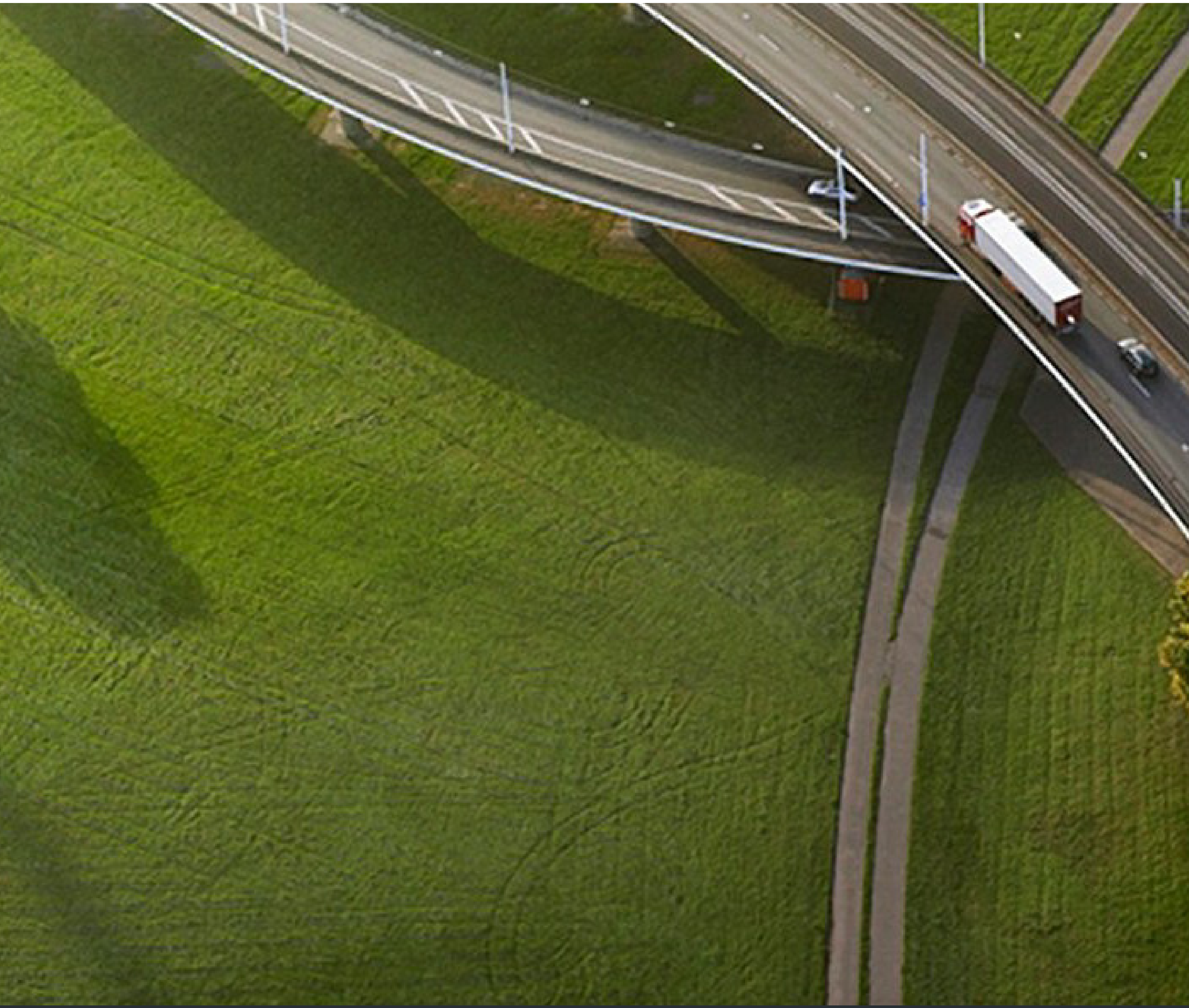
Harmonize
your enterprise



OpenScape Business V2
Installing OpenScape Business S

Installation Guide

A31003-P3020-J101-05-7631

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

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

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

Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany

Reference No.: A31003-P3020-J101-05-7631

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

Availability and technical specifications are subject to change without notice.

UNIFY Harmonize your enterprise

unify.com

Contents

1 Introduction and Important Notes 5
1.1 About this Documentation 5
1.1.1 Documentation and Target Groups 5
1.1.2 Types of Topics 7
1.1.3 Display Conventions 7

2 Preparing for the Installation of OpenScape Business S 8

3 Installing the Linux Server 9
3.1 Prerequisites 9
3.2 Installation in a Virtual Environment. 12
3.2.1 VM Co-Residency and Quality of Service policy 14
3.2.2 Time Synchronization of the Guest Operating System Linux 15
3.2.2.1 How to Configure Time Synchronization for the Guest Operating System Linux in VMWare 16
3.3 Linux Security Aspects and RAID Array 16
3.4 Initial Startup without a Software RAID 18
3.4.1 How to Install and Configure SLES 11 SP4 without a Software RAID 18
3.5 Initial Startup with a Software RAID. 22
3.5.1 How to Deactivate the BIOS RAID 23
3.5.2 How to Install and Configure SLES 11 SP4 with a Software RAID 24
3.6 Configuring a Uniform Time Base 29
3.6.1 How to Configure an SNTP Server. 30
3.7 Updates 30
3.7.1 How to Enable Automatic Online Updates 31
3.7.2 How to Enable Online Updates Manually 32
3.8 Backup and Restore 32

4 Initial Setup for OpenScape Business S. 33
4.1 Prerequisites for the Initial Setup 33
4.2 Components. 35
4.3 IP Address Scheme 36
4.4 Dial Plan. 37
4.5 Installing the Communication Software 38
4.5.1 How to Install the Communication Software 40
4.6 Function Check with the OpenScape Observer. 42
4.6.1 How to Copy OpenScape Observer to the PC 42
4.6.2 How to Start OpenScape Observer from the PC 44
4.7 Starting Up 44
4.7.1 How to Start the Initial Installation Wizard 44
4.7.2 System Settings 45
4.7.2.1 How to Set the Display Logo and the Product Name 45
4.7.2.2 How to Select the Country Code and the Language for Event Logs. 46
4.7.2.3 How to Activate an Additional LAN Port as a WAN Interface 47
4.7.3 UC Solution. 47
4.7.3.1 How to Define the UC Solution 48
4.8 Basic Configuration 48
4.8.1 How to Start the Basic Installation Wizard 49
4.8.2 System Phone Numbers and Networking 49

