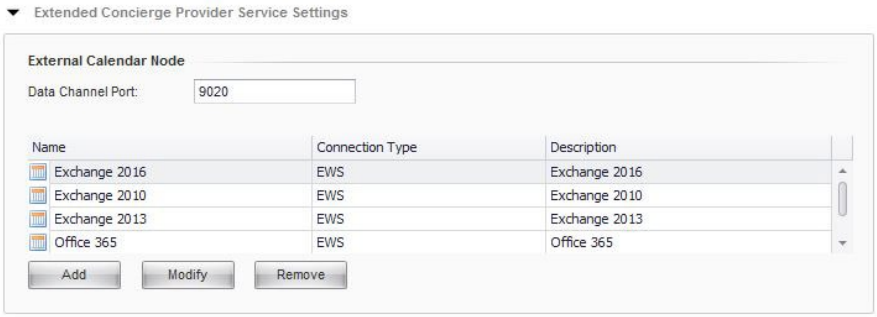
- *Formula for processing channels:*
  *(Amount of channels – 2) / (1 + Ratio-value) * (Ratio-value)*
  *= 8 / 4 * 3 = 6 Channels*
- *Formula for operational channels:*
  ((Amount of Channels – 2) / (1 + Ratio-value)) + 2
  = 8 / 4 +2 = 4 Channels

Setting the ratio slider to 5 allows you having more processing channels and increases the risk not to have enough operational channels for the Concierge user to park and transfer calls

Setting the ratio slider to 1 ensures the operational handling but can lower the number of contacts that can be in queue.

6.3.1.4 External Calendar Connector (Professional only)

By activating **External Calendar Connector** in the upper pane, a new area appears for creating connectors to external calendars, like e.g. Exchange 2016.



Click **Add** to create a new connector for an external calendar to display calendar information of the contacts available in ETB.

A new window **External Calendar** opens that allows the specification of the connection.

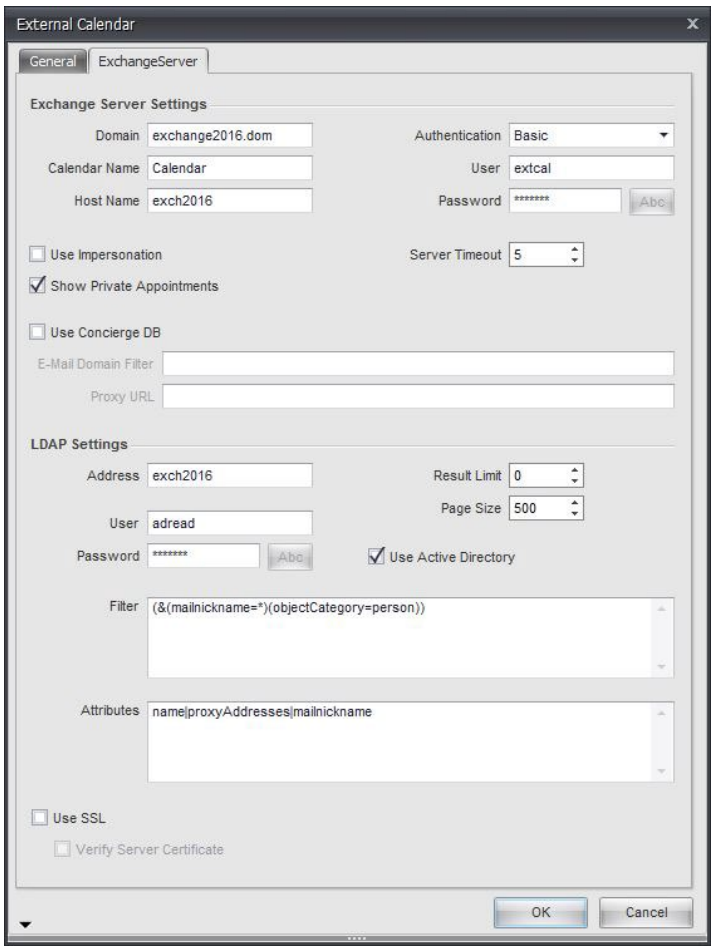
Under **General** - give the **External Calendar** name, a Description and specify the **Connection type**. You can choose between **EWS**, **WebDAV** or **Offline DB**.

NOTE:
WebDAV is supported until Exchange Server 2007. It has been discontinued in later versions. EWS is supported in Exchange Server 2010, 2013, 2016 and 2019.

The latter type of connection allows importing a **CSV file** with calendar information as well as the **data import directly from a MS SQL database**. The corresponding parameter (with EWS or WEBDAV) can be configured under **ExchangeServer** tab

Exchange

Example for Exchange 2016 integration:



Enter the configuration parameters as of the table.

Variable	Description
Exchange Server settings	
Domain	Domain name of the Exchange server
Calendar Name	Name of the Calendar for Concierge user to choose
Host Name	Name of the Exchange server
Authentication	Authentication for the user Basic Integrated FormBased OAuth(User/Password) OAuth(Client Secret)
User	User name for the Exchange node to access the Exchange server.
Password	Encrypted password for the user
Use Impersonation	Usage of impersonation
Show Private Appointments	Visibility of private appointments (without info)

Variable	Description
Exchange Server settings	
Use Concierge DB	Use Concierge DB for LDAP settings (mostly used with Office 365)
E-Mail Doman Filter	Domains for which e-mail addresses are queried by the connector (separate domains with ";") - (mostly used with Office 365)
Proxy URL	Proxy server URL or PAC script URL - (mostly used with Office 365)
LDAP Settings	
Server Timeout	Max. duration for Exchange server timeout
Use Concierge DB	Use Concierge DB instead of LDAP for possible e-mail accounts
Address [:port number]	IP address of LDAP server
User	The LDAP user
Password	Encrypted password for the LDAP user
Filter	For LDAP Type 2 only: Filter for LDAP data
Attributes	For LDAP Type 2 only: LDAP fields delivered
Result Limit	Result Limit for LDAP queries
Page Size	Page Size for LDAP queries
Use Active Directory	Usage of Active Directory
Use SSL	SSL usage
Verify Server Certificate	Should server certificate be verified?

NOTE:
The Integrated and FormBased authentication methods only work with the WebDAV Connection Type. Therefore, when using the Connection Type EWS, Authentication must be set to Basic or OAuth.

NOTE:
The authentication protocols supported are Kerberos, NTLM, and OAUTH. For more details about Kerberos Authentication, please verify item 6.4.9 of **OpenScape Concierge V4R2, Professional, Administrator Documentation**, and consult the respective documentation from Microsoft.

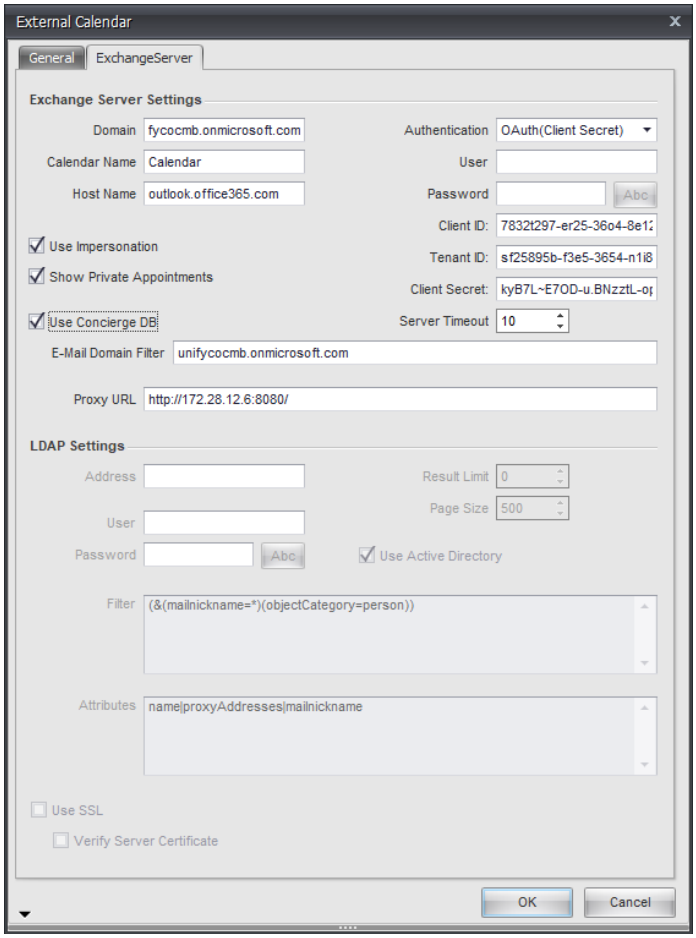
In case of LDAPS configuration, you have to make sure, that you enter the **port number into the Address field** and **tick the SSL checkbox.**

To use a different LDAP port than 389 (default), add the port number into the Address field using the address:port format (eg 127.0.0.0:3500).

If Use Concierge DB is activated the LDAP settings come from Concierge DB instead. Enter the E-Mail Domain Filter.

Office 365

Example for Office 365 integration:



If the "OAuth(User/Password)" authentication is selected, additionally to the user and password settings, the "Application (client) ID" and "Directory (tenant) ID" must be configured.

If the “OAuth(Client Secret)” authentication is selected the “Application (client) ID” , ”Directory (tenant) ID” and ”Client Secret” must be configured.

NOTE:

For Office 365 the parameter **Use Concierge DB** has to be activated and the fields **DomainFilter** and **ProxyURL** have to be filled in.

The “Application (client) ID”, ”Directory (tenant) ID” and ”Client Secret” could be obtained from the Microsoft Azure application registration portal.

OfflineDB

The corresponding parameter with OfflineDB can be configured under **Offline / DB** tab:

Variable	Description	Default
Offline / DB (MSSQL DB)		
DB Host Name	Database server name	

Variable	Description	Default
DB Name	Database name	
DB User Name	User name for the database	
DB Password	Encrypted password for the database	
DB Command TO	Max. duration for execution of database commands	30
Use CSV Importer	Use CSVImporter for offline data refresh	no
Source ID	Source Id for the offline data source	1
Ini CSV Importer	Configuration file for CSVImporter	
Date Time Format	Date and time format	yyyyMMdd HH:mm:ss

NOTE:
The CSV file of the customer is imported to the external MS SQL DB and read out by the Connector.
Scripts are available for creating the database with its tables, the INI file specifies where and when the database is read out.

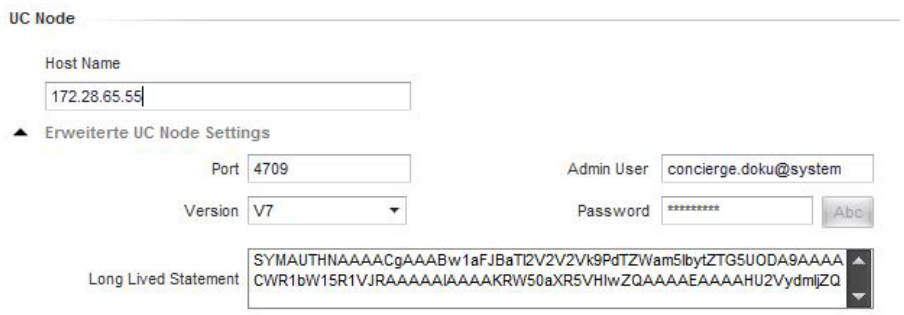
Thus two options are available:
1) the customer imports data to the database directly or …
2) the customer delivers the CSV file that is imported with the given importer tool. In this case the database parameters on the right side of the window are to be configured

For more information on External Calendar – see section 10 External Calendar Integration

6.3.1.5 UC Node

By activating **UnifiedCommunications** under **Presence Information**, a new area appears below for the connection parameters of UC integration that are configured as of the following table:

Parameter	Description
Host name	Host name or IP address of UC Server
Port	Port for access to UC Server **IMPORTANT**: This port has to be activated in OSV!
Version	Version the UC Node connects to. For all versions 7 or higher choose **V7**, for all versions up to V7 choose **≤ 6**
Admin User	User for accessing the UC system
Admin Password	Password for access to UC system
Long Lived Statement	Access key for UC server (to be generated on UC server as described in section 11.1.4 Permission-based preparations)



NOTE:
For Concierge accessing the UC server, a user account in UC is required. In a standard small UC deployment the account of the CMP administrator can be configured.
In a Very Large deployment this is not allowed. A new default user account has to be created / taken.

The new UC user must have a profile that supports UC functionality. An ONS number is not required. The credentials of that new user are then inserted in System Management in the fields **Admin User** and **Admin Password** as visible above!

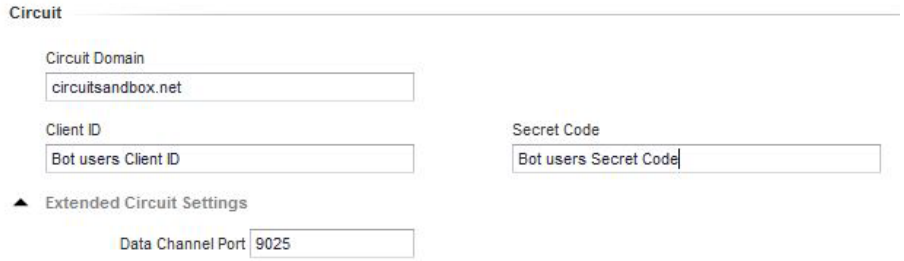
For a quick description how to create a new UC user please refer to in section 11.1.6.1 Creating a new OpenScape UC user.

For more information on UC – see section 11 UC, Circuit, Skype Or Microsoft Team Node for OpenScape Concierge

6.3.1.6 Circuit Node

By activating **Circuit** under **Presence Information**, a new area appears below for the connection parameters of Circuit integration that are configured as of the following table:

Parameter	Description
Circuit Domain	Name of Circuit domain e.g. eu.yourcircuit.com
Client ID	Bot users Client ID
Secret Code	Bot users Secret Code
Data Channel Port	Port number of the Circuit Data Channel communication between OS Concierge client and Circuit Node (default 9025)



NOTE:
For Concierge accessing the Circuit server, an OAuth 2.0 app credentials (bot user) in your Circuit domain such as eu.yourcirucuit.com is required. Please refer to section 11.2 Circuit Node.

6.3.1.7 Skype Node

By activating **Skype** under **Presence Information**, a new area appears below for the connection parameters of Circuit integration that are configured as of the following table:

Parameter	Description
Application Name	Name of Trusted Application on Skype for Business Server
User Agent	Name of the associated User Agent
Data Channel Port	Port number of the Skype Data Channel communication between OS Concierge client and Skype Node (default 9026)
Application Port	Port of the Trusted Application on Skype for Business Server

NOTE:
For Concierge accessing the Skype for Business server, the OSC Servers (Main and/or Standby) must be Skype for Business Trusted Application servers and member of one Trusted Application Pool.
Please also refer to 11.3 Skype Node.

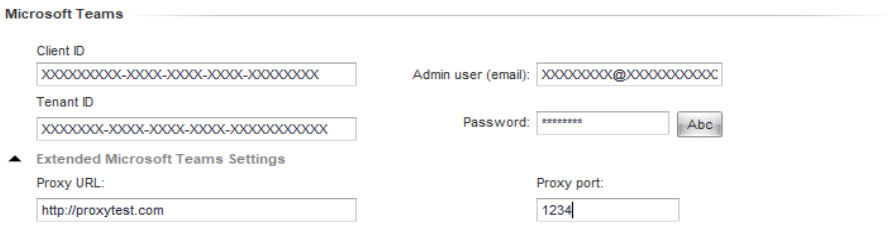
6.3.1.8 Teams Node

Activating the Microsoft Teams under Presence Information, a new area to fill the respective Microsoft Teams credentials will be displayed.

In the table below we can see their descriptions:

Parameter	Description
Client ID	Client or application ID generated on Microsoft Azure Portal
Tenant ID	Tenant id generated on Microsoft Azure Portal

Parameter	Description
Admin user (email)	Service user account configured as owner of the application in Microsoft Azure portal
Password	Password from the service user account configured



NOTE: For Concierge integration with Microsoft Teams, you must have an Application registered on Azure Portal with specific permissions and configurations. For more information: please refer to section 11.4 Teams Node

NOTE: To configure a proxy/port to connect to the API you can extend the Microsoft Teams Settings as the image above.

6.4 Saving the current design

Under “File → Save As” you can save the current design / configuration in System Management as an XML file and for backup purpose.

6.5 Publish installation data - activating the current design

To activate the current configuration in the system, data must be written on the main server machine’s database, press “**F5**” or “**Action** / **Publish Installation Data**”.

NOTE:
When the service **OpenScape Concierge** is started for the first time, an empty XML file is created to connect to when starting System Management. The file is named „*OscceService.Installation.xml*“.

All changes that are published with “F5” are then written into this XML file on the server.
!! Do not modify this XML file manually !!

6.6 Load and publish installation data…

In case you configured a configuration file with System Management in offline mode, you can load and publish this file via **Action** / **Load And Publish Installation Data…**

We recommend to wait a few minutes after loading the file to enable the system to save the file and then to restart the **OpenScape Concierge Service**.

6.7 Controlling deployment

In the following some basics are outlined that can be checked after the first configuration.

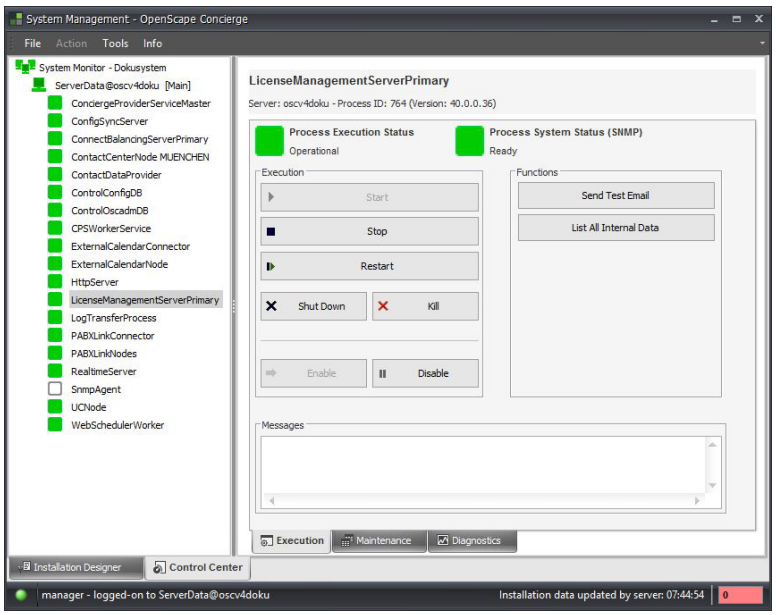
In System Management change the tab (left on the bottom of the GUI) to **Control Center.** It offers the possibility to control the processes, set debug levels and work on diagnostics. Watch the status of the system components in the left pane.

In the right pane there are three tabs: **Execution**, **Maintenance** and **Diagnostics**. These folders are helpful for monitoring the components’ status.

NOTE:
First time after the installation the server will start creating the databases on the specified database servers. This may take a while.

Left from a components or service a colored icon displays the status. For example one can see the “**ControlOscadmDB**” element that indicates the creation of tables for the OSCADM database which hosts the Electronic Telephone Book (ETB) data.

If everything comes up properly, the icons become green. Components that are not configured stay grey!



NOTE:
First time after a new installation, if the configuration is published, the **ConfigSync, ControlConfigDB, ControlOscadmDB** and **License-Management** will be started.
These processes must be up and running successfully to proceed. Check the green icon left from the processes. The system will not run, if one of these processes does not start up properly.

If it is not the case please check your **configuration parameter** (Server names, port numbers etc.) and publish again.

Please also check that all **server names are written in lower case letters**!

6.7.1 Control Center execution status of processes

The following exemplifies the view of the **PABXLinkConnector** that connects to all Function nodes in the system.

Go to tab **Control Center**, highlight **the PABX Link Connector** on the left; on the right pane change to **PABXLinkConnector's Maintenance** (tab on the bottom). Find the tab **Function Nodes List** on the right upper area and open this.

One can see the settings of multiple Function Nodes as well as their status. When the Function Node is active the LED becomes green.

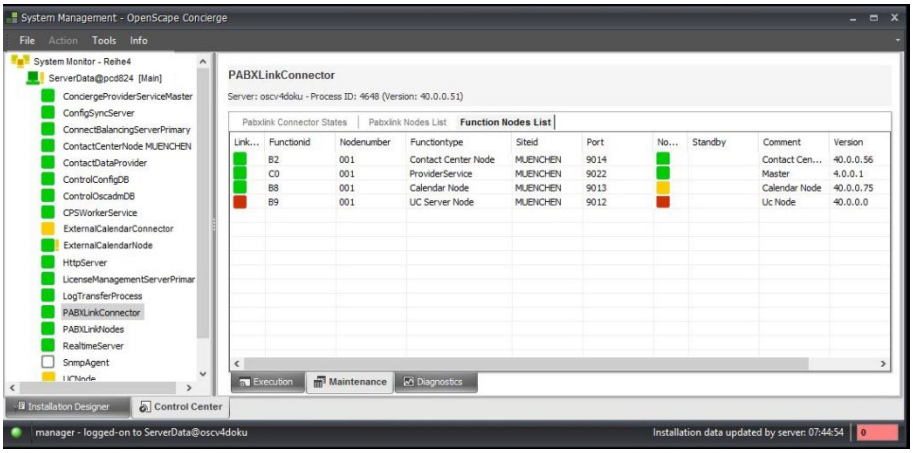


Table: Control Center execution status of processes

Symbol	Description
	Running and operational
	Running and limitedly operational
	Running with status “stopped”
	Closing
	Activated but not running
	Operational and deactivated (will not be started after a re-start of the OpenScape Concierge Service)
	Limitedly operational and deactivated
	Stopped and deactivated
	Not Running and deactivated

Table: Control Center SNMP status/functional status of processes

Symbol	Description
	Limited function
	No function

The exclamation mark will only be displayed in case the SNMP-status is “worse” than the execution status of the process.

NOTE:
In case the word “Debug” is displayed next to the process, the diagnose level is set to “Debug”. Please be aware that a large amount of diagnosis data will be saved now. This might limit the performance of the server. Please also make sure enough hard disk space is available!

6.8 System Management tool settings

When starting the System Management application the application settings are read from the ***SystemManagement.ini*** file in the installation folder and the user settings from the ***SystemManagement.user.ini*** file in the default folder *<dir>:\Users\User\AppData\Roaming\Unify\OpenScape Concierge\SystemManagement*

6.8.1 Application settings

The following table shows the required parameters of the application settings.

DO NOT change any setting unless Unify service staff advises you to do so.

Name	Description	Default Value
[ApplicationSettings]		
ApplicationIdleAutoExitInterval	Interval of inactivity in minutes, after which the application closes automatically	120
PabxAreaCodeRequired	Mandatory field in System Management – true or false	false
PabxAccessCodeNationalRequired	Mandatory field in System Management – true or false Enter **false** in case country doesn't use national access codes (i.e. Denmark).	true
PabxAccessCodeLocalRequired	Mandatory field in System Management – true or false	false
SiFileConnection	Connection data for SmartInspect file logging	file(append="true", filename="$FileNameSIL$", maxsize="10000", maxparts="10", rotate="daily", caption="SilFile")
SiPipeConnection	Connection data for SmartInspect console logging	pipe(pipename="smartinspect", caption="SilPipe", reconnect="true", reconnect.interval="1s")
ShowExceptionCounter	Runtime exceptions are shown in status bar	true
[ServerConfig]		
PrimaryHost	Network name of the primary Connect-Balancing server	*(Value is set during OSC Setup)*
PrimaryPort	Port number of the primary Connect-Balancing server	20001
SecondaryHost	Network name of the secondary Connect-Balancing server	*(Value is set during Setup – can be empty)*
SecondaryPort	Port number of the Connect-Balancing server	20001

6.8.2 User settings

The following table shows the required parameters of the user settings. The user individual settings are written into the personal user data folder when closing the application. The parameters with * can be set in System Management tool under Options.

Name	Description
[UserSettings]	
SaveSettingsDirectory *	Directory for saving settings data
BackupSettingsDirectory *	Directory for automatic backup of server installation data
MainWindowSize	Size of application window
MainWindowLocation	Position of application window
LanguageName	Code of GUI language under the terms of ISO 639-1 (DE or EN).
SettingsViewSplitterPosition	Horizontal position of the splitter in the view "Settings"
SetupsViewSplitterPosition	Horizontal position of the splitter in the view "Configuration"
MonitoringViewSplitterPosition	Horizontal position of the splitter in the view "Monitoring"
OnlineInstallationStandbyServer	Address of the Standby server – added during the installation – although it might not be available yet
ConfigurationSplitterPostion	Horizontal position of the configuration splitter

6.8.3 Command line parameter

The following table shows the parameter, which can be used as command line parameter on starting the application.

Each parameter has to be set in format /Name: Value.

Name	Description	Use	Value	Default value
multiple	Multiple application instances can be started	optional	true / false	false
delay	Delay of application start in seconds	optional	0..32768	0

7 Maintenance

7.1 Backup

For each OpenScape Concierge system, several databases can be used, depending on the applications in use and the deployment. The databases might run on the local OSC Server (*Main Server*) or on an external Database Server.

Furthermore the basic configuration settings that are created with the System Management are stored in an *XML file* on the Main Server.

NOTE:
After installation and basic configuration of the system it is recommended for the service engineer, to perform a first full backup of the system configuration and the databases.

A description how to perform a (first) single backup of the config file and the databases is described. Additionally some hints how a backup of multiple instances can be done.

7.1.1 Backup of *OscceService.Install.xml* file

The Configuration in System Management is stored in the *OscceService.Installation.xml* which is located in the installation folder, usually under *"C:\Program Files (x86)\OpenScape Concierge\config\runtime". In* this folder there are also backups of that file available.

NOTE:
Save this folder for a **complete backup of the configuration files**.

Remark: The current design / configuration can also be saved as an XML file in *System Management* and under "**File → Save As**" and choosing the corresponding path.

7.1.2 Database backup

For backing up the databases a ***.sql*** script (see below) is required that is started via a batch or command in the Windows Power Shell command line interface.

The script must be stored in the folder `C:\backup`; it backs up the data into the folder `C:\backup`.

7.1.2.1 *backup.sql* – example

The following example of a ***backup.sql*** script performs the SQL statements for backing up all databases of an OSC Server:

```
SELECT GETDATE();
GO
USE master;
GO
BACKUP DATABASE configDB TO DISK = 'c:\backup\configDB.bak' WITH INIT;
GO
BACKUP DATABASE OSCADM TO DISK = 'c:\backup\OSCADM.bak' WITH INIT;
GO
```

All various databases that might be available on the local server, like `configDB` or `OSCADM` are backed up one time in one instance.

A previously created backup will be overwritten.

→ Please ensure that this folder with the script is available before proceeding!

7.1.2.2 Starting the backup.sql manually

The backup.sql script can be started via the Power shell command line interface using the following statement:

If Sql Server Instance name is default (MSSQLSERVER):

sqlcmd -U sa -P <password of user SA> -S <ComputerName> -i "c:\backup\backup.sql" > "c:\backup\backup.log"

If Sql Server Instance name is other than default:

sqlcmd -U sa -P <password of user SA> -S <ComputerName>\<InstanceName> -i "c:\backup\backup.sql" > "c:\backup\backup.log"

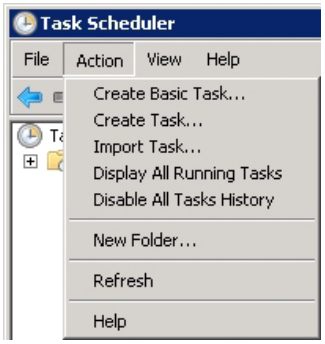
In the folder C:\backup a log file can be found after running the script.

NOTE:
Please ensure that the users involved (here User ***SA***) do have the necessary permissions to access the database and write down data into the `C:\backup` folder.

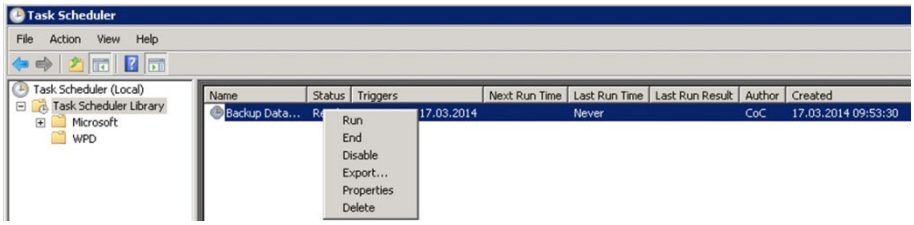
7.1.2.3 Scheduled backup

Create a command file, e.g. `back_me_up.cmd` containing the `Sqlcmd` statement above and create a scheduled task for the job.

1. Open the Task Scheduler under "**Start > Administrative Tools**".
2. Select **Action > Create Task** and use the "**`back_me_up.cmd`**".



3. Change the time when the Backup should start.
4. Change the user account which performs the export, but be sure that the user has enough rights on the Databases and the server.
5. After creation select the task with a right mouse click and run it.



Now all the Databases of the local SQL-Server should be exported to `c:\Backup`.

7.1.2.4 Modifying the backup parameters

NOTE:
The script above performs a database backup of all databases on the OSC Server (s); This should be done right on all involved servers after implementation of the system.
One instance of the backup is created.

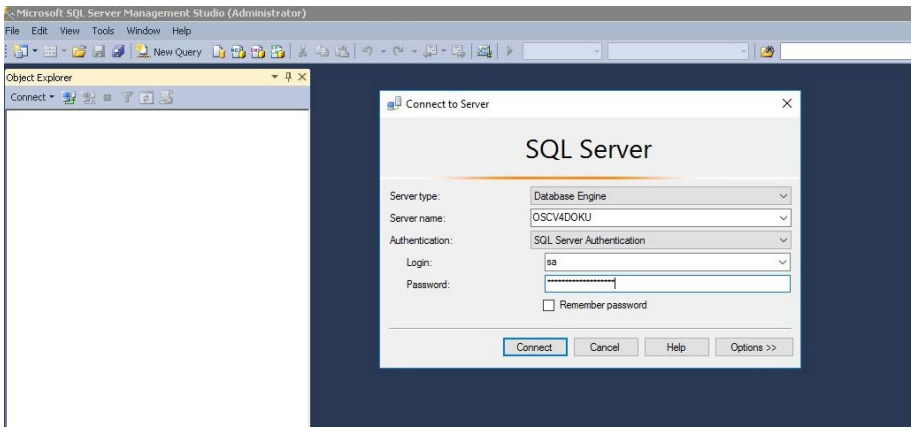
For backing up multiple versions of the databases, please modify the *backup.sql* file correspondingly.

NOTE:
Only personal skilled for MS SQL Server is recommended to modify the settings for the automatic backup!

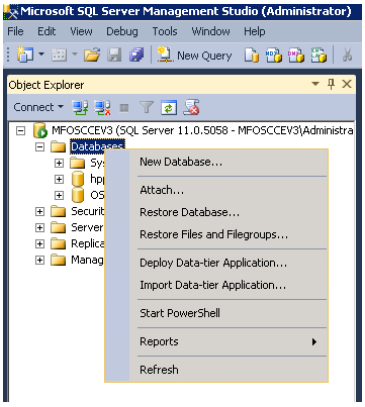
7.1.3 Restore database

The following steps show you how to restore the databases.

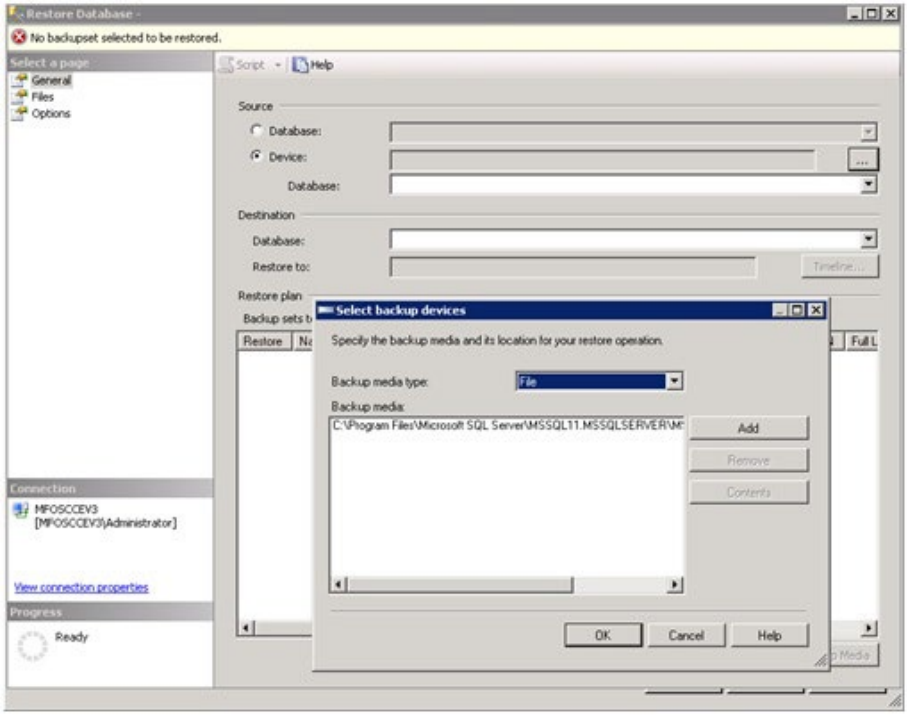
1. Stop the OpenScape Concierge Service on every OSC Server which is connected to the databases.
2. Open the SQL Server Management Studio.
3. Logon with a user that is configured as administrator in the System Management under Basics / Configuration Database, normally the ‘sa’ account.



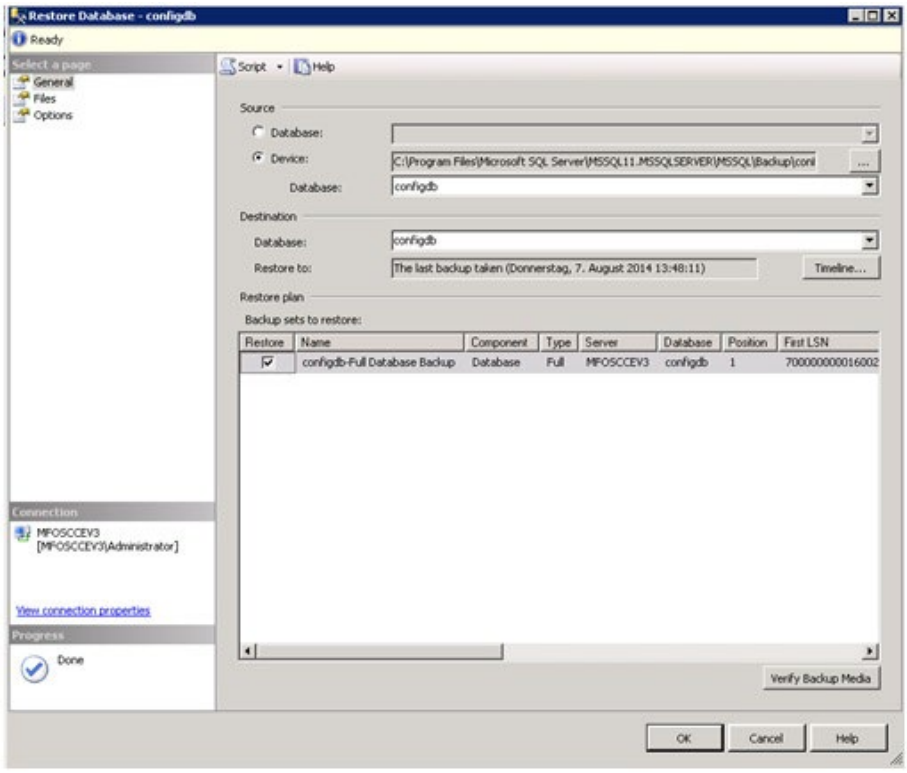
4. Open the Database tree view. With a right-click on **Databases** select **Restore Database**…



5. A new window opens. Select **Device** as Source and choose the backup file of the database which you want to be restored in the “Select Database devices” window.