4.8.2.1 How to Enter the System Phone Numbers for a Point-to-Point connection 50
4.8.2.2 How to Enter the System Phone Numbers for a Point-to-Multipoint Connection 50
4.8.2.3 How to Activate or Deactivate Networking 51
4.8.3 Station Data 52
4.8.3.1 How to Display the Station Data 53
4.8.3.2 How to Delete all Call Numbers 53
4.8.3.3 How to Adapt Preconfigured Station Numbers for the Individual Dial Plan 54
4.8.3.4 How to Import the Station Data from an XML File 55
4.8.4 Internet Telephony 55
4.8.4.1 How to Configure a Predefined ITSP 56
4.8.4.2 How to Deactivate Internet Telephony 63
4.8.5 Stations 63
4.8.5.1 How to Configure IP and SIP Stations 64
4.8.6 Configuring UC Suite 66
4.8.6.1 How to Configure the UC Suite 67
4.8.7 Configuring UC Smart Mailboxes. 67
4.8.7.1 How to Configure UC Smart Voicemail Boxes 67
4.8.8 Conference Server Settings 68
4.8.8.1 How to Edit the Conference Server Settings 68
4.8.9 E-mail Delivery (Optional) 69
4.8.9.1 How to Configure the Sending of E-mails. 69
4.9 Closing Activities 70
4.9.1 How to Activate and Assign the Licenses 71
4.9.2 How to Provision the UC Smart Client for Installation 73
4.9.3 How to Provision the UC Suite Clients for Installation 74
4.9.4 How to Perform a Data Backup 75
4.10 Commissioning of IP Phones 75
4.10.1 How to Configure an IP Phone 77
4.10.2 How to Configure a SIP Phone 78
4.11 Uninstalling the Communication Software 80
4.11.1 How to Uninstall the Communication Software 80
4.12 Used Ports 80

Index 83

1 Introduction and Important Notes

This introduction provides you with an overview of the documentation structure. The introduction should assist you in finding information on selected topics faster.

1.1 About this Documentation

This document provides information on the initial startup of the Linux server, which is required for the operation of OpenScape Business S, and the subsequent initial setup of OpenScape Business S.

This document is intended for administrators and service technicians.

1.1.1 Documentation and Target Groups

The documentation for OpenScape Business is intended for various target groups.

Sales and Project Planning

The following documentation is intended for sales and project planning.

- Feature Description
  This documentation describes all the features. This document is an extract from the Administrator Documentation.

Installation and Service

The following documentation is intended for service technicians.

- OpenScape Business X1, Installation Guide
  This document describes the installation of the hardware and the initial installation of OpenScape Business X1.
- OpenScape Business X3/X5/X8, Installation Guide
  This document describes the installation of the hardware and the initial installation of OpenScape Business X3/X5/X8.
- OpenScape Business S, Installation Guide
  This documentation describes the initial installation of the OpenScape Business S softswitch.
- OpenScape Business X1, Service Documentation
  This documentation describes the hardware of OpenScape Business X1.
- OpenScape Business X3/X5/X8, Service Documentation
  This documentation describes the hardware of OpenScape Business X3/X5/X8.

Administration

The following documentation is intended for administrators.

- Administrator Documentation
  This documentation describes the configuration of features that are set up using the OpenScape Business Assistant (WBM). The Administrator documentation is available in the system as online help.
- Configuration for Customer Administrators, Administrator Documentation
  This documentation describes the configuration of features that can be set up using the OpenScape Business Assistant (WBM) with the **Basic** administrator profile.
- Manager E, Administrator Documentation
  This documentation describes the configuration of features that are set up using Manager E.

UC Clients / Telephone User Interfaces (TUI)

The following documentation is intended for UC users.

- myPortal Smart, User Guide
  This documentation describes the configuration and operation of the UC client myPortal Smart.
- myPortal for OpenStage, User Guide
  This documentation describes the configuration and operation of myPortal for OpenStage.
- myPortal for Desktop, User Guide
  This documentation describes the installation, configuration and operation of the UC client myPortal for Desktop.
- myPortal for Outlook, User Guide
  This documentation describes the installation, configuration and operation of the UC client myPortal for Outlook.
- Fax Printer, User Guide
  This documentation describes the installation, configuration and operation of Fax Printer.
- myPortal to go User Guide
  This documentation describes the configuration and operation of the mobile UC client myPortal to go for smartphones and tablet PCs.
- myAgent, User Guide
  This documentation describes the installation, configuration and operation of the Contact Center client myAgent.
- myReports, User Guide
  This documentation describes the installation, configuration and operation of the Contact Center client myReports.
- myAttendant, User Guide
  This documentation describes the installation, configuration and operation of the attendant console myAttendant.
- OpenScape Business Attendant, User Guide
  This documentation describes the installation, configuration and operation of the attendant console OpenScape Business Attendant.
- UC Smart Telephone User Interface (TUI), Quick Reference Guide
  This documentation describes the voicemail phone menu of the UC solution UC Smart.

- UC Suite Telephone User Interface (TUI), Quick Reference Guide
  This documentation describes the voicemail phone menu of the UC solution UC Suite.

1.1.2 Types of Topics

The types of topics include concepts and tasks:

Type of topic	Description
Concept	Explains the "What" and provides an overview of context and background information for specific features, etc.
Task (operating instructions)	Describes task-oriented application cases (i.e., the "How") step-by-step and assumes familiarity with the associated concepts. Tasks can be identified by the title **How to ...**.

1.1.3 Display Conventions

This documentation uses a variety of methods to present different types of information.

Type of information	Presentation	Example
User Interface Elements	Bold	Click **OK**.
Menu sequence	>	**File > Exit**
Special emphasis	Bold	**Do not delete** Name.
Cross-reference text	Italics	You will find more information in the topic*Network*.
Output	Monospace font, e.g., Courier	`Command not found.`
Input	Monospace font, e.g., Courier	`Enter` LOCAL as the file name.
Key combination	Monospace font, e.g., Courier	`<Ctrl>+<Alt>+<Esc>`

2 Preparing for the Installation of OpenScape Business S

Before OpenScape Business S can be installed and put into operation for the first time, some preparatory activities must be performed.