6. Acknowledge with **OK** and the Destination Database will automatically be filled. If more than one restore set is stored in the backup file, select the appropriate.



7. Click **OK** and the restore process starts.
8. After the restore process has finished, click **OK** to finish the process.
9. Start the OpenScape Concierge Service on every stopped OSC Server again.

7.2 External SQL-Server for ConfigDB / OSCADM

The following describes the steps for OpenScape Concierge to use an external SQL Server. Two scenarios are described, one for using the external SQL Server right from the start implementation/installation the other when the deployment changes and an external SQL-Server is implemented then.

7.2.1 Implementing an external SQL server from start

1. Install the external Database server – see OpenScape Concierge, Server, Installation Guide.
2. Open System Management and enter the Database Configuration for an external SQL Server, see section 6.1.2 Configuration Database and OpenScape Concierge, Server, Installation Guide.

7.2.2 Moving ConfigDB / OSCADM to an external SQL Server

The following describes the steps for OpenScape Concierge that was installed with a local MSSQL-Express Database moving to the deployment with the Databases on external SQL Server.

NOTE:
Each user that accesses the MS SQL database requires a CAL (Client Access License).

Make sure you have the SA user password of standard OSC installation ready!

Procedure

1. Install the external Database server
2. Change in the System Manager the Database Configuration to the external SQL Server, see section 6.1.2 Configuration Database.
3. Apply the Change
   → the ControlConfigDB and or ControlOscadmDB process will restart and install the Databases and users on the new SQL Server.

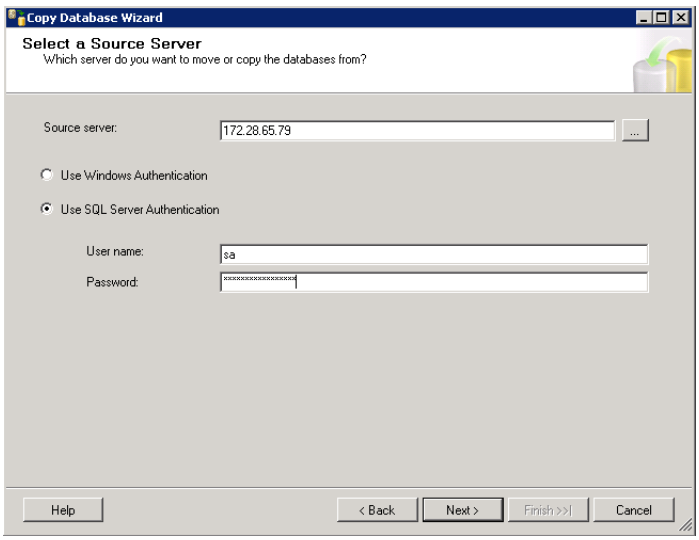
Procedure of migrating data to the external DB server

Follow the next steps for migrating data from the local SQL Express to the new database server:

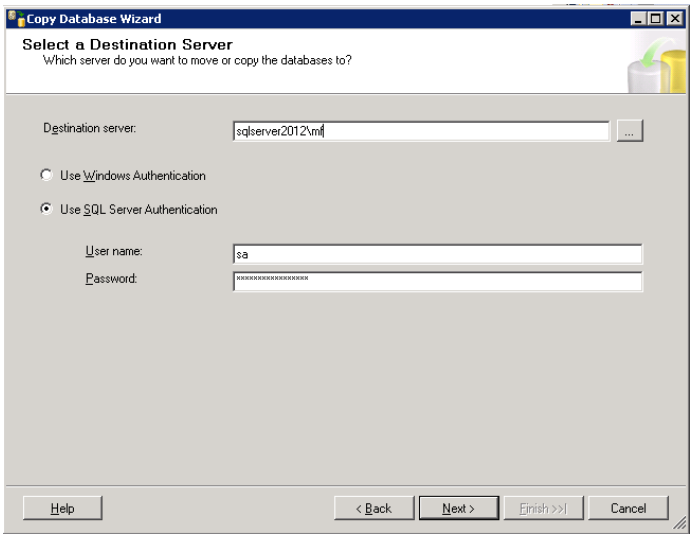
1. Stop **OpenScape Concierge Service** and all Clients connected to the source database.
2. Start the **Microsoft SQL Server Management Studio** on the destination server.
3. Right Mouse Click on the ConfigDB / OSCADM and select -> **Task** -> **Copy Database.**

The **Copy Database Wizard** starts.

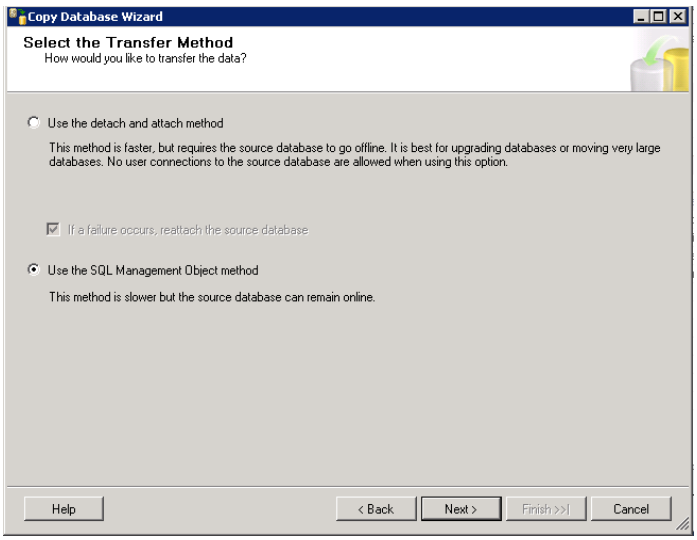
4. Press **Next>** for selecting the **Source server**.



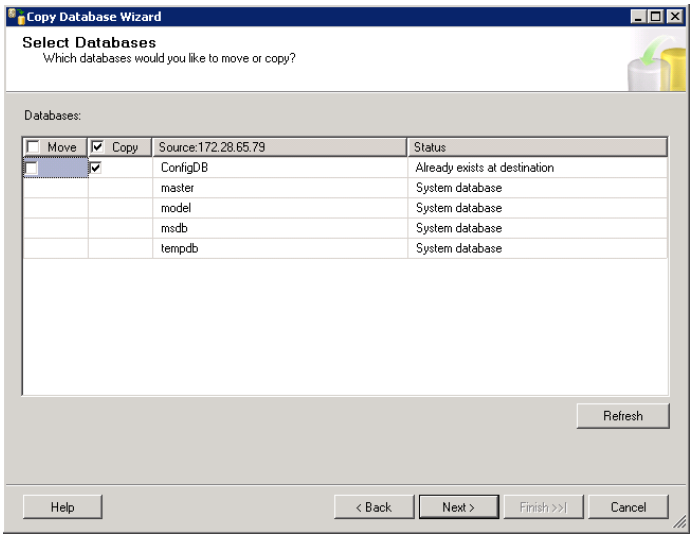
5. Enter the IP address of the OSC Server with the MS SQL Express database in the field **Source server**.
6. Specify the logon credentials, here User **SA.**
7. Press **Next>** for selecting the **Destination server**.



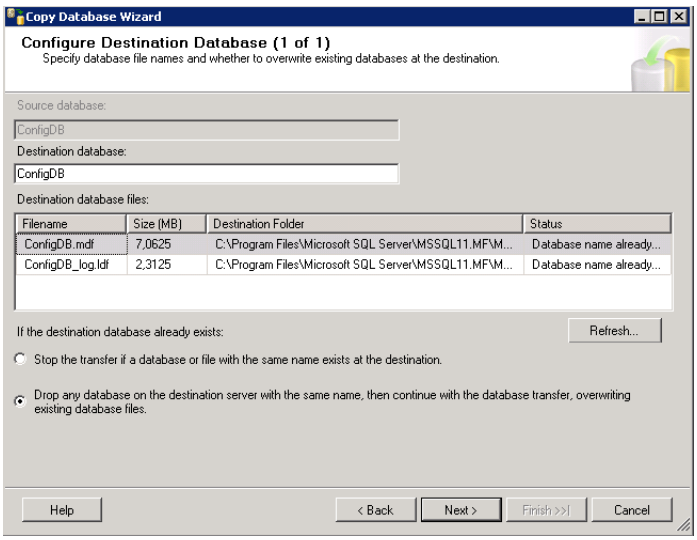
8. Enter name or IP address of the new Database Server with the MS SQL database in the field **Destination server**.
9. Specify the logon credentials, here User **SA**.
10. Press **Next>** for selecting the **Destination server**.



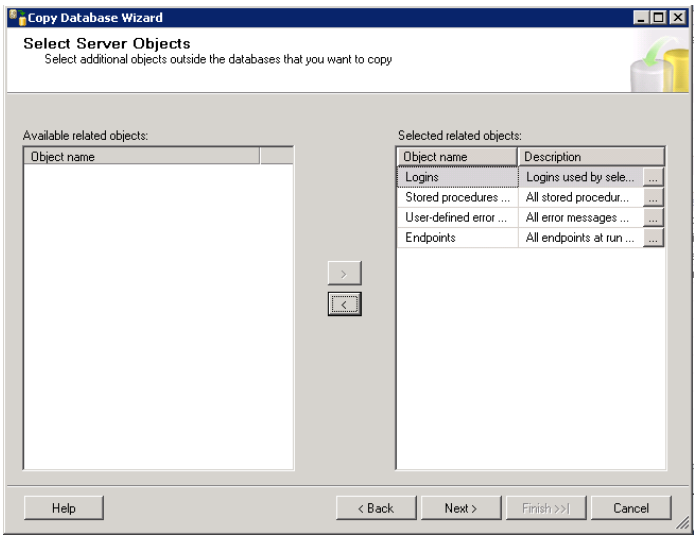
11. Select the option Use the SQO Management Object method
12. Press Next> for selecting the Databases.



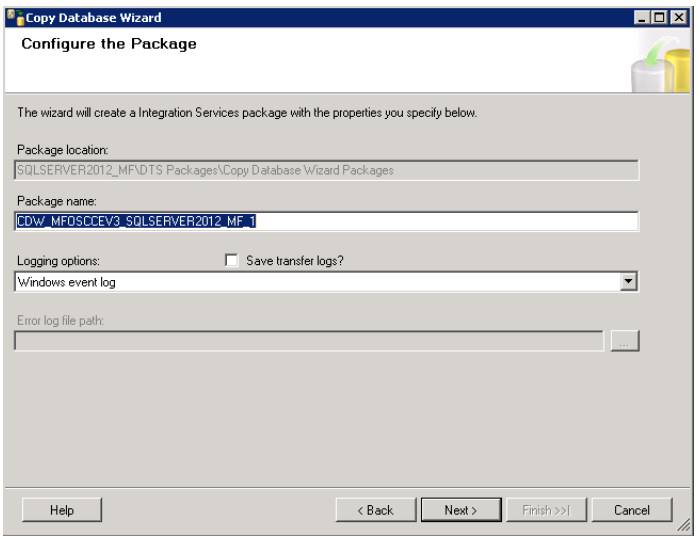
13. Choose **ConfigDB** and if using Concierge the **OSCADM** database.
14. Press **Next>** for **configuring the Destination Databases**.



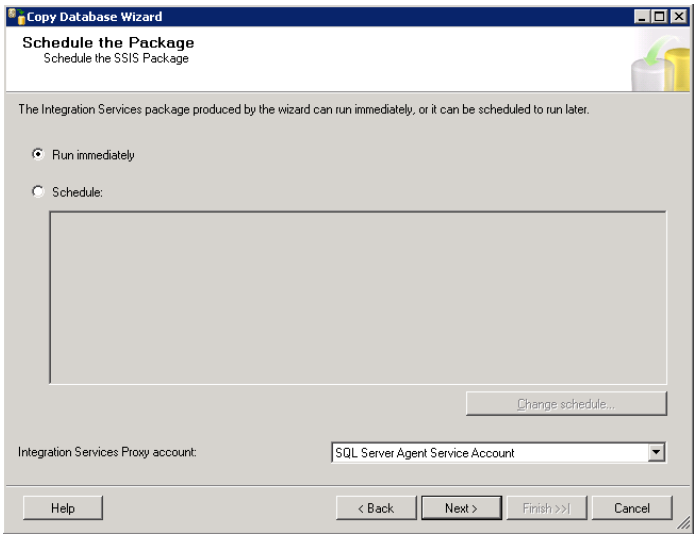
15. Check the option to **drop any database on the destination server** that has the same name…
16. Press **Next>** for **selecting the Server Objects**.



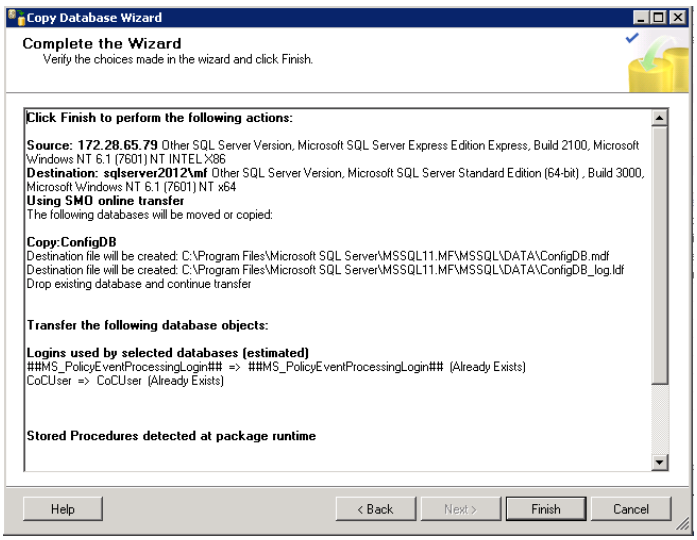
17. Select all available related objects on the left pane and move them to the right pane by pressing the button **[>].**
18. Press **Next>** for **configuring the package**.



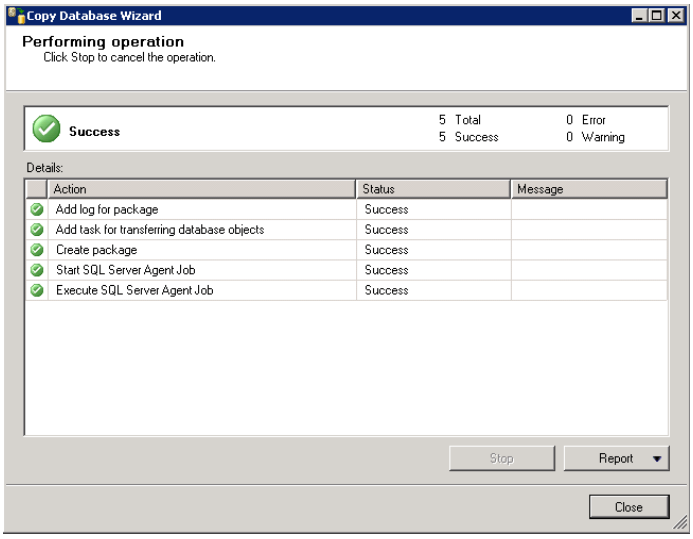
19. Give the package a meaningful name.
20. Press **Next>** for **scheduling the package**.



21. Select the option **Run immediately**.
22. Press **Next>** for **completing the wizard**.



23. Press **Finish** for performing the copy operations.
24. A control window opens. All operations should be successful.



25. Press **Close** for closing the wizard.
26. Start the **OpenScape Concierge Service** again when copying is finished. Log into the Systemmanagement and change the database settings to the destination Server for the corresponding databases

8 Basic Data Center configuration for Concierge

After setting the basic server data in **System Management** the Concierge Application has to be configured in Concierge **Data Center**.

8.1 Basic settings for quick startup

The following sections describe step by step the required settings for a basic deployment – the simplest deployment that allows the Concierge user to log on and handle a call.

For testing if the application is configured properly so far, running a first connectivity test with the Concierge Client GUI is described in section 8.11 Option: Arrange a basic test call.

NOTE:
Generally one can say, that Data Center is configured from top to bottom. Open the sections one by one and configure the settings you require.

8.2 Systemmanager access to Data Center

Click **OSCDataCenter** on the desktop, to start the OpenScape Concierge DataCenter application.

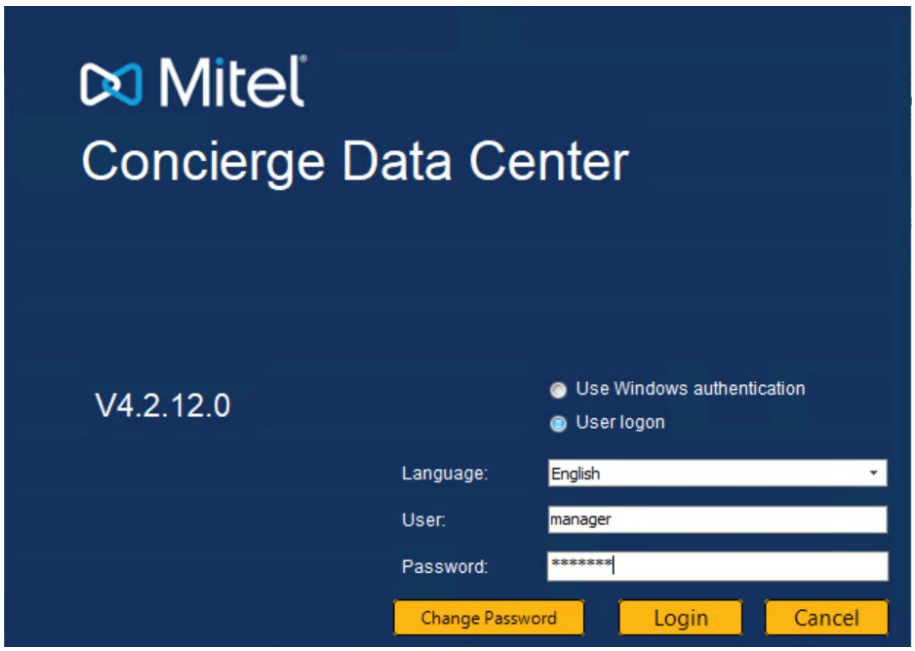
NOTE:
You also find a shortcut to Data Center under the **Start Menu** or double click the ***DataCenter.exe*** in the installation path under "\bin\Concierge\Concierge Management" like e.g. "`C:\Program Files (x86)\OpenScape Concierge\bin\Concierge \Concierge Management\DataCenter`".