For OpenScape Business S, the OpenScape Business communication software is installed on a Linux server.

The prerequisites for the Linux server and the installation of the Linux operating system can be found in chapter on *Installing the Linux Server*.

The prerequisites for OpenScape Business S and the installation of the OpenScape Business communication software can be found in the chapter *Initial Setup of OpenScape Business S*.

3 Installing the Linux Server

For OpenScape Business S and OpenScape Business UC Booster Server, the OpenScape Business communication software is installed on a Linux operating system. The communication software can be operated directly on a Linux server or in a virtual environment with VMware vSphere or Microsoft Hyper-V.

> ***INFO:*** In the following, whenever a description applies to both OpenScape Business S and the OpenScape Business Booster UC Server, the generic term OpenScape Business is used for the sake of simplicity.

Either the regular SLES 11 SP4 64-bit version or an SLES 11 SP4 64-bit version optimized by the manufacturer of the server PC must be installed as the Linux operating system.

These installation instructions describe the initial startup of the Linux server. This depends on whether or not the Linux server is using a software RAID. The installation of the OpenScape Business communication software and the subsequent configuration of OpenScape Business are described in the *OpenScape Business Administrator Documentation*.

The initial startup of the Linux server described here is based on the English user interface. The installation and configuration can, of course, also be performed in a different interface language.

3.1 Prerequisites

The prerequisites and general constraints for the operation of OpenScape Business on the Linux server (the server PC) are described below.

Hardware

The server PC must satisfy the following minimum requirements:

- 64-bit capable
- Equipped for 24/7 operation.
- Certified by the PC manufacturer for SLES 11 SP4 64 bit
- The communication software for OpenScape Business must be the only application running (excluding virus scanners)
- At least a dual-core processor with 2.0 GHz per core (for OpenScape Business Contact Center or more than 500 users: at least a quad-core processor with 3.3 GHz per core)
- At least 2 GB RAM (recommended: 4 GB RAM)
  The following features require 4 GB RAM:
  - Fax as PDF
  - More than 500 users

  - OpenScape Business Contact Center
  - Gate View
  - XMPP
- LAN connection with min. 100 Mbps
- DVD drive, keyboard, mouse
- Screen resolution: 1024x768 or higher
- The size of the hard disk depends on the number of users:

# Users	Hard disk size
Up to 50 users	60 GB or more
Up to 100 users	100 GB or more
Up to 500 users	200 GB or more
OpenScape Business Contact Center	200 GB or more
More than 500 users	500 GB or more

The installation can be performed even if the minimum requirements are not satisfied; however, this could result in problems during operation.

Software

To install the Linux operating system on the server PC, the **SLES 11 SP4 64-bit** Linux version is required.

When procuring the OpenScape Business communication software, you can purchase a DVD or .ISO file with this version of Linux. This DVD or .ISO file may only be used in conjunction with the communication software.

Some PC manufacturers offer their own optimized Linux installation disks for their server PC models. These can be used if they support the Linux version SLES 11 SP4 64 bit.

Keep the Linux DVD or .ISO file handy during the installation of the OpenScape Business communication software, since some software packages (RPM) required for the communication software may need to installed later from this DVD or .ISO file.

SLES 11 SP4 64-bit Certification

The server PC must be certified for SLES 11 SP4 64 Bit.

Novell offers PC manufacturers a certification program called "YES" for the certification of their server PCs. The results can be found on the Internet at:

`http://developer.novell.com/yessearch/Search.jsp`

If no certification is available, the PC manufacturer must be asked whether the server PC is compatible with SLES 11 SP4 64 Bit. If any additional hardware (e.g., a network or graphics card) that is incompatible with SLES 11 SP4 64 Bit is installed, a suitable driver must be obtained from the card vendor, regardless of the certification. If no driver is available, the corresponding card must be replaced by a model that is compatible with SLES 11 SP4 64 Bit.

Registering with Novell

Although the installation and operation of SLES 11 SP4 64 bit is possible without registering with Novell, registration at Novell is required in order to obtain security patches and software updates. To do this, you will need to create a customer account with Novell with the help of the activation code (see also *Updates*). It is recommended that the customer account be set up before the Linux installation.

A Novell Activation Code (registration code) can be procured via the order item "OpenScape Business SLES Upgrade Key".

Infrastructure

The internal network must satisfy the following conditions:

- LAN with at least 100 Mbps and IPv4
- Uniform time base (e.g., via an NTP server)
- Fixed IP address for the server PC

Internet Access

The server PC must have Internet access for:

- Registering with Novell
- Security patches and general Linux software updates

OpenScape Business requires an Internet connection for:

- OpenScape Business software updates
- OpenScape Business features such as Internet telephony, for example
- Remote Service (SSDP)/RSP.servicelink

Network Configuration

During the Linux installation, you will be prompted for the network configuration details. Consequently, it is advisable to create an IP address scheme containing all network components and their IP addresses before the network configuration.

The following is an example of an IP address scheme with the IP address range `192.168.5.x`:The parameters shown in bold are the minimum mandatory specifications required during the Linux installation.

Parameters	Sample values
External DHCP server or Linux DHCP server	DHCP server of the Internet router (external)
DHCP address range	192.168.5.50 through 192.168.5.254
Subnet mask of the network or network segment	**255.255.255.0**
Fixed IP address of the Linux server This IP address must be outside the DHCP range.	**192.168.5.10**
Internet Router	192.168.5.1

Parameters	Sample values
Server with fixed IP address (optional), e.g., e-mail server	192.168.5.20
Clients with fixed IP address (optional) This IP address must be outside the DHCP range.	192.168.5.1 through 192.168.5.49
Default Gateway, i.e., the Internet router in the example	**192.168.5.1**
DNS Server (i.e., the Internet router in the example)	**192.168.5.1**
Domain name when using a DNS server (e.g., the Internet domain name	**customer.com**
Host name of OpenScape Business The name can be freely selected, but should be coordinated with the network administrator.	**comm_server**

If the actual network data is not available at time of installation, the network should be configured with the data of this sample network.

After the successful installation of Linux, the network data can be edited at any time with YaST and adapted to the network.

Skipping the network configuration is not recommended, since the subsequent installation of OpenScape Business cannot be successfully completed without a fully configured network.

3.2 Installation in a Virtual Environment

The communication software can run in a virtual environment.

To set up a virtual environment, the virtualization software (host operating system) must be first installed and configured on the server PC. Linux is then installed as a guest operating system. Finally, the communication software is installed within the Linux operating system.

For licensing in a virtual environment, an Advanced Locking ID is generated and used for the softswitch instead of the MAC address of the server PC.

The following virtualization software has been released:

- VMware vSphere Version 4 or 5, including the latest patches
  For details on the hardware requirements of the physical server PC, refer to the "VMware Compatibility Guide and the "VMware Management Resource Guide" at www.vmware.com.

To determine the hardware requirements at the physical server PC, VMware offers an online search function for certified and tested hardware under "Compatibility Guides" on their Internet homepage at `http://www.vmware.com/guides`

- Windows Server (2008 R2, 2012, 2012 R2) Hyper-V, including the latest patches.
  For details in the hardware requirements of the physical server PC, refer to technet.microsoft.com.

You will find all necessary information about Hyper-V in the section Library -> Windows Server 2012 R2 (or your current windows server system) -> Server Roles and Technologies -> Hyper V on the Microsoft technet page.

The description of the installation and configuration of the virtualization software is not part of this documentation. The installation of Linux and the communication software in a virtual environment is exactly the same as for a direct installation on the server PC.

Disk Provision guidelines can be found at `https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc_50%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html`

The following minimum requirements must be configured for Linux and the communication software in the virtual environment:

Parameters	VM Settings
Guest Operating System	SLES 11 SP4 64 Bit
VM HD Capacity	Up to 50 users: 60 GB or more Up to 100 users: 100 GB or more Up to 500 users: 200 GB or more OpenScape Business Contact Center: 200 GB or more As of 500 users: 500 GB or more
Virtual Disk Mode	Default
Virtual Disk Format Type	Thin Provisioning (dynamic HD Capacity) or Thick Provisioning (fixed HD Capacity)
vCPUs	2 4 for OpenScape Business Contact Center or more than 500 users
vCPUs Shares (High/Normal)	High
vCPU Reservation	2 GHz
vCPU Limit	Unlimited

Parameters	VM Settings
VM Memory	2 GB 4 GB for: - Fax as PDF - More than 500 users - OpenScape Business Contact Center - Gate View - XMPP
VM Memory Shares (High/Normal)	Normal
VM Memory Reservation	4 GB
VM Memory Limit	Unlimited
Number of vNICs	1
VMware Manual MAC Used	NO
Virtual Network Adapter Support	YES, vmxnet3 driver
VMware Tools Installation	YES

The VM (Virtual Machine) may utilize the CPU up to 70%; values above that can result in erratic behavior.

The following VMware vSphere features are supported:

- Thin Provisioning
- High Availability (HA)
- VMotion
- Data Recovery (VDR)
- DRS (Automatic VMotion)
- Storage VMotion

The following VMware vSphere features are not supported:

- Fault tolerance

The following Microsoft Hyper-V features are supported:

- Thin Provisioning
- High Availability (HA)
- Live Migration
- Data Recovery

The screen saver for the virtual environment must be disabled.

3.2.1 VM Co-Residency and Quality of Service policy

This VM Co-Residency and Quality of Service Policy provides the rules for the parties responsible for deploying the Unify VMs and managing the virtual environment when deploying Unify VMs on consolidated network and hardware resources:

- It is up to the parties responsible for deploying the Unify VMs and managing the virtual environment to ensure the performance criteria is met. Uncertainty can be reduced by pre-deployment testing, baselining, and following the rules of Unify VM Configuration and Resource Guide (VM R&C) including this policy.
- VMs with Unify real time and mission critical applications shall be protected from other applications in the routing and switching network to ensure voice/ video network traffic get the needed bandwidth and protection from delay and jitter.
- VMs with Unify real time and mission critical applications shall be protected from other applications when the virtualization host shares compute, storage, and network hardware among multiple application virtual machines (e.g. you cannot schedule Unify real time.
- Adherence to Unify Virtualization and Resource configuration rules (e.g. physical/virtual hardware sizing, co-residency policy, etc.) is required in order to ensure Unify VMs get the needed CPU, memory, storage capacity and storage/network performance.
- Unify VMs shall not be hosted on the same HW with third-party VMs that have incomplete resource requirements defined.
- Host hardware shall be continuously monitored (e.g. by vCenter) and operated below 80% CPU usage with a %RDY value of 5% max.
- The total amount of RAM, Storage, and NW (including Storage Network) throughput shall not be exceed the capacity of the Host hardware (no over subscription).
- Even if the host processor is hyper-threading-capable and HT is enabled, a physical core shall only be counted once.
- vCPU Shares shall be configured to guarantee mission critical Unify VMs (including real time VMs) are never starved for CPU time.
- Customers are responsible to fulfill the requirements, even if the VM is moved around in the environment, e.g. by manually re-configuring the CPU shares of a VM if it gets moved to another VM host or resource pool.
- Disaster Recovery plans need to take into account the additional resources required when failing over to fail over site (datacenter 2).

3.2.2 Time Synchronization of the Guest Operating System Linux

The time synchronization (uniform time base for date and time) between the host operating system VMware vSphere or Microsoft Hyper-V and the guest operating system Linux must be disabled. The uniform time base should be obtained by the guest operating system via an NTP server.

3.2.2.1 How to Configure Time Synchronization for the Guest Operating System Linux in VMWare

Step by Step

1) Right-click in the VMware client **vSphere Client** on the guest operating system Linux and select the menu item **Edit Settings**.

2) Under the **Virtual Machine Properties** on the **Options** tab, disable the option **Synchronize guest time with host** under the **VMware Tools** entry in the **Advanced** area.