Most basic settings are system wide and require the ***systemmanager*** *account,* other settings are done on a tenant's base and thus need the ***tenant's manager*** *account* to work in Data Center.

NOTE:
Data Center allows multiple instances to run on one PC at the same time. So settings can be done in parallel!

The **systemmanager** account is required for the first time an administrator logs on to the OpenScape Concierge DataCenter after installation.

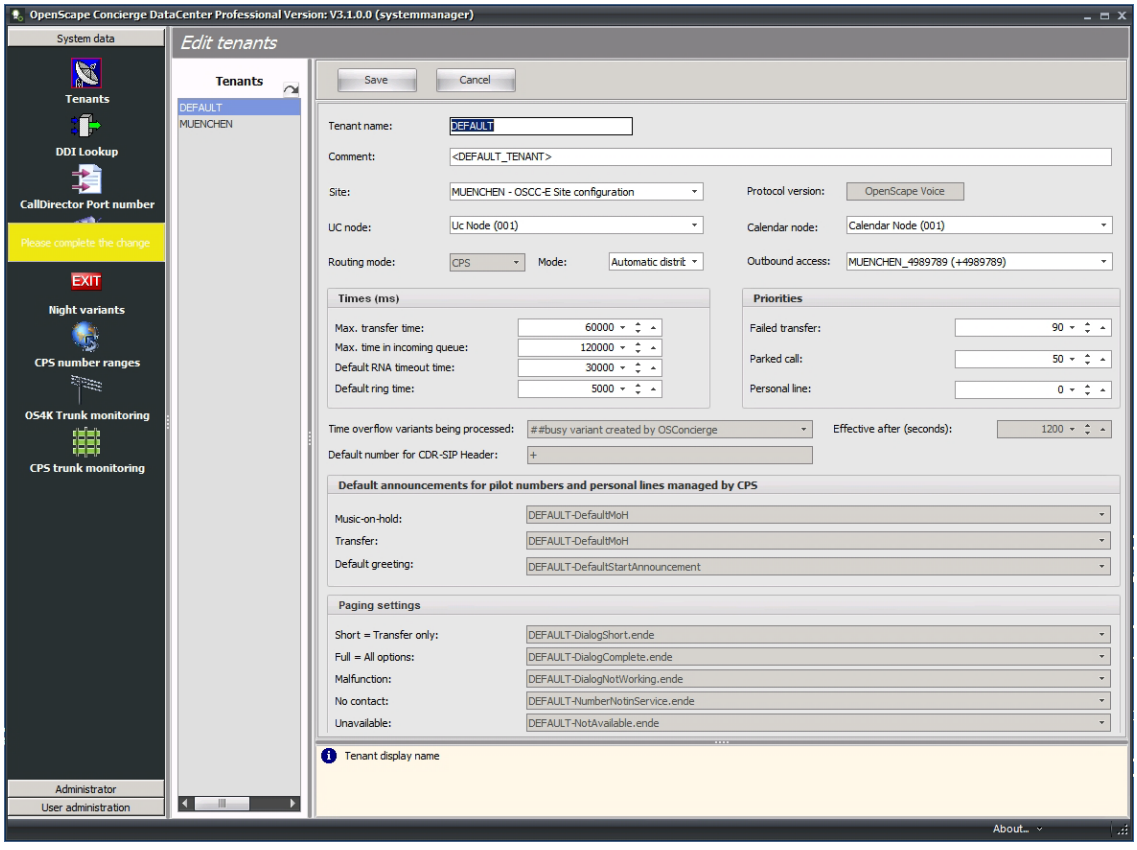
The default password "manager" can be changed with the menu behind the **Change password** button. Confirm the logon with the **Login** button.



After first log on to the system a message will appear that tenant data and site configuration in DDI lookup table is not configured yet. Acknowledge this with **OK** button!

8.3 System data / Tenants

The "Concierge DataCenter" window with the "System data" menu appears--
→ Press the **Tenants** button on the left.



During the installation a default tenant is created automatically. It is recommended to use this with the name DEFAULT if multi-tenancy is not required!

NOTE for Concierge Plus:
Only Concierge Professional allows configuration of more than one Tenant, usage of External Calendar, usage of OSCC node and Paging settings.

Default values are inserted for the tenant and should be updated as of the customer's environment.

The white fields can be modified by the Systemmanager user. The fields that are grayed out can be modified by the tenant's Manager user.

Press the **New** button in the upper line of the window to create new tenants if required.

Remarks: When creating a new tenant in the system, it automatically creates two new users for that tenant. A manager account named "<tenant name>\manager" and a user account named "<tenant name>\user".

8.3.1 Tenant's general settings

Tenant's general settings are the **Tenant name**, a **Comment** that is optional, the **Site** and the Number range.

Press the **Change** button to edit the fields.

NOTE: The **Tenant name**, the **Site** and **Outbound access** are mandatory fields to fill out, where site and outbound access are given by the settings in System Management.

UC, Circuit, Skype or Microsoft Teams node, Calendar Node (Professional only) and **Contact Center Node** (Professional only) can be activated if required.

Some options are determined by the settings in System Management and can be selected from dropdown menus where applicable.

Depending on selected **Presence Information** system entered in System Management / Concierge the function node selection option is labeled **UC node, Circuit node, Skype node or Microsoft Teams node** in **Tenants.**

NOTE:
The chosen **Presence Information** system is a system wide setting, relevant for all Tenants.

8.3.2 Routing Mode

The **Routing Mode** depends on whether OpenScape Contact Center is integrated or not: With OSCC the automatic routing of OSCC defines the call handling as well as time overflow variants and night variants.

Remark: Different Tenants can work with different Routing Modes.

Without OSCC node the type of routing is defined by CPS.

The type of routing (**Art**) is independent of the Routing Mode and allows

- Automatic distribution
- Only pick mode

NOTE:
The integrated automatic distribution of CPS is based on the configuration of DDI Lookup entries, User Accounts and Groups, Supergroups (Professional only) as explained in the appropriate OpenScape Concierge, Administrator documentation .

Time overflow variants

The **Night variants** with its timer settings can be selected depending on the settings in the Night variants menu described below.

8.3.3 Times

In the area **Times** you modify the default values for the times for the Concierge user / application handling the customer calls – the unit is milliseconds.

Max. transfer time defines how long the system tries to reach the target person the call has been transferred to.

If this threshold is exceeded in a call transfer scenario, the call will stay in the „Processing Queue“ window in the Concierge GUI; the status in the GUI changes the target person is no more called.

Max. time in incoming queue describes the time the system will hold the call to wait for agents answering before the call is routed to the specified *Time Overflow variant*.

This tenant’s time value and the time overflow variant can be overwritten on a DDI lookup entry base.

Default RNA timeout time is the maximum time a call from CPS is ringing on the Concierge user’s phone. If that time is exceeded before the attendant accepts the call, CPS takes that call away from that user and puts the user’s routing state into “unavailable”. The call will be routed to another available attendant.

Default ring time defines the time the caller hears the ring tone until the call is connected by the Concierge / CPS system.
For cost free services adjust the times with this parameter!

NOTE: The tenant’s times values act as default values for that tenant; the values can be overwritten for each DDI lookup entry individually.

8.3.4 Priorities

Right besides the Times pane Priorities can be configured for different types of calls. A priority of a call describes its importance in terms of the order of visibility in the Caller queue and ACD distribution.

These settings are overwritten by the tenant’s manager account and described below.

Paging settings

These settings are configured with the tenant's manager account.

Default announcements for pilot numbers and personal lines managed by CPS

These settings are configured with the tenant's manager account.

8.4 System data / DDI Lookup

In the next step the DDI lookup table entry has to be created on system manager's level. There are different settings to care about depending on the communication platform type and whether the system integrates with OpenScape Contact Center or not.

NOTE:
In sections
4.4.6 DDI Lookup entry example for OSV without OSCC
5.4.8 DDI Lookup entry example for OS4000 without OSCC
5.5.4 DDI Lookup entry example for OS4000 with OSCC
are descriptions of pilot number settings in the PABX with the corresponding settings in the DDI lookup table depending on the integration with OSCC or not.

Please refer to these sections for details on the available pilot number configurations!

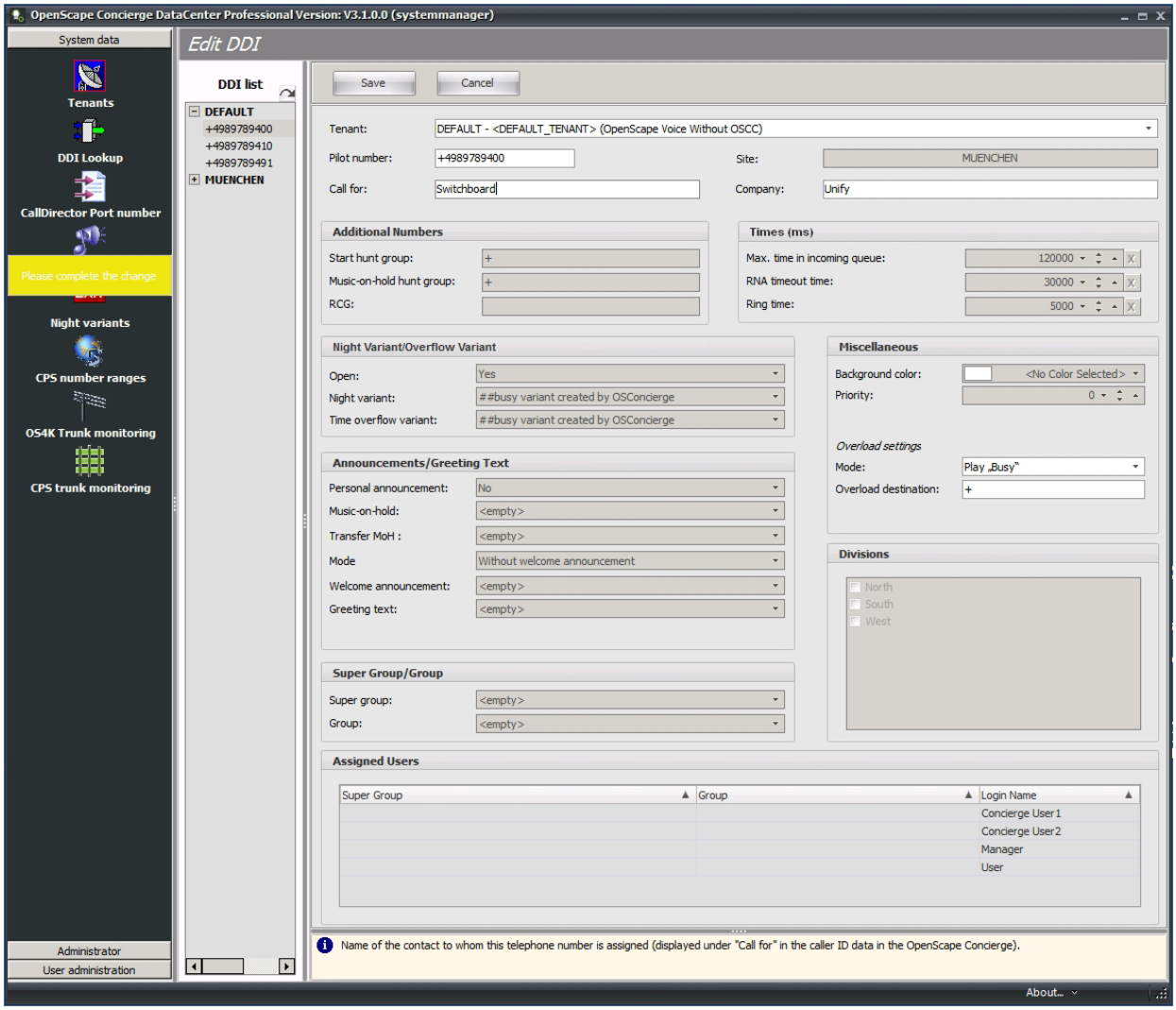
Procedure

1. Press the New button in the **Edit DDI** window to create a new entry for a pilot number (the number that the customer dials to reach the attendant - also known as Service Number or DDI).
2. Choose the tenant from the dropdown list.
3. Enter the Pilot number in full E164 format including the "+" in front
4. Insert purpose of this pilot number (Main, Internal, Call Forwarding, etc) and the company's name.
5. In case OSCC integrates and OSV is used the start hunt group (HG), also known as initial hunt group and MoH hunt group have to be specified under Additional Numbers.
   When using OpenScape 4000 the RCG number behind the pilot number's DNIT needs to be inserted for monitoring purpose!
6. Under **Miscellaneous** the Overload can be defined in case CPS is overloaded, means the SIP trunk does not provide free "processing channels" anymore. The caller can hear the busy tone or the call can be routed to an overflow destination, please see also section 6.3 Section Applications.

Repeat that procedure for all required service numbers!

NOTE:
The number of OSCC DDIs is limited to 1000 entries.

for Concierge Plus:
The number of DDIs is limited to 6 for Concierge Plus.



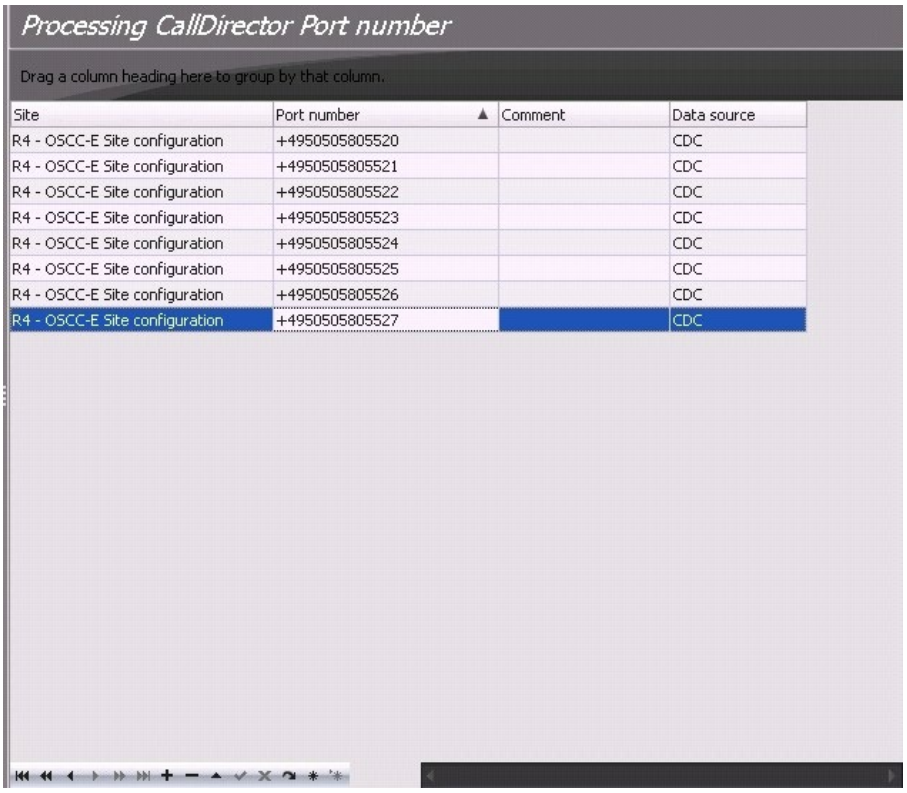
Additional pilot numbers for further services numbers can be created if required!

NOTE:
Some fields in the DDI Lookup entry are grey as the Data Center is started with the *systemmanager* account. These values can be defined in using the Tenant's Manager account.

For Concierge Plus:
Super Group/ Group and Divisions section is only available with Concierge Professional

8.5 System data / Call Director Port number (with Professional and OSCC only)

For properly monitoring calls that are handled by Call Director's voice processor this table needs to have all of these ports configured in the PABX!

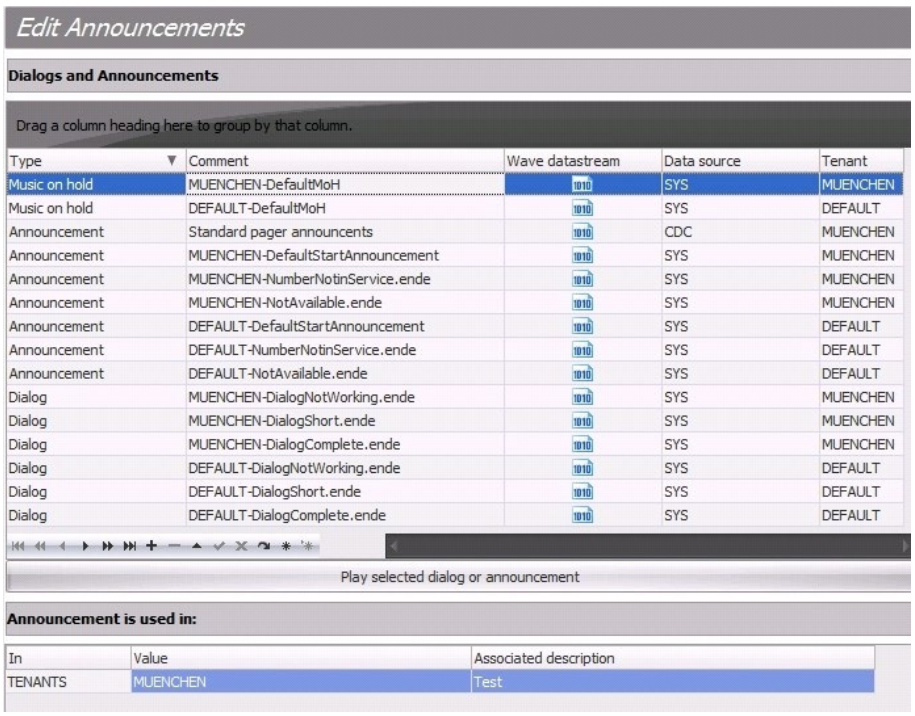


Configure the location, where the Call Director SIP service resides and the Port number or extension number of all Call Director ports in OSCC - the values must match those configured in OSCC Telephony Center.