3) Edit the NTP settings for the guest operating system Linux in the `./etc/ntp.conf` file as follows in accordance with the parameters shown in bold:

```
************************************************
...
tinker panic 0
# server 127.127.1.0
# local clock (LCL)
# fudge 127.127.1.0 stratum 10
# LCL is unsynchronized
...
server 0.de.pool.ntp.org iburst
restrict 0.de.pool.ntp.org
restrict 127.0.0.1
restrict default kod nomodify notrap
...
************************************************
```

INFO: The NTP server **de.pool.ntp.org** is an example and may need to be replaced by an NTP server address that can be reached by the guest operating system Linux.

3.3 Linux Security Aspects and RAID Array

The security of the Linux server can be enhanced by observing all Linux security aspects and by using a RAID array.

Firewall

When connected to the Internet, a firewall is needed to prevent unauthorized access from outside. After installing Linux, the Linux firewall is enabled. The installer of the communication software adjusts the firewall settings so that the communication software can be operated properly. The ports for the communication software are opened, and all other ports are closed. All communication software services, except for CSTA (CSTA interface) and SSH (Secure Shell), are released.

If an external firewall is used in the network, the Linux firewall must be disabled, and the addresses and ports required for the communication software must be opened (see "Ports Used" *Used Ports*in the installation instructions for OpenScape Business S or OpenScape Business UC Booster Server).

Virus Scanners

A virus scanner is not included in the Linux installation package. When connected to the Internet, the virus scanner Trend Micro Server Protect for Linux is recommended. The current version of this virus scanner can be obtained from the Release Notes of the communication software if required.

In order to prevent potential performance problems resulting from the use of the virus scanner, the regular disk scans should be scheduled for times when the communication software is not being used or is only used at a minimum.

Intrusion Detection System (AppsAmor)

The installation routine of the application server does not make any changes to the Linux Intrusion Detection System (AppsArmor). The default settings of the Linux installation are used. No further settings are required for the operation of the communication software.

During the installation of the softswitch, the integrated intrusion detection system (AppsArmor) is updated and activated. No further settings are required for the operation of the communication software.

Redundancy

Recommendations for Improving Reliability (Redundancy):

- Two hard disks in a RAID 1 array.
- Second power supply for the Linux server
- Uninterruptible power supply
  When using IP phones, the LAN switches and IP phones should also be connected to an uninterruptible power supply.

RAID1 Array

In a RAID1 array, the contents of the first hard drive are mirrored on the second hard drive. If one hard drive fails, the system continues to run on the second hard drive.

A RAID array may be set up as a software RAID or hardware RAID (BIOS RAID or hardware RAID controller).

For specific details on performing an installation with a software RAID, see *Initial Startup with a Software RAID*.

A hardware RAID frequently requires a separate driver that is not included in the Linux operating system. This driver is usually provided by the PC manufacturer and must be installed according to manufacturer's instructions. If the driver is not compatible with the Linux version or if no Linux driver is offered, the hardware RAID cannot be used. The description of hardware-based RAID systems is not part of this documentation. In such cases, please contact the manufacturer for the appropriate Linux drivers and configuration details.

3.4 Initial Startup without a Software RAID

The initial startup of the Linux server without a software RAID includes the Linux installation and configuration, while taking into account that no software RAID is being used.

The required settings for the communication software are made during the installation and configuration.

Linux Partitions

The hard drive must be partitioned during the initial start-up as follows:

Partition	Type	Size	File system	Mount	Note
Partition 1	Primary Partition	2 GB	Swap	swap	corresponds to the size of the working memory
Partition 2	Primary Partition	15 GB	Ext3	/	for the Linux operating system
Partition 3	Primary Partition	Rest[1]	Ext3	/home	For the communication software

[1] Up to 50 users: min. 40 GB - Up to 100 users: min. 80 GB - More than 500 users: min. 180 GB - With OpenScape Business Contact Center: min. 180 GB - More than 500 users: min. 480 GB

INFO: The installation routine of the communication software checks these partition sizes and may reject the installation.

INFO: Some server PCs require an additional boot partition. If Linux suggests a boot partition, it should be accepted in the proposed size.

3.4.1 How to Install and Configure SLES 11 SP4 without a Software RAID

Prerequisites

- The BIOS setup of the Linux server is set so that the server will boot from the DVD or .ISO file.
- To register with Novell, Internet access and the activation code are required.

Step by Step

1) Insert the SLES 11 DVD or .ISO file into the DVD drive and boot up the system from the DVD or .ISO file. The Startup window of the Linux installation appears.

2) Press the F3 key and select an appropriate screen resolution (e.g., **1280 x 1024**).

3) Select the menu item **Installation** and confirm this by pressing the Enter key.

4) In the **Welcome** window, select the country settings for the Linux operating system:

a) Select **English (US)** as the user interface language in the **Language** drop-down list.

b) Select the keyboard layout for the desired country from the **Keyboard Layout** drop-down list.

5) Read through the license agreement and accept the license terms by enabling the check box **I Agree to the License Terms**. Then click **Next**.

6) Click in the **Media Check** window on **Start Check** to check the DVD or .ISO file for any existing read errors. Then click **Next**.

7) Activate the **New Installation** option in the **Installation Mode** window and click **Next**.

8) In the **Clock and Time Zone** window, select the correct region and time zone. Adjust the date and time if needed with **Change** on and then click **Next**.

9) In the **Server Base Scenario** window, enable the option **Physical Machine** and click **Next**.

10) Click in the **Installation Settings** window on **Partitioning**.

11) Activate the radio button **Custom Partitioning (for experts)** and click **Next**.

12) Navigate in the **System View** menu tree to **Hard Disks > sda**.

13) Delete all preassigned partitions (sda1, sda2, etc.) by marking the partition, clicking on **Delete**, and then confirming the Delete operation with **Yes**.

14) Create a swap partition:

a) Click on **Add**, activate the **Primary Partition** radio button, and then click **Next**.

b) Under **Custom Size**, enter the size of the swap partition. As a rule, the swap partition corresponds to the size of the working memory (e.g.: with 4 GB RAM, the swap partition should be set to 4 GB, with the entry: `4GB`).

c) Click **Next**.

d) In the **File system** drop-down list, select **Swap** and click on **Finish**.

15) Create the partition for the Linux operating system:

a) Click on **Add**, activate the **Primary Partition** radio button, and then click **Next**.

b) Under **Custom Size**, enter the partition size (e.g., if 15 GB are sufficient - Enter: `+15GB`) and click **Next**.

c) Enable the **Format partition** radio button and select the item **Ext3** in the **File system** drop-down list.

d) Enable the **Mount partition** radio button and select the item **/** in the **Mount Point** drop-down list.

e) Click on **Finish**.