8.6 System data / Announcements

For using an announcement / wave file with Concierge it has to be previously registered in Data Center. This can be done under System data, section **Announcements**. There the **Edit Announcements** window shows all wave files that are registered in Concierge Data Center.

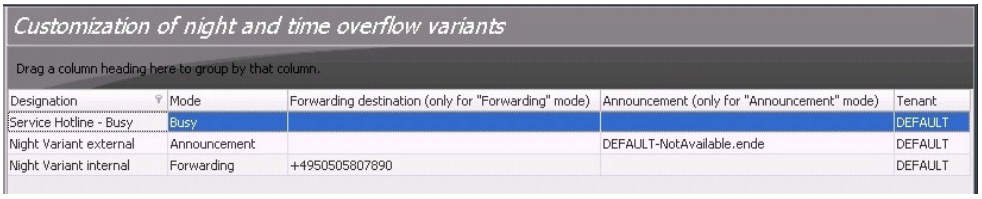
For detailed description please refer to appropriate OpenScape Concierge, Administrator documentation.



8.7 System data / Night Variants

Night variants and **overflow variants** define the options available for handling an incoming call in case no attendant or not enough attendants are available for handling an incoming call or if the service number is closed.

Configure night variants and time overflow variants under **System data** button **Night Variants**.



Three modes of night variants or time overflow variants can be configured:

1. **Mode Busy:** A busy signal is played to the caller
2. **Mode Announcement:** An announcement telling that no attendant is available is played to the caller
3. **Mode Forwarding:** The call will be forwarded to an extension number, which can handle the call with an answering machine or an overflow hotline.

Procedure

1. Use the + button on the bottom line to create a new entry. Specify a designation. Choose a mode as described above.
2. In case the mode *Forwarding* is used, configure the forwarding destination.
3. In case the mode *Announcement* is used, choose an Announcement from the dropdown list.
4. Assign the tenant's name.

NOTE:
For detailed description please refer to appropriate OpenScape Concierge, Administrator documentation.

8.8 System data / CPS number ranges

The Concierge Provider Service (CPS) is the central application of Concierge for handling and controlling calls.

Without OSCC integration all incoming calls are handled by CPS.

If calls are put on hold or parked, they are connected back to CPS that keeps them locally until further handling is required.

CPS is connected to the PABX as a SIP endpoint using a SIP trunk connection.

As CPS number ranges are handled quite differently with Concierge Professional and with Concierge Plus it is recommended to read following sections:

For OSV only:

4.4.2.1 Formula for estimating the number range of internal CPS resources for details on the size of the corresponding ranges.

For OS4000 only:

5.4.1.1 Formula for estimating the number range of internal CPS resources

And for information on configuration:

Appropriate OpenScape Concierge, Administrator documentation under section CPS number ranges.

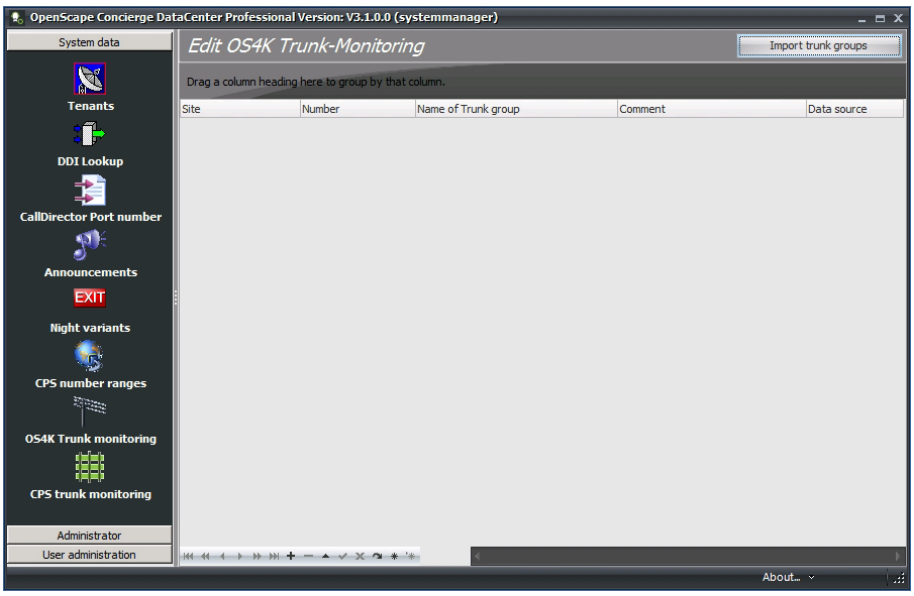
8.9 System data / OS4K Trunk monitoring table (with OS 4000 only)

Only the *systemmanager* is authorized to create or delete entries in this dialog.

Description

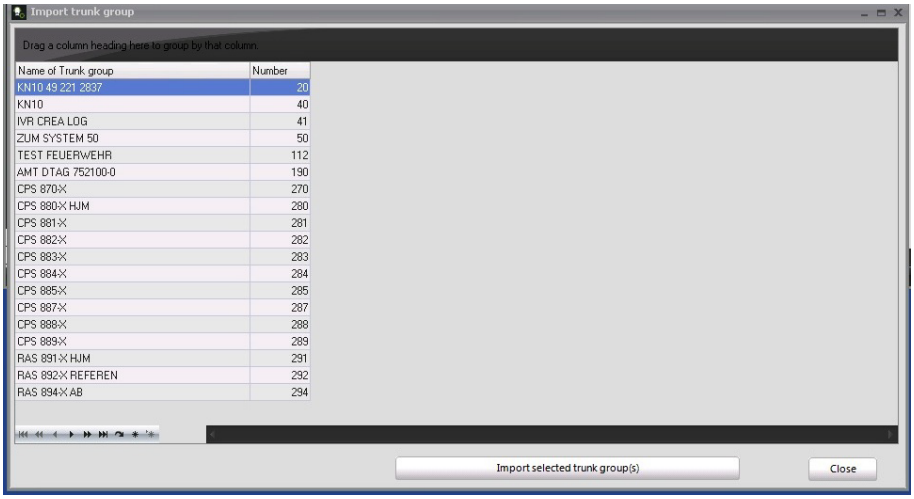
In case of integration with OS4000 the trunks of the OS4000 have to be monitored in order to correctly receive all information about a call even in complex call scenarios.

Multiple call number ranges for several locations (sites) can be defined.



Procedure

1. Click on **Import Trunk groups** button – a new windows opens.
2. Select the trunk groups you want to import from the list.
   The data is read via the ConfigSync Service from the switch and saved in the ConfigDB (PabxTrunkgroups table).
   The CPS takes up the trunk group configuration and learns during runtime the corresponding Loden for monitoring.
   In case the Loden change they will be updated via the daily ConfigSync.
   The selected trunk groups only have to be modified manually in case the OS4K trunk groups change, e.g. assebly units were added or removed.
3. Click on the **Import selected trunk goups** to show them in the OS4K Trunk Monitoring window



NOTE:
Only trained staff should configure the OpenScape/ OS4000 and adopt the configuration to the customer's environment.

Table: Data fields

Column	Description
Site	Name of the site for which the call number range is defined.
From	Begin of the trunk number range for the defined site.
To	End of the trunk number range for the defined site.
Comment	Input field for comments
Datasource	CDC stands for the data source OpenScape Concierge DataCenter or CDI for the automatically imported data from the Data Importer data source.

NOTE:
Review your trunk number configuration, when the OS4K was newly generated due to a patch for example. Also review your trunk number configuration, when new trunk groups were added or deleted.

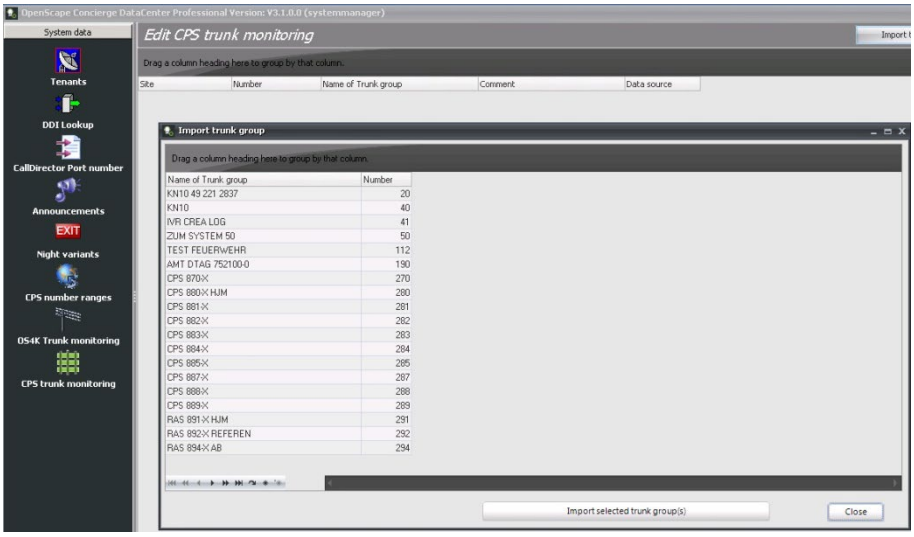
8.10 System data / CPS Trunk Monitoring (with OS4000 only)

Only the *systemmanager* is authorized to create or delete entries in this dialog.

In case of using IP / SIP trunks with OpenScape 4000 the CPS trunks have to be monitored similar to the OS4K trunks described above.

Procedure

1. Click on **Import Trunk groups** button – a new windows opens.
2. Select the trunk groups you want to import from the list.
   The data is read via the ConfigSync Service from the switch and saved in the ConfigDB (PabxTrunkgroups table).
   The CPS takes up the trunk group configuration and learns during runtime the corresponding Loden for monitoring.
   In case the Loden change they will be updated via the daily ConfigSync.
   The selected trunk groups only have to be modified manually in case the CPS trunk groups change, e.g. assebly units were added or removed.
3. Click on the **Import selected trunk goups** to show them in the CPSTrunk Monitoring window



NOTE:
Only trained staff should configure the OpenScape 4000 and adopt the configuration to the customer's environment.

Table: Data fields

Column	Description
Site	Name of the site for which the call number range is defined.
From	Begin of the trunk number range for the defined site.
To	End of the trunk number range for the defined site.
Comment	Input field for comments
Datasource	Data source of the configured values

NOTE:
Review your trunk number configuration, when the OS4K was newly generated due to a patch for example.

8.11 Option: Arrange a basic test call

The settings that have been configured up to now are minimum settings for running basic deployment of a Concierge system. Thus a first test with a basic call for checking the application and its connection can be performed here.

PABX settings

Be sure that the configuration in the communication platform and –if used– in OpenScape Contact Center is done. Verify, that the pilot number calls are routed to CPS (without OSCC) or to the hunt groups as required by OSCC.

Start Concierge Client

Find the ***Concierge.exe*** in the installation path under "\bin\Concierge" like e.g. "*C:\Program Files (x86)\OpenScape Concierge\bin\Concierge*" and double click it.

Logon without OpenScape Contact Center

Without OpenScape Contact Center Integration log on to the Concierge Client GUI by entering the tenant's name "default", a dropdown list then appears with the default "user" and the password "user".

Logon with OpenScape Contact Center integration

With OpenScape Contact Center integration the Concierge's user accounts must match the OSCC agent's users. This is done in Concierge Data Center:

1. Logon with the tenant's manager account (e.g. "DEFAULT\manager") and the password "manager" to Data Center
2. Change to the area "User administration" and press the Accounts button. The User Accounts list appears.
3. Press the button **OSCC agents import dialog.**
   A list of business units and users in OSCC appears
4. Select the users that you want to synchronize from OSCC to your tenant's database.

Log on to the Concierge Client GUI with one of the user accounts by entering the tenant's name. A dropdown list then appears with the corresponding users just synchronized.
The password of the OSCC users will not be synchronized. It is managed in Concierge Data Center.

Perform a basic test call

Verify that the Concierge user is in the **Available** state.

From a second phone device dial the main line's phone number and find the incoming call in the Concierge's caller queue.

Without OSCC: it depends on the tenant's type of routing (manually picking or automatically routing) how to handle it with the Concierge client application. Per default the automatic routing by CPS is enabled.

With OpenScape Contact Center the calls are be routed automatically to the attendant's phone.

9 Further procedure

In order to configure Concierge Client and Concierge Management applications – continue with:

OpenScape Concierge Plus, Administrator documentation

or

OpenScape Concierge Professional, Administrator documentation.

10 External Calendar Integration

General information

Concierge uses an account to access the external calendar system and requests the calendar entries of the contacts of interest. In the following sections this account has the name “extcal”. It is described, which type of access (WebDAV / EWS) and permissions this account needs on the different MS Exchange system to gather the required information.

The linking element between the contact in Electronic Telephone Book (ETB) and the external calendar system is the email address of a contact.

Thus a successful integration will only work if the contacts in ETB do have the email address in their availabilities that is also used to refer to the user in the external calendar system.

NOTE:
The following sections describe settings in Microsoft Exchange Server and should only be customized and conducted by trained service personnel e.g. MS Exchange administrators.
The descriptions and configuration settings are not meant to be carried out by people who are not skilled in MS Exchange Server administration.

10.1 Exchange 2010, 2013, 2016 and Office 365 via EWS

Prerequisites:

- The User ***extcal*** in Exchange2010, 2013, 2016 or in Office 365 respectively with the corresponding permissions is required (see below).
- A LDAP user (AD) is required with permission to readout the Exchange Alias.
- The OSC license must include the External Calendar Connector.
- The email address in the OpenScape Concierge Database for the identification of the user in Exchange must be unique.

Remarks to EWS

EWS (Exchange Web Services) is used to link the ExternalCalendar-Connector with the Exchange Server and this way EWS allows OpenScape Concierge access to the MS Exchange Calendar.

Test the EWS connection by entering the following URL in a browser session on the OSC server:

“https://<exchange-svr>/EWS/Exchange.asmx”

where <exchange-svr> is the name of the MS Exchange server machine.

Note that the server name must be resolved on the OSC Server.

The test link for Office 365 is as follows:

https://outlook.office365.com/ews/Exchange.asmx

Enter the credentials of the user ***extcal***.

NOTE:
For Office 365 enter the user name with the domain name. (i.e. extcal@unifycoc.onmicrosoft.com)

As a result of a successful connection the Exchange server replies with a ***Service*** / ***Services*** web page. This can either be an XML file which describes the types of messages that are supported or a web page that

confirms that that a new service has been created, depending on the configuration.

Most important is that the authentication process with the user ***extcal*** succeeds.

NOTE:
LDAP access can be tested using a LDAP-Browser, like e.g. the Softerrra LDAP browser available under http://www.ldapbrowser.com

---

Overview

A domain user account, here the user ***extcal*** (as described above) must be created.

IMPORTANT:
The following requirements apply only if the appointment details should be displayed. Therefore it is suggested to clarify the customer needs before preparing Exchange system for the integration.

This user account must be granted the „Impersonation“ permission which allows the user to act with the rights of another user in the system – for example to access the calendar information of another user.

10.2 Integration Exchange Server via EWS

Prerequisites

A domain user account, here the user ***extcal*** (as described above) must be created. This user account must be granted the „Impersonation“ permission which allows the user to act with the rights of another user in the system – for example to access the calendar information of another user.

NOTE:
Please check that the „Impersonation“ user has a valid Mail ID (like e.g. ***extcal***@<domain>) in the AD/LDAP directory.

For detailed information please check the following internet sources:

https://www.codetwo.com/kb/how-to-set-impersonation-rights-manually/

https://blog.westmonroepartners.com/application-impersonation-and-ews-with-3rd-party-applications-in-office-365/

https://eightwone.com/2014/08/13/application-impersonation-to-be-or-pretend-to-be/

https://help.salesforce.com/articleView?id=000212263&type=1

10.2.1 Setting the Impersonation Permission

With the Exchange Management Shell (EMS) two scripts can run to assign the „Impersonation“ permission to the user ***extcal*** as well as to define the scope to which the impersonation permission applies.

Assign the Impersonation permission to a specific user (*extcal*):

new-ManagementRoleAssignment

-Name:_suImpersonateRoleAsg

-Role:ApplicationImpersonation -User: extcal@<domain>

(Here ***extcal*** is the domain user and extcal@<domain> the Email address of it)

Define the scope to which the impersonation permissions apply.

new-ManagementScope

-Name:_suImpersonateScope

-ServerList: <exchange-svr>

(Here access is allowed to the whole server system <exchange-svr>)

10.2.1.1 Verification of the settings

Using the Exchange Management Shell (EMS) the configuration of permissions can be checked (open the shell):

- Get-ManagementRoleAssignment -Role ApplicationImpersonation

Verify, that the Command output indicates role assignments with the Role „ApplicationImpersonation“ for the account ***extcal***:

```
_suImpersonateRoleAsg | ApplicationImpersonation |
extcal | User | Direct | extcal
```

Use the command

- Get-ManagementScope _suImpersonateScope

for verifying that the Management scope that applies to the ***extcal*** account is correct, the following information should be displayed:

```
_suImpersonateScope | ServerScope | False |
|          | DistinguishedName
```

10.3 Remarks to the offline connection

The Offline connection is used for connecting the ExternalCalendar Connector with calendar systems that do not allow an online query to the calendar information of users.

The corresponding data has to be delivered in a specified CSV format from the customer.

Use a batch process for importing this information once a day into an external database which then can be accessed from the ExternalCalendar Connector.

Procedure

- Calendar data from an arbitrary system has to be delivered as CSV file in the specified structure.
  An example for a csv file with calendar information can be found on the OpenScape Concierge DVD under
  Tools\ExternalCalendarConnector\appointment Test.csv
- An SQL script is delivered with all components required for creating a database to run the CSV import. The customer has to deliver the SQL database server.
  The required script ***Create Database Appointments V1_1 with Tables.sql*** is also on the OpenScape Concierge DVD under *Tools\ExternalCalendarConnector.* **NOTE:** You might have to amend the path to MDF and LDF file within the script!

In case a database had already been created in advanced, use the script ***Create Tables Appointments V1_1.sql*** in the same directory on the DVD to create the tables only.

- A database user with the corresponding permissions is required (see below).

10.4 Remarks to LDAPS Configuration

Please make sure that you enter the port number into the Address field and tick the SSL checkbox – see section 6.3.1.4 External Calendar Connector (Professional only).

The correct parameter for the LDAP server can be easily obtained, when configuring an example syncjob in DataCenter / ContactDataProvider and test the source parameters.

10.5 Multiple External Calendar Connector Configuration

NOTE: a maximum of 10 external calendars can be configured.

Before configuring connections to multiple external calendar systems (e.g. multiple Exchange Server), please consider the following requirements:

- Depending on the calendar system subscriber volume, the RAM requirements of the server hardware needs to be validated. **ExternalCalendarConnector** keeps all the email aliases returned by the configured LDAP-Filter in the memory. In order not to affect the system performance, a validation of subscriber volume check and available RAM space check have to be done before configuring multiple connections
  In case of not having enough resources in the server, architectural changes should be considered. (e.g. installing additional **ExternalCalendarConnector** on a separate server hardware).
- Each external calendar system (e.g. Exchange Server) has to be pre-configured according to requirements mentioned in the previous sections of this chapter.
- Each external calendar system (e.g. Exchange Server, Office365) must have a unique domain.
- Connection data for each system should be provided by the customer (e.g. server names, access information).

10.6 Check External Calendar node

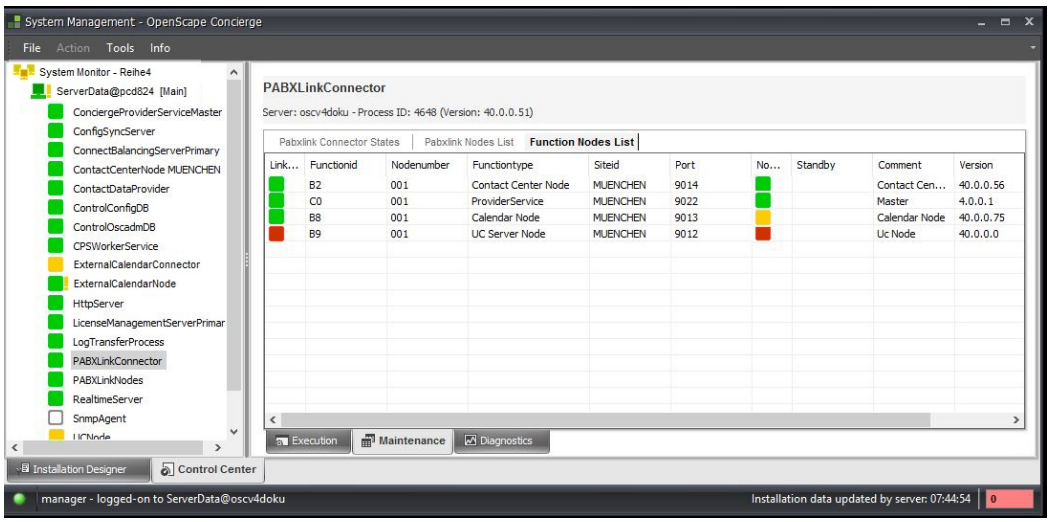
A further function node should be checked in the PABX Link Connector's Function Node List:

Go to **System Management \ Tab Control Center**. Highlight **the PABX Link Connector** on the left; on the right pane change to PABXLinkConnector's **Maintenance** (tab on the bottom). Find the tab **Function Nodes List** on the right upper area and open this.

If the configuration has been successful the PABX Link Connector recognizes the new Node and the Node becomes active after a while.

In case it does not become active, the CoC PABXLinkConnector Service should be restarted.

When the Function Node is active (LED is green) the Exchange Service can also be started.



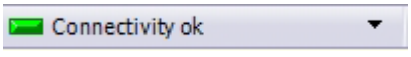
The following parameters should be configured there:

Table: Parameters External Calendar Node

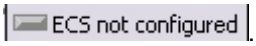
Field	Description	Value
FunctionID	Unique Function Node ID (B0 – BF)	B8
Node Number	Number of Node	00n
SiteID	Site ID assigned to the function node (Master Side ID	As of System Management
TCP/IP Port	Port no. for connecting the Function Node with the Connector.	9013
Comment	Description of the Node	

10.7 Monitoring success

To verify the correct configuration of the connection parameters and to display the present connection status the OpenScape Concierge application shows the status of the respective connection partner in the status bar.



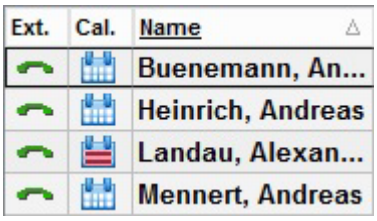
When the status display for the External Calendar Server is „gray“ it is not configured.



When the LED is green and shows **ok** the connection to the Exchange Server is established.

10.7.1 Tabular display in contact search

The search result is displayed in table form. The calendar (absence or presence), the status of the phone, optional the UC, Circuit, Skype or Microsoft Teams presence status as well as the name and other parameters are displayed for every contact the search result matches.



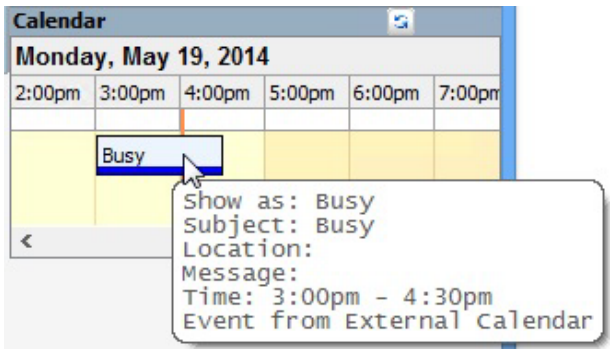
Calendar view: The Calendar view indicates the current absent information in the Calendar. If there is a current absence entry it the symbol is “red”.

 . The view does not refresh automatically.

10.7.2 Detail view for selected contacts - Calendar

A coupling with an Exchange Server allows displaying the calendar entries in the detail view of a selected contact if he/she can be identified by the email address.

Depending on the settings of the client configuration and on the authorization in Exchange either the absence / presence data or the detail data can be displayed for the contact.



The calendar is visible in the calendar view of the detail view as well as in the phonebook search mask for the contact.

Detail view for selected contact - Calendar / absence – multiple views.

10.8 Refreshing list of possible email accounts

After adding a new external calendar connector and publishing the changes in System Management, the email accounts retrieved by the new calendar system cannot be queried in Concierge, even if ETB data has valid email addresses.

In order to solve this problem, please delete the XML file located under C:\ProgramData\OpenScape Contact Center Extensions\CalFunctionNode\XML and restart ExternalCalendarNode in SystemManagement/Control Center by Shutdown button.

OSC Service starts it automatically.

11 UC, Circuit or Skype Node for OpenScape Concierge

11.1 UC Node

The UC node of Concierge connects with OpenScape UC system for displaying the presence status and the media state of the UC extension to the attendant that wants to transfer a call to the corresponding user.

Remark: It does not include individual status text.

For Concierge accessing the UC presence service, a user account is required as described in section 11.1.6.1 Creating a new OpenScape UC user.

The linking element between the contact in Electronic Telephone Book (ETB) and the UC system is the extension number.

Thus a successful integration will only work if the contacts in ETB do have the extension number in the availabilities that is also used to refer to in the UC system.

NOTE:
The following sections describe settings on the OpenScape UC Server and should only be conducted by trained service personnel.
The descriptions and configuration settings are not meant to be carried out by people who are not skilled in UC Server administration.

The UC Node is parameterized by the configuration settings in System Management as described in section 6.3. Section Applications

11.1.1 UC prerequisites

- The UC system is readied for operation
- The UC system can be reached from the OSC Server
- The UC port and the UC licenses have to be activated in OSV.
- Open OSV Firewall for UC Node
- Configure Presence Service Max Subscriptions in UC environment

11.1.2 Open OSV firewall for UC node

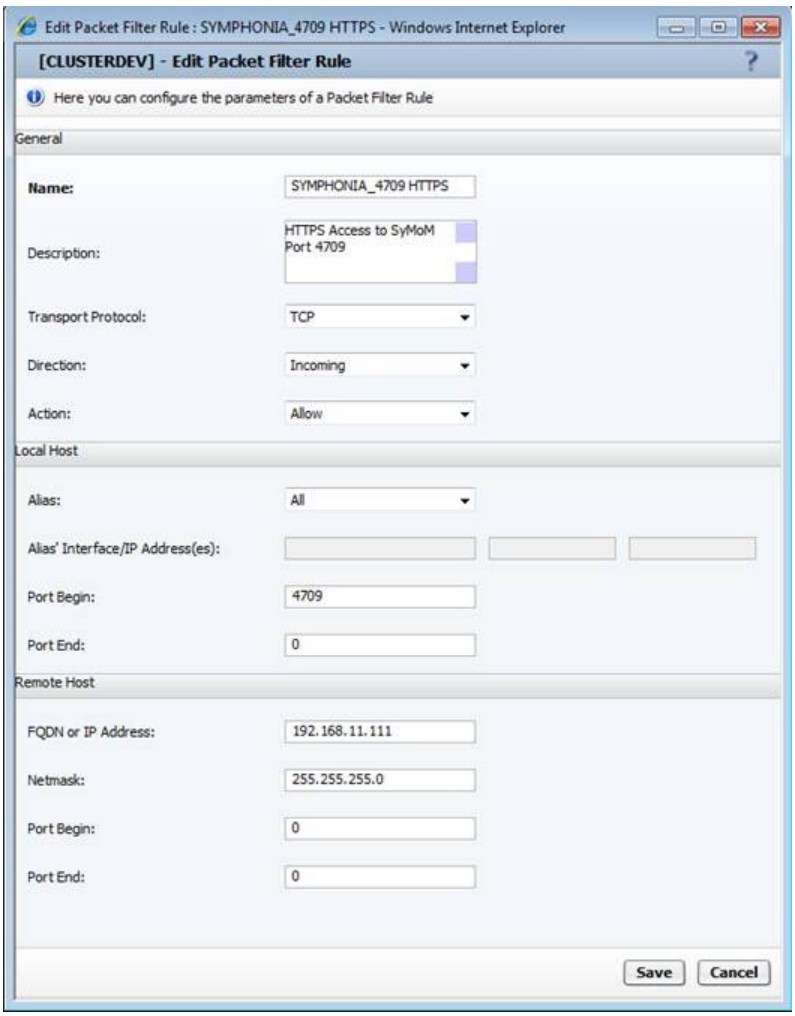
In order that the UC node can connect with the OSV, the server has to be activated in OSV firewall.

Procedure

In CMP go to

“Configuration -> OpenScape Voice -> Administration -> General Settings -> Packet Filter Rules”,

Add the server and enter as destination port in OSV **port 4709** for HTTPS protocol.



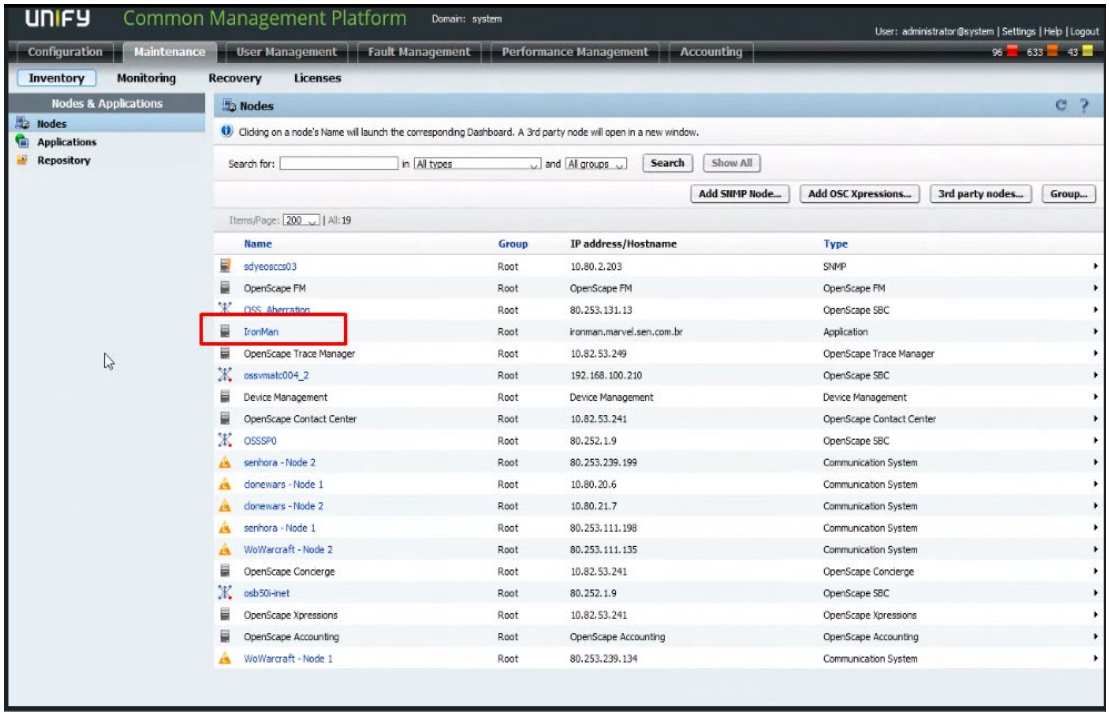
11.1.3 How to set Max Subscription in UC environment

Due to internal limitations of the UC environment the value Max Subscription must be raised to the max. number of UC users on the installation.

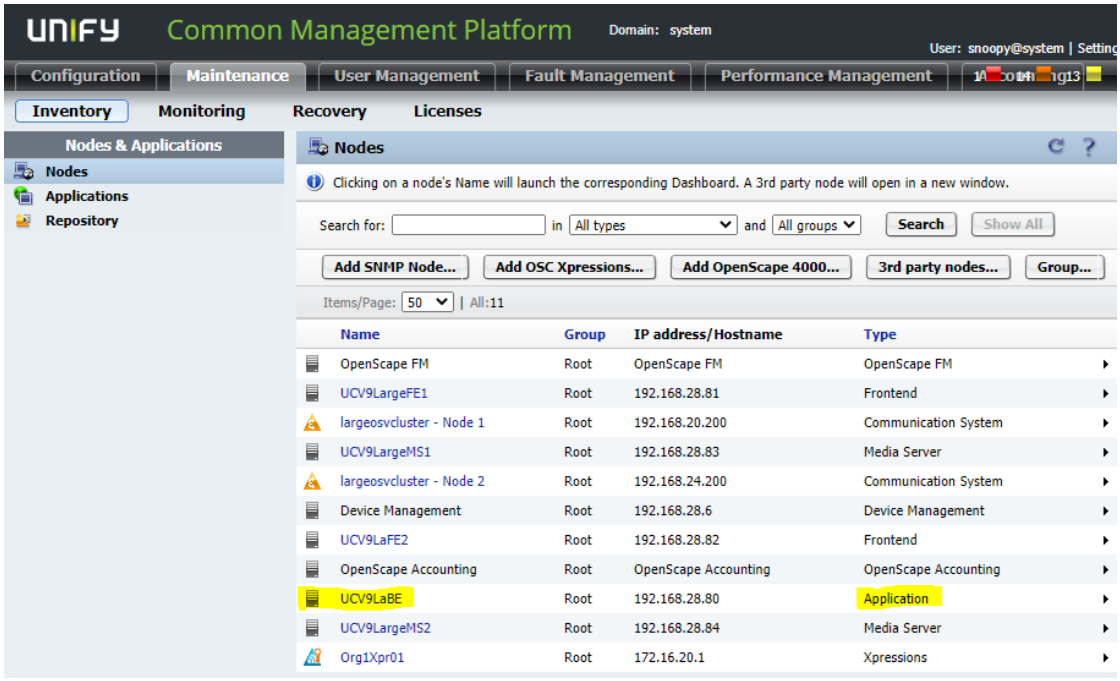
NOTE:
This means that every user is able to create a subscription list with that number of subscriptions.

With your default browser open the Common Management Portal (CMP) on your OSV installation.

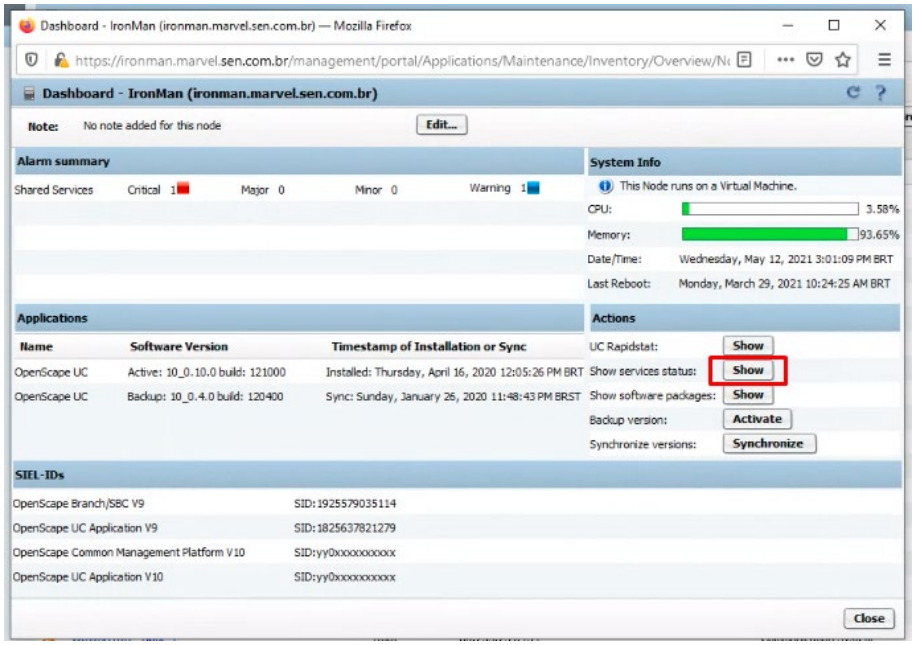
1. Navigate to Maintenance and select Nodes on the left side.
2. Click on the "UC Backend" node which will take you to the UC configuration (in this example, due to an UC small deployment scenario, the UC Backend function is in the same server/Application).