16) Create the partition for the communication software:

a) Click on **Add**, activate the **Primary Partition** radio button, and then click **Next**.

b) Under **Custom Size**, enter the partition size (the suggested value corresponds to the remaining space on the hard disk) and click **Next**.

c) Enable the **Format partition** radio button and select the item **Ext3** in the **File system** drop-down list.

d) Enable the **Mount partition** radio button and select the item **/home** in the **Mount Point** drop-down list.

e) Click on **Finish**.

17) Click on **Accept**. You are returned to the **Installation Settings** window.

18) Click on **Install**.

19) Accept the license terms for the Agfa Monotype Corporation Font Software with **I Agree** and click on **Install**. The hard disk is now partitioned. The installation of the Linux operating system takes about 20 - 30 minutes. A restart is then performed.

20) Select the item **Boot from Hard Disk** in the Startup window of Linux.

21) After the Linux server is up, enter the password for the system administrator with the "root" profile. The password should comply with conventional security policies (i.e., have at least 8 characters, at least one lowercase letter, at least one uppercase letter, at least one number and at least one special character). Then click **Next**.

22) Configure the settings for the host name and domain name:

a) If desired, change the proposed host name under **Hostname** (to `comm_server`, for example.

b) If desired, change the proposed domain name under **Domain Name** (to `<customer>.com`, for example).

c) Clear the **Change Hostname via DHCP** check box.

d) Clear the **Assign HostName to Loopback IP** check box.

e) Then click **Next**.

23) Click in the **Network Configuration** window on **Network Interfaces**.

24) Configure the network card:

- ***a)*** Select the desired network card in the **Overview** window and click on **Edit**. The MAC address of the network card selected here is assigned later in the licensing process to the individual licenses.
- ***b)*** Enable the radio button **Statically assigned IP Address**.
- ***c)*** Under **IP Address**, enter the assigned IP address of the Linux server (e.g., `192.168.5.10`. The IP address must conform to the IP address scheme of your internal network and must not have been assigned to any network client, since this would otherwise result in an IP address conflict.
- ***d)*** Under **Subnet Mask**, enter the assigned subnet mask of the Linux server (e.g., `255.255.255.0`. The subnet mask must match the IP address scheme of your internal network.
- ***e)*** Then click **Next**.

25) Specify the DNS server and the default gateway.

- ***a)*** In the **Network Settings** window, click on the **Host name/DNS** tab.
- ***b)*** Enter the IP address of the DNS server under **Name Server 1**. If no DNS server is available in the internal network, enter the IP address of the Internet router (e.g., `192.168.5.1`).
- ***c)*** In the **Network Settings** window, click on the **Routing** tab.
- ***d)*** Under **Default Gateway**, enter the IP address of the Internet router (for example:. `192.168.5.1`).
- ***e)*** Click **OK**.

26) Click in the **Network Configuration** window on **Next**.

27) Activate the radio button **Yes, Test Connection to the Internet via** in the **Test Internet Connection** window and select the network card via which the Internet connection is to be set up.

28) Click on **Next**.

29) After the test succeeds, click **Next**.

30) Register with Novell for patches and software updates:

- ***a)*** In the **Novell Customer Center Configuration** window, enable the option **Configure now (Recommended)** and click **Next**. You will be redirected to the Novell web page.
- ***b)*** Enter your e-mail address and activation code there. After a successful registration, the update window appears.
- ***c)*** Click on **Run Update**.
- ***d)*** Select what you want to install from the list of patches (exception: Service Packs may not be installed) and click **Accept**. The updates are downloaded and installed.

31) Then click **Next**.

32) Click in the **Network Services Configuration** window on **Next**., since no changes are required at the CA Management and the OpenLDAP server.

33) Activate the radio button **Local (/etc/passwd)** in the **User Authentication Method** window and click **Next**.

34) Create a new user with restricted privileges. This is required so that you are not logged in as "root" with all administrator privileges during normal operation.

a) Enter the full name of the user under **User's Full Name**, e.g., `John Doe`.

b) Enter a freely selectable name under **Username**, e.g., `john2000`.

c) Enter a password for the user under **Password** and **Confirm Password**. The password should comply with conventional security policies (i.e., have at least 8 characters, at least one lowercase letter, at least one uppercase letter, at least one number and at least one special character).

d) Make sure that the **Receive System Mail** and **Automatic Login** check boxes are cleared.

e) Click on **Next**.

35) Click in the **Release Notes** window on **Next**.

36) Confirm the test of the graphics card with **OK**.

37) Verify the hardware configuration in the **Hardware configuration** window. As a rule, the hardware is automatically recognized correctly, and nothing needs to be configured here. If you want to change some settings, this can be done via the **change** button.

38) Click on **Next**.

39) If you leave the check box **Clone This System for AutoYAST** enabled in the **Installation Competed** window, all the configuration settings made here will be saved to a file (requires approx. 1-2 minutes). This enables further Linux servers to be quickly and conveniently installed with the same configuration settings. For more information on this, see the description of the operating system.

40) Click on **Finish**.

41) Log in as the "root" user:

42) The Linux installation is complete. Remove the DVD from the DVD drive.

Next steps

Configure an NTP server (for a uniform time base).

3.5 Initial Startup with a Software RAID

The initial startup of the Linux server with a software RAID includes the Linux installation and configuration, while taking into account that a software RAID is being used.

Proceed as follows:

1. Disable the BIOS RAID (optional)
   If a RAID array is to be set up via a software RAID, any integrated RAID BIOS that may be present on the motherboard of the server PC must be first disabled in the BIOS.
2. Install and configure SLES 11 SP1 with a software RAID
   The required settings for the communication software are made during the installation and configuration.

Linux Partitions

The hard drive must be partitioned during the initial start-up as follows:

Partition	Type	Size	File system	Mount	Note
Partition 1	Primary Partition	2 GB	Swap	swap	corresponds to the size of the working memory
Partition 2	Primary Partition	15 GB	Ext3	No mount point	for the Linux operating system
Partition 3	Primary Partition	Rest[1]	Ext3	No mount point	For the communication software

[1] Up to 50 users: min. 40 GB - Up to 100 users: min. 80 GB - More than 500 users: min. 180 GB - With OpenScape Business Contact Center: min. 180 GB - More than 500 users: min. 480 GB

The mount points are assigned after the partitioning when setting up the RAID system.