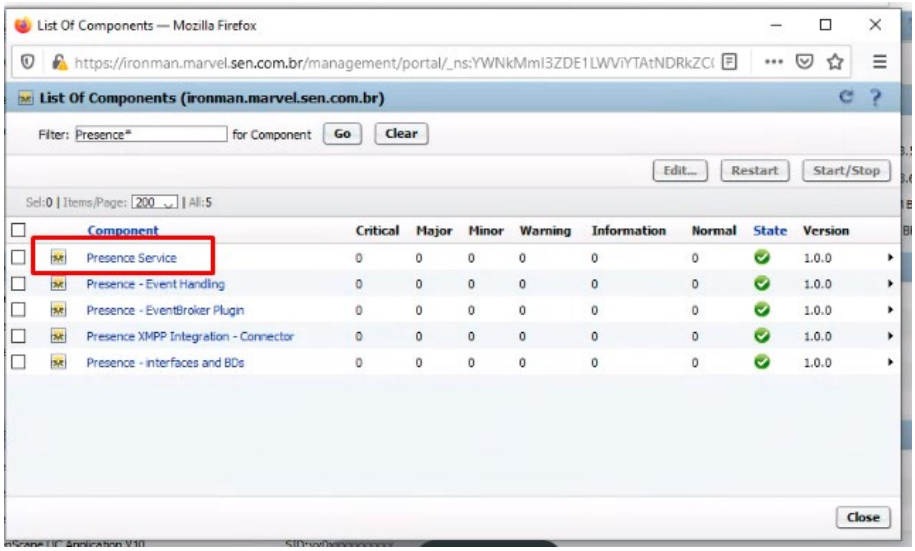
In either Large or Very Large UC deployments, the UC Backend function would be in a separated server as seen in this example below:



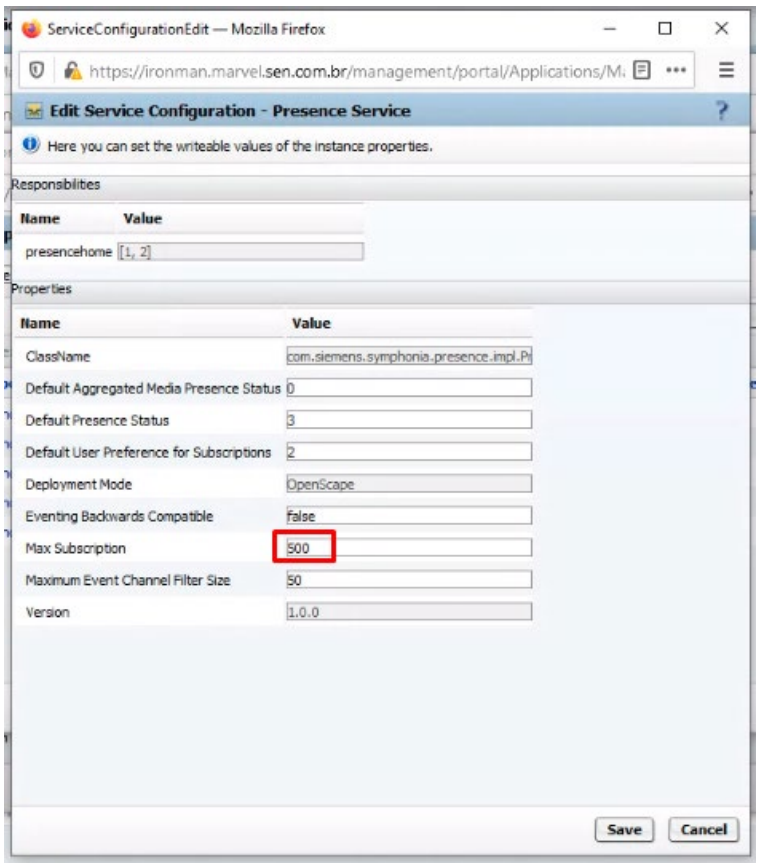
1. The Dashboard opens. Press the **Show** Button for “Show services status” in the **Action** area.



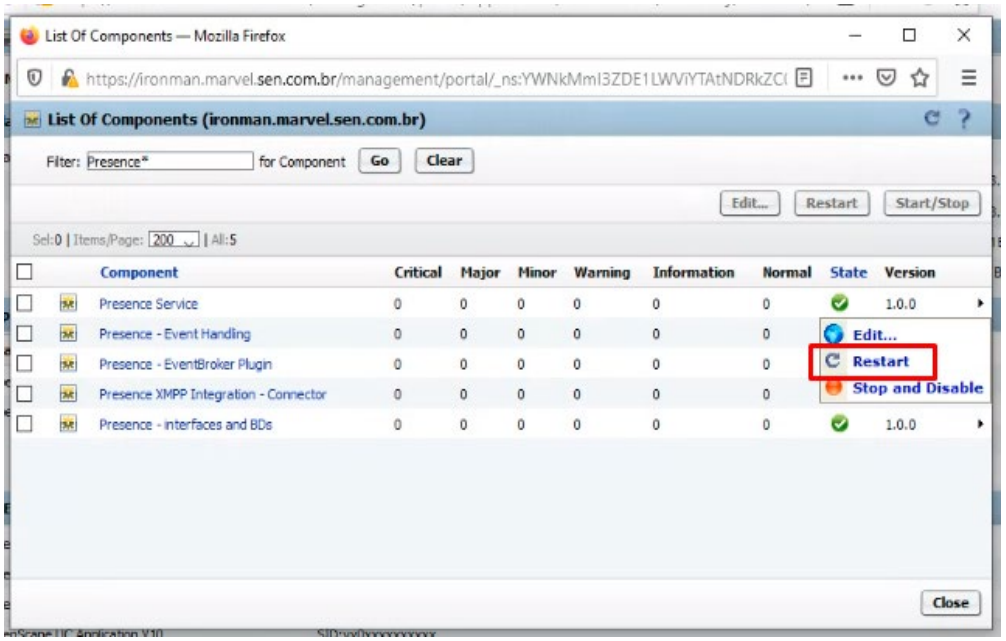
2. You see the NodeList. Filter the list for the “Presence Service” component.



3. In next window select the parameter “Max Subscriptions”, edit the value to the max. number of UC users on the installation. Press **Save** and close the window.



4. The Presence Server has to be restarted after this change, therefore open the submenu for “Presence Service” on the right and use the restart option.



11.1.4 Permission-based preparations

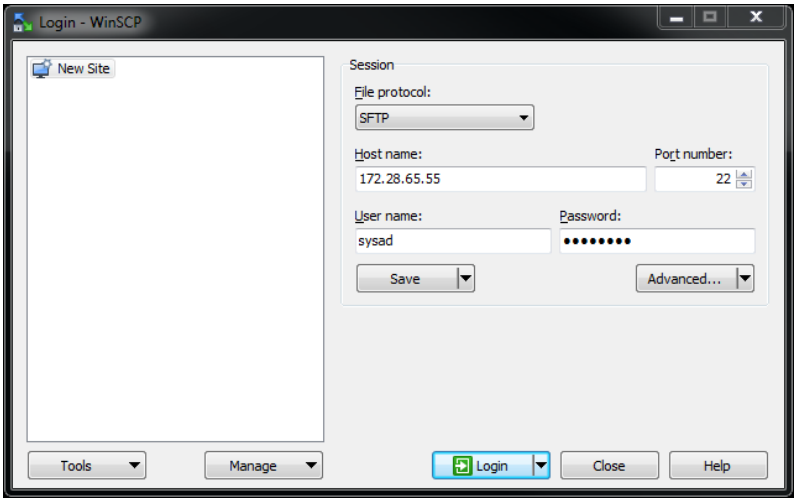
The UC system contains a file with **a key associated with the permissions for accessing the UC system**. This key is the so called the “**Long Lived**

Statement". The file containing this key must be fetched via SSH (Secure Shell) from the UC Server and the key from the file entered in **System Management**.

11.1.4.1 Generating the key

On the OpenScape Concierge Tools in the SWS you will find a tool name GenerateLongLivedStatement.zip. Download the file from SWS. It must be copied to the UC Application Backend Server. This can be done for example with the WinSCP program.

The host name or the IP address, the user name and the password from the UC Application Backend Server must be entered here.

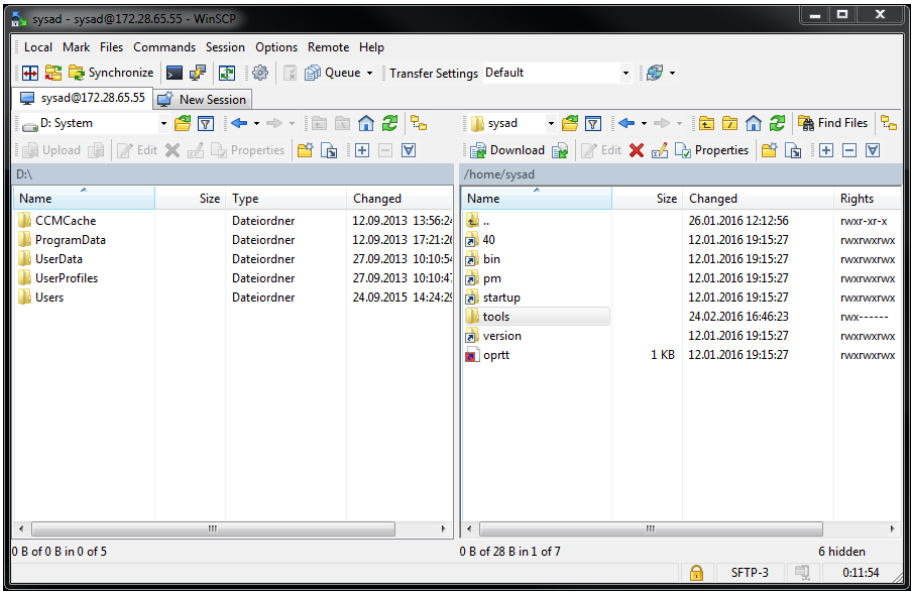


The user logs on with **Login**.

A warning is issued the first time the user logs on. This must be confirmed with **Yes**. At this point the servers exchange their keys in order to ensure secure communication.

The OSC Server is shown on the left-hand side and the UC Application Backend Server on the right-hand side.

Please copy the folder **\GenerateLongLivedStatement** under Tools from the Setup DVD to the UC Application Backend Server.



For the next step of installation, you need an access to the console of the UC Application Backend Server. Either you can use a remote access with SSH Protocol or you work on the UC Application Backend Server itself.

You can use the application **putty** in Windows environment. After the connection is established with the user (e.g. “sysad”), change to folder “tools” (formerly copied). In the folder you will find two shell scripts with the name ***createserviceLongLivedStatement_be.sh*** and ***createServiceStatment_fe.sh***.

1. First you must change the mode of the first shell script to „executable“. (Command: *chmod +x ~/*GenerateLongLivedStatement*/createLongLivedStatement_be.sh)*.
2. Then you have to generate the ***SymphoniaStatement.cfg*** file. With

   ./createLongLivedStatement_be.sh

   you execute the shell script to generate ***SymphoniaStatement.cfg***.

NOTE:
For Large or very Large deployment only:
Copy the GenerateLongLivedStatement folder to OpenScape UC Application Frontend Server.
The output file *SymphoniaStatement.cfg* from *UC Application Backend Server* must be copied to this directory, too.

For Small Deployment do the following steps on **UC Application Backend Server**, for Large and very Large Deployment on selected **UC Application Frontend Server.**

The second script is needed for creating the ***LongLivedStatement.txt*** file. Change the mode to executable and run the script.

*chmod +x ~/*GenerateLongLivedStatement*/createServiceStatement_fe.sh*

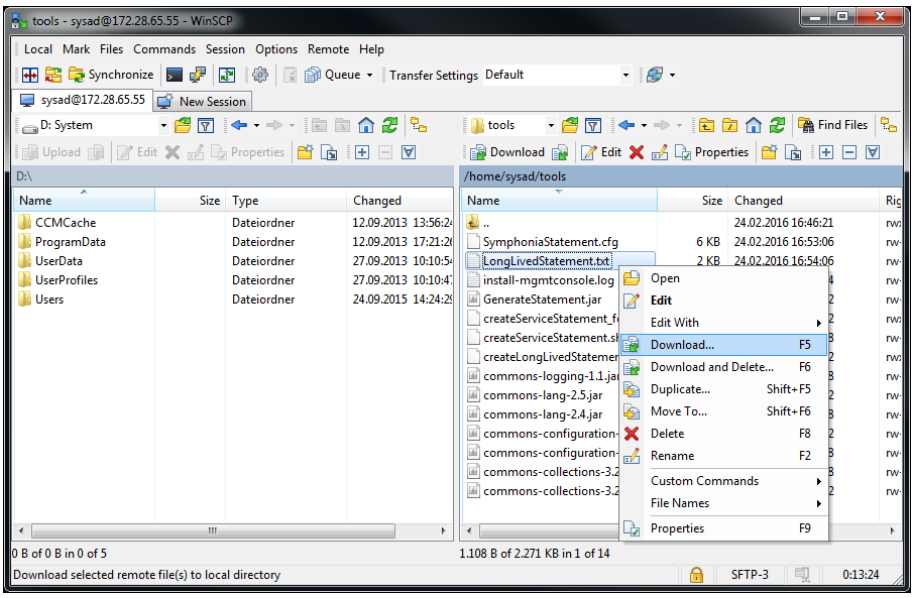
./createServiceStatement_fe.sh

After executing the script ***LongLivedStatement.txt*** will be created in the same folder.

NOTE:
The shell script is available from OSCC-E V3R0 Patch 2 on.

11.1.4.2 Getting the key

Copy the key from the UC Server the key was created on to OSC Server.



The new file ***LongLivedStatement.txt*** must be copied from the UC Server to the OSC Server. A menu opens by right-clicking the file.

When you select **Copy** a new window opens. The destination for the copy process should be selected here and confirmed with **Copy**.

The file is transferred from the UC Server to the destination directory on the OSC Server.

The WINSCP can be exited. Use the **OK** button to confirm you want to exit from the program.

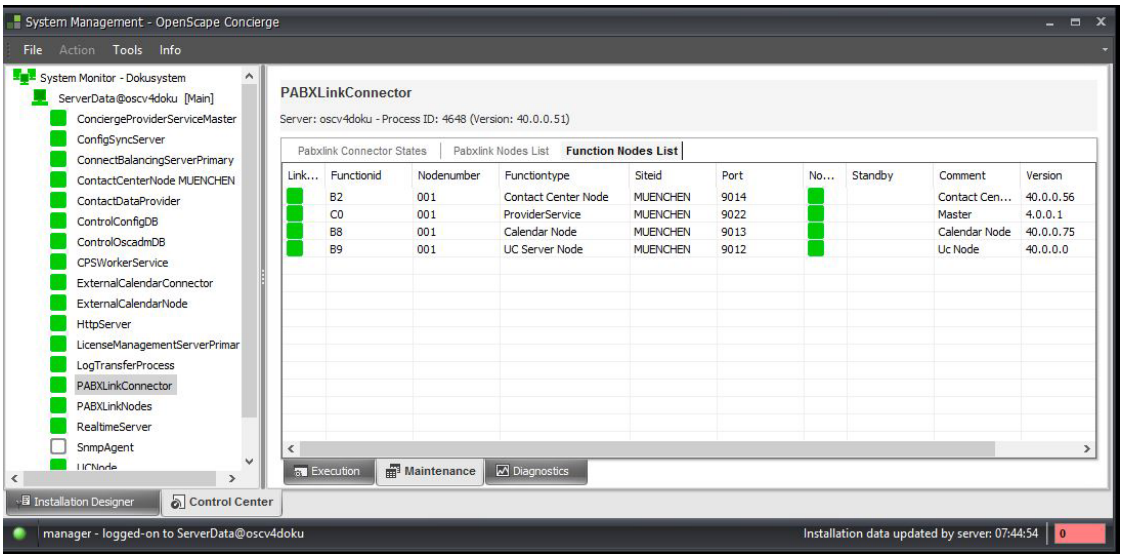
11.1.5 Saving keys in System Management

Open the previously copied ***LongLivedStatement.txt*** file additionally with any editor. The content of the ***LongLivedStatement.txt*** file should be copied into the field **Long Lived Statement** in System Management, in section applications\ Concierge as described in section 6.3 Section Applications.

11.1.6 Check and activate UC function node

This should be checked in the PABX Link Connector's Function Node List:

Go to **System Management ** Tab **Control Center**. Highlight **the PABX Link Connector** on the left; on the right pane change to PABXLinkConnector's **Maintenance** (tab on the bottom). Find the tab **Function Nodes List** on the right upper area and open this.



The following parameters should be configured there:

Table: Parameters UC Node

Field	Description	Value
FunctionID	Unique ID of the function node (B0 – BF)	B9
Node Number	Number of node	001 If this is also entered in the ucconfig.ini file
SiteID	Site ID assigned to the function node (Master Side ID)	LOC001
TCP/IP Port	Port number that connects the function node to the connector.	9012
Comment	Description of the function node	UC Node
Version	Version of UC System	
Ipaddress	IP address of UC System	

Once successfully concluded, the PABX Link Connector recognizes the new node and the node is activated after a short while.

If the function node is not activated, the PABXLinkConnector should be restarted under the tab Execution (tab on bottom)

Once the function node has been activated (LED is green), the UC Service can likewise be started.