INFO: The installation routine of the communication software checks these partition sizes and may reject the installation.

INFO: Some server PCs require an additional boot partition. If Linux suggests a boot partition during the installation, it should be accepted in the proposed size.

3.5.1 How to Deactivate the BIOS RAID

Prerequisites

- An integrated RAID controller (BIOS RAID) is available on the motherboard of the PC.

Step by Step

1) Restart the PC. During the startup, you will see whether the BIOS RAID has been enabled. If the BIOS RAID is not enabled, skip to step 3.
2) Disable the active BIOS RAID:
   a) Press the appropriate key combination at the right time during the startup to enter BIOS RAID setup. The combination will be shown to you during the startup (e.g., CTRL M for LSI MegaRAID BIOS).
   b) Clear the BIOS RAID configuration. Example for LSI MegaRAID BIOS: Management Menu > Configure > Configuration Menu > Clear Configuration.
   c) Exit the setup of the BIOS RAID and restart the PC.
3) Disable the RAID configuration in the BIOS setup of the PC:
   a) Press the appropriate key (e.g., F2 or Del) at the right time during the startup to enter BIOS setup of the PC.
   b) Disable the SATA RAID. Example for a Phoenix BIOS: Advanced > Advanced System Configuration > SATA RAID Disabled.
   c) Save your changes and exit the BIOS setup of your PC (with the F10 key, for example).
4) Restart the PC.

Next steps

Install and configure SLES 11 with a software RAID

3.5.2 How to Install and Configure SLES 11 SP4 with a Software RAID

Prerequisites

- Any possibly existing hardware RAID is disabled.
- The BIOS setup of the Linux server is set so that the server will boot from the DVD or .ISO file.
- To register with Novell, Internet access and the activation code are required.

Step by Step

1) Insert the SLES 11 DVD or .ISO file into the DVD drive and boot up the system from the DVD or .ISO file. The Startup window of the Linux installation appears.
2) Press the F3 key and select an appropriate screen resolution (e.g., **1280 x 1024**).
3) Select the menu item **Installation** and confirm this by pressing the Enter key.

4) In the **Welcome** window, select the country settings for the Linux operating system:

- ***a)*** Select **English (US)** as the user interface language in the **Language** drop-down list.
- ***b)*** Select the keyboard layout for the desired country from the **Keyboard Layout** drop-down list.

5) Read through the license agreement and accept the license terms by enabling the check box **I Agree to the License Terms**. Then click **Next**.

6) Click in the **Media Check** window on **Start Check** to check the DVD or .ISO file for any existing read errors. Then click **Next**.

7) Activate the **New Installation** option in the **Installation Mode** window and click **Next**.

8) In the **Clock and Time Zone** window, select the correct region and time zone. Adjust the date and time if needed with **Change** on and then click **Next**.

9) In the **Server Base Scenario** window, enable the option **Physical Machine** and click **Next**.

10) Click in the **Installation Settings** window on **Partitioning**.

11) Activate the radio button **Custom Partitioning (for experts)** and click **Next**.

12) Partition the two hard disks:

- ***a)*** Navigate in the **System View** menu tree to **Hard Disks > sda** (first hard disk of the software RAID).
- ***b)*** Delete all preassigned partitions (sda1, sda2, etc.) by marking the partition, clicking on **Delete**, and then confirming the Delete operation with **Yes**.
- ***c)*** Partition the first hard disk by using the **Add** button.

  Use the following data for the partitioning:

Partition 1	Primary Partition	2 GB	Format Swap, Mount Point = swap, fstab Option = Device name
Partition 2	Primary Partition	15 GB	Format Ext3, no Mount Point
Partition 3	Primary Partition	Rest	Format Ext3, no Mount Point

- ***d)*** Navigate in the **System View** menu tree to **Hard Disks > sdb** (second hard disk of the software RAID).
- ***e)*** Complete steps b and c for the second hard disk as well.

13) Specify the software RAID settings:

- ***a)*** Select the menu item **RAID** and click on **Add RAID**.
- ***b)*** Select **RAID 1 (Mirroring)**.

c) Select the two partitions sda2 and sdb2 in the **Available Devices** area on the left and transfer them with **Add** to the **Selected Devices** area on the right.

d) Click on **Next**.

e) Confirm the default value for the Chunk Size with **Next**.

f) In the next window, select the mount point "/" for the first RAID device (/dev/md0) and click **Finish**.

g) Then click on **Add Raid** again.

h) Select **RAID 1 (Mirroring)**.

i) Select the two partitions sda3 and sdb3 in the **Available Devices** area on the left and transfer them with **Add** to the **Selected Devices** area on the right.

j) Click on **Next**.

k) Confirm the default value for the Chunk Size with **Next**.

l) In the next window, select the mount point "/home" for the second RAID device (/dev/md1) and click **Finish**.

14) Click on **Accept**. The partitioning data is saved; the actual partitioning of the hard disk occurs later. You are returned to the **Installation Settings** window.

15) Specify the Boot Loader settings:

a) Click on the **Expert** tab.

b) Click on **Booting** and then on the **Boot Loader Installation** tab.

c) Clear the **Boot from Boot Partition** check box.

d) Select the **Boot from Master Boot Record** and **Boot from Root Partition** check boxes.

e) Click on **Boot-Loader Options**.

f) Select the **Set active Flag in Partition Table for Boot Partition** and **Write generic Boot Code to MBR** check boxes.

16) Click **OK** twice to confirm your selection. You are returned to the **Installation Settings** window.

17) Click on **Install**.

18) Accept the license terms for the Agfa Monotype Corporation Font Software with **I Agree** and click on **Install**. The hard disks are now partitioned. The installation of the Linux operating system takes about 20 - 30 minutes. A restart is then performed.

19) Select the item **Boot from Hard Disk** in the Startup window of Linux.

20) After the Linux server is up, enter the password for the system administrator with the "root" profile. The password should comply with conventional security policies (i.e., have at least 8 characters, at least one lowercase letter, at least one uppercase letter, at least one number and at least one special character). Then click **Next**.

21) Configure the settings for the host name and domain name:

- ***a)*** If desired, change the proposed host name under **Hostname** (to `comm_server`, for example.
- ***b)*** If desired, change the proposed domain name under **Domain Name** (to `<customer>.com`, for example).
- ***c)*** Clear the **Change Hostname via DHCP** check box.
- ***d)*** Clear the **Assign HostName to Loopback IP** check box.
- ***e)*** Then click **Next**.

22) Click in the **Network Configuration** window on **Network Interfaces**.

23) Configure the network card:

- ***a)*** Select the desired network card in the **Overview** window and click on **Edit**. The MAC address of the network card selected here is assigned later in the licensing process to the individual licenses.
- ***b)*** Enable the radio button **Statically assigned IP Address**.
- ***c)*** Under **IP Address**, enter the assigned IP address of the Linux server (e.g., `192.168.5.10`. The IP address must conform to the IP address scheme of your internal network and must not have been assigned to any network client, since this would otherwise result in an IP address conflict.
- ***d)*** Under **Subnet Mask**, enter the assigned subnet mask of the Linux server (e.g., `255.255.255.0`. The subnet mask must match the IP address scheme of your internal network.
- ***e)*** Then click **Next**.

24) Specify the DNS server and the default gateway.

- ***a)*** In the **Network Settings** window, click on the **Host name/DNS** tab.
- ***b)*** Enter the IP address of the DNS server under **Name Server 1**. If no DNS server is available in the internal network, enter the IP address of the Internet router (e.g., `192.168.5.1`).
- ***c)*** In the **Network Settings** window, click on the **Routing** tab.
- ***d)*** Under **Default Gateway**, enter the IP address of the Internet router (for example:. `192.168.5.1`).
- ***e)*** Click **OK**.

25) Click in the **Network Configuration** window on **Next**.

26) Activate the radio button **Yes, Test Connection to the Internet via** in the **Test Internet Connection** window and select the network card via which the Internet connection is to be set up.

27) Click on **Next**.

28) After the test succeeds, click **Next**.

29) Register with Novell for patches and software updates:

a) In the **Novell Customer Center Configuration** window, enable the option **Configure now (Recommended)** and click **Next**. You will be redirected to the Novell web page.

b) Enter your e-mail address and activation code there. After a successful registration, the update window appears.

c) Click on **Run Update**.

d) Select what you want to install from the list of patches (exception: Service Packs may not be installed) and click **Accept**. The updates are downloaded and installed.

30) Then click **Next**.

31) Click in the **Network Services Configuration** window on **Next**., since no changes are required at the CA Management and the OpenLDAP server.

32) Activate the radio button **Local (/etc/passwd)** in the **User Authentication Method** window and click **Next**.

33) Create a new user with restricted privileges. This is required so that you are not logged in as "root" with all administrator privileges during normal operation.

a) Enter the full name of the user under **User's Full Name**, e.g., `John Doe`.

b) Enter a freely selectable name under **Username**, e.g., `john2000`.

c) Enter a password for the user under **Password** and **Confirm Password**. The password should comply with conventional security policies (i.e., have at least 8 characters, at least one lowercase letter, at least one uppercase letter, at least one number and at least one special character).

d) Make sure that the **Receive System Mail** and **Automatic Login** check boxes are cleared.

e) Click on **Next**.

34) Click in the **Release Notes** window on **Next**.

35) Confirm the test of the graphics card with **OK**.

36) Verify the hardware configuration in the **Hardware configuration** window. As a rule, the hardware is automatically recognized correctly, and nothing needs to be configured here. If you want to change some settings, this can be done via the **change** button.

37) Click on **Next**.

38) If you leave the check box **Clone This System for AutoYAST** enabled in the **Installation Competed** window, all the configuration settings made here will be saved to a file (requires approx. 1-2 minutes). This enables further Linux servers to be quickly and conveniently installed with the same configuration settings. For more information on this, see the description of the operating system.

39) Click on **Finish**.

40) To enable the PC to start from both hard disks, the following adaptations are needed (based on this example of a software RAID with the hard disks sda and sdb):

a) Log in as the "root" user.

b) Open a root shell and run the following commands there:

```
grub --device-map=/boot/grub/device.map
root (hd0,1)
setup (hd0)
root (hd1,1)
setup (hd1)
quit
```

41) The Linux installation is complete. Remove the DVD from the DVD drive.

Next steps

Configure an NTP server (for a uniform time base).

3.6 Configuring a Uniform Time Base

The communication system and IP stations (IP phones, client PCs) should have a uniform time base (date and time). This time base is provided by an SNTP server.

The following variants are possible as a time base:

- **SNTP server on the internal network (recommended)**
  If possible, an existing SNTP server on the internal network should be used. If this is the case, the IP address, URL or DNS name of the SNTP server is required.
- **SNTP Server on the Internet**
  If Internet access is available and set up, an SNTP server from the Internet can also be used. In this case, the URL or DNS name of the SNTP server is required.
- **OpenScape Business X3/X5/X8 as an SNTP server**
  Alternatively, the OpenScape Business X3/X5/X8 communication system can be used as an SNTP server. This requires the OpenScape Business X3/X5/X8 to be connected to the Central Office via ISDN lines and the system time to be obtained from the CO. In this case, OpenScape Business X3/X5/X8 must be first set up for use as an SNTP server (see the Administrator Documentation), and the IP address of the OpenScape Business X3/X5/X8 must then be entered in Linux as an SNTP server.

The IP phones receive the date & time automatically from the OpenScape Business S softswitch or, in the case of the OpenScape Business UC Booster Server, from the OpenScape Business X3/X5/X8 communication system. The date and time on the client PCs on which the OpenScape Business communications clients are installed must be synchronized with the OpenScape

Business S softswitch or the OpenScape Business X3/X5/X8 communication system (see the operating system instructions of the client PCs for details).

3.6.1 How to Configure an SNTP Server

Step by Step

1) Click on **Computer** in the task bar.
2) In the menu tree, click on **System > YaST**.
3) Enter the password for the root user and click **Continue**. The YaST2 Control Center is opened.
4) Click **System** in the menu tree.
5) In the **System** area, click on **Date