11.1.6.1 Creating a new OpenScape UC user

For Concierge accessing the UC presence service, a user account is required. In a **standard small UC deployment** a CMP administrator account can be used.

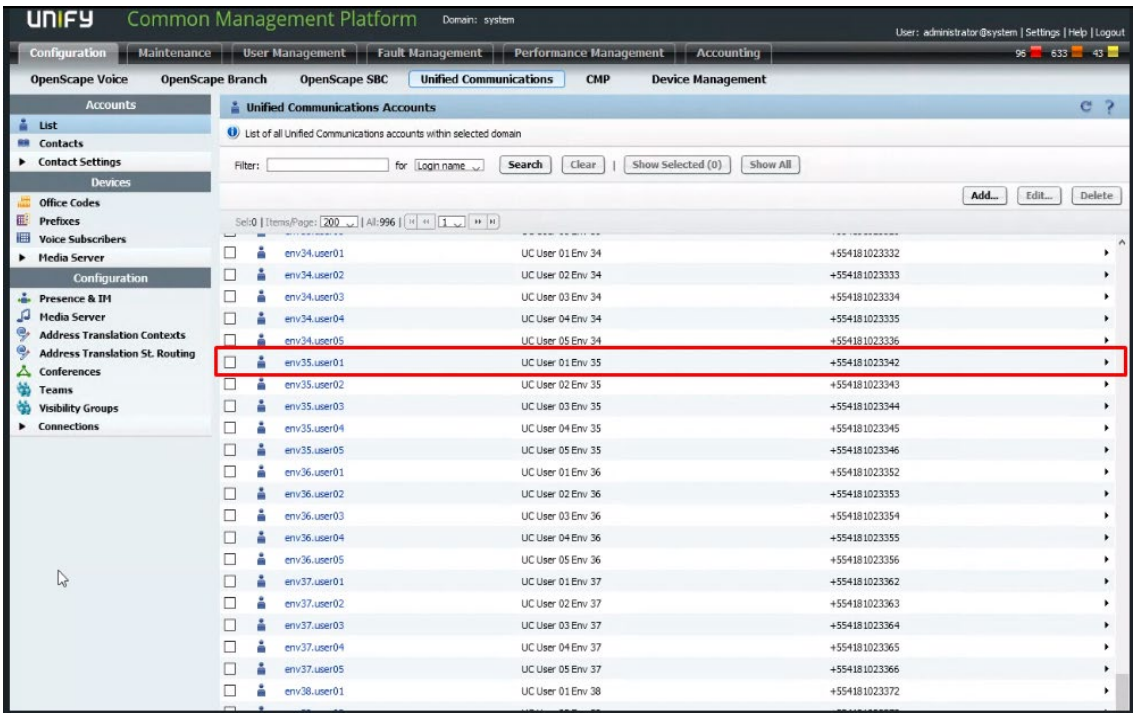
In a **Very Large deployment** it is mandatory to create an additional UC account for connection purpose.

NOTE:
In all kinds of deployments an additional UC account can be used instead of the CMP administrator account.

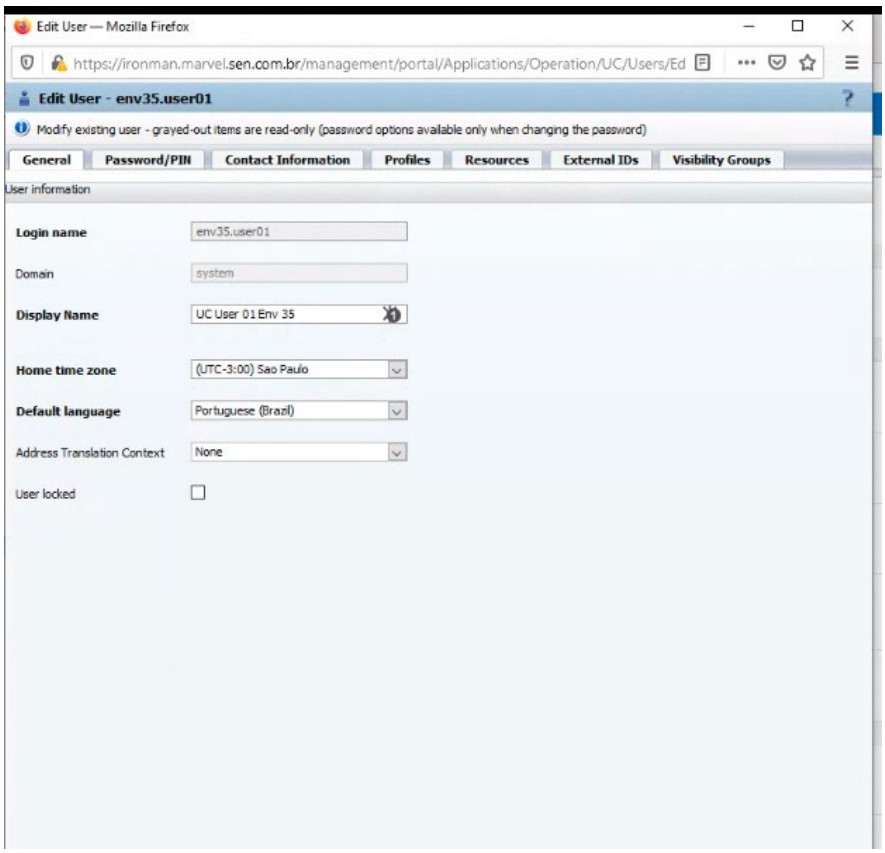
A new user account can to be used. This UC user must have a profile that supports UC functionality. An ONS number is not required. The credentials of that new user are then inserted in **System Management** in the fields **Admin User** and **Admin Password** as visible in section 6.3 Section Applications.

NOTE:
The user needs to have an IM address, that usually is composed of the *<UC login name>@<XMPP.domain>*, e.g. concierge@A.unify.net

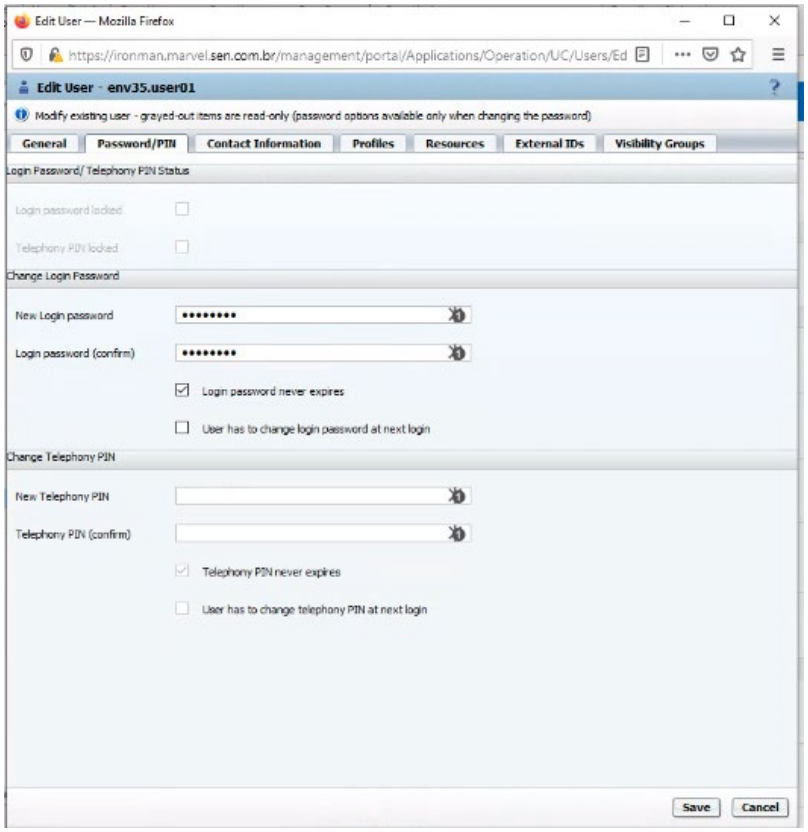
The following displays how to create a new OpenScape UC user for the UC node to access OpenScape UC (next screenshots will show a user already created as example).



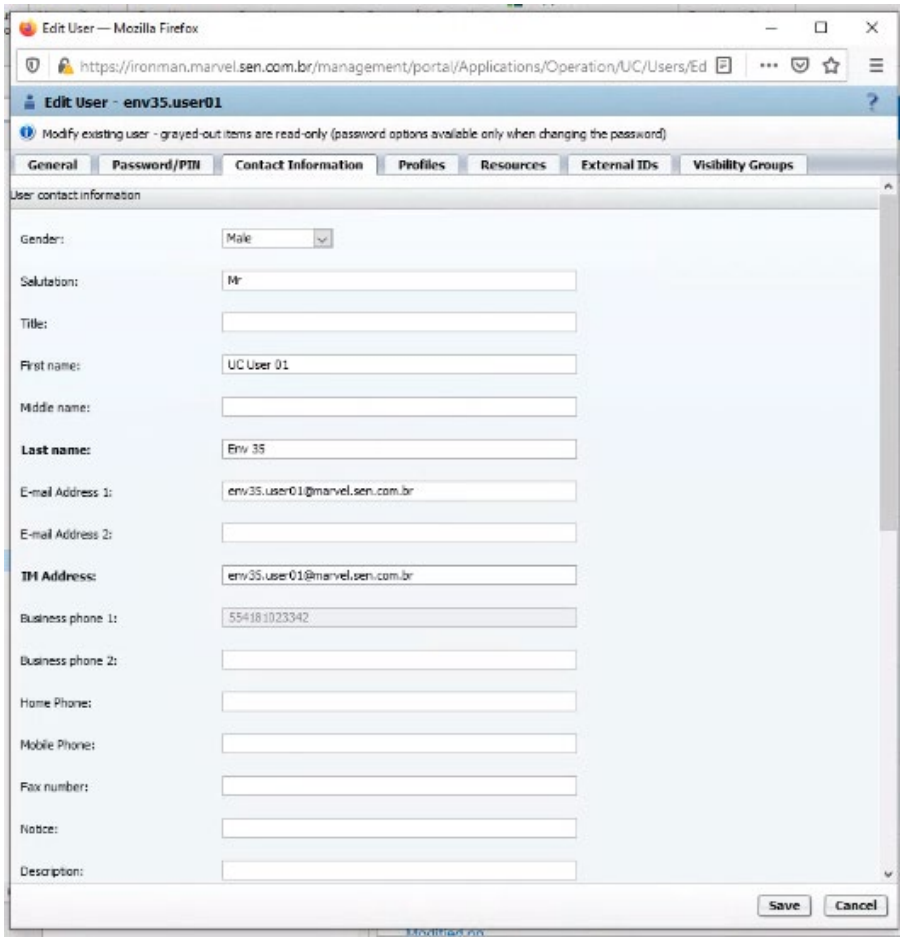
Press the **Add** button.



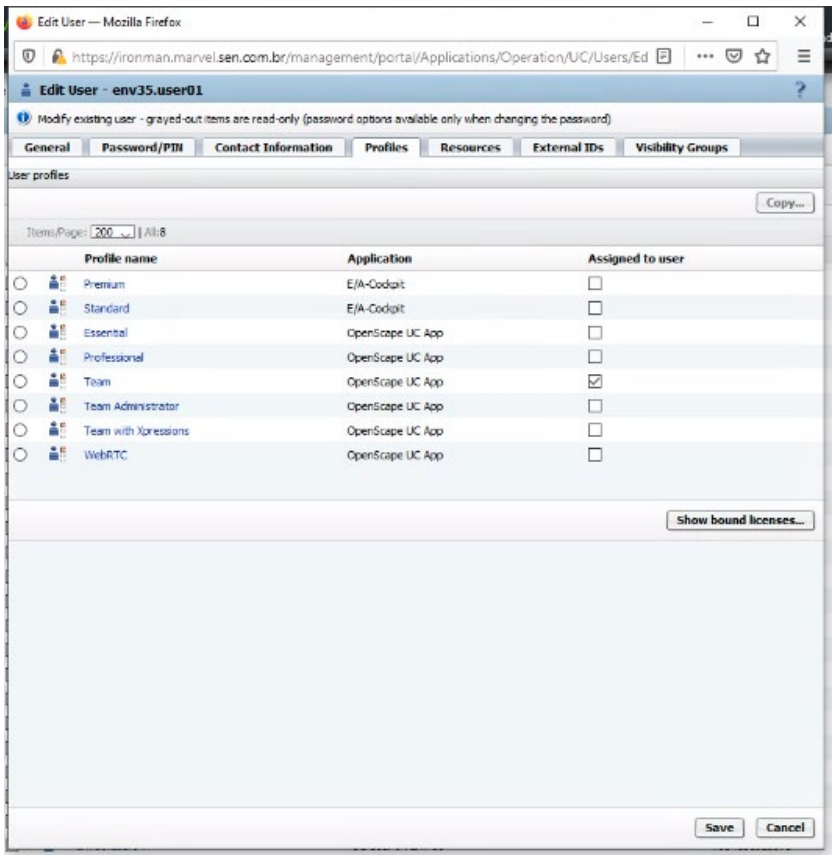
Configure **Login Name** and **Display Name**.



Configure and confirm the **password**.

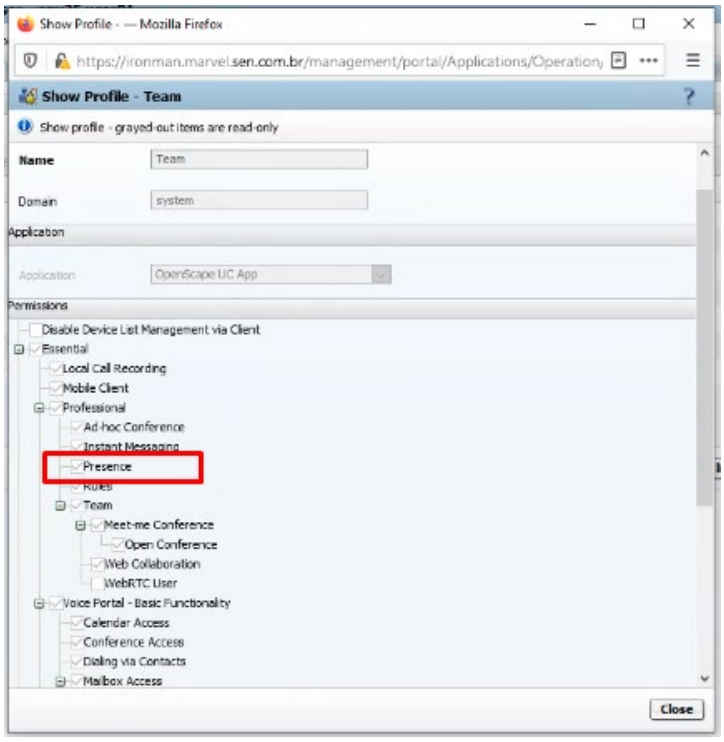


For receiving the presence information in a **Very Large Deployment** the **IM address** needs to be configured.



Add a **profile** that has the **permission presence** activated.

NOTE:
Please check the permissions of the chosen profile by clicking on the **profile** hyperlink (in this example, “Team” – see next screenshot).



11.2 Circuit Node

For Concierge accessing the Circuit server, an OAuth 2.0 app credentials (bot user) in your Circuit domain such as eu.yourcirucuit.com is required.

The user subscription request can be done via the link: http://developers.circuit.com under step 3 “Go Live”– “Register your application”.

The response on the user subscription request will include the Client ID and Secret Code information.

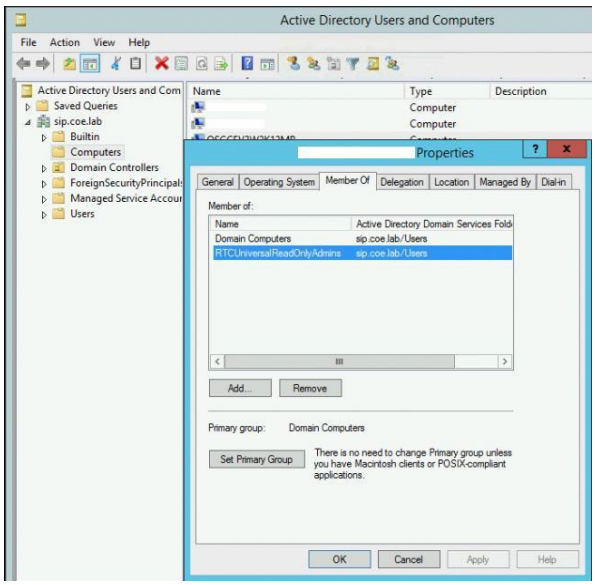
11.3 Skype Node

For Concierge accessing the Skype for Business server, a trusted application name and port are required.

The information can be retrieved from Skype for Business administration website under Topology / Trusted Application tab.

The User Agent string (of application endpoint) must be provided by the Skype administrator, especially if client policies are used.

In addition to access the Skype for Business list of users, the computer(s) hosting OSC main or standby service needs to be member of „RTCUniversalReadOnlyAdmins“ group.



NOTE:
As part of the Skype for Business replication additional Microsoft SQL Server service and agent (RTCLOCAL) are required (installed and running)!

11.4 Teams Node

For Concierge Integration with Microsoft Teams and to show the Microsoft Teams user state presence in Concierge client UI it is necessary an application registered with specific configurations and permissions on Azure Portal.

After the application registration, you can get the information (Client ID, Tenant ID, administrator account, and password) to configure the Microsoft Teams integration in the Concierge System Management tool.

NOTE: The Microsoft Teams service account used for the application must have the multi-factor authentication deactivated.

NOTE: The Application Registration on the Azure portal must have:

• The following delegated permissions (with granted admin consent) are necessary for the Application in the ** API permissions area: Presence.Read, Presence.Read.All, User.Read, User.Read.All, User.ReadBasic.All;

• The property 'allowPublicClients' must be as 'true' in the Manifest area;

• The Supported account types configuration must be as 'Multiple Organizations'.

NOTE: for more information about how to register a Microsoft Teams application in Microsoft Azure Portal you can consult the respective Microsoft Graph API documentation.

mitel.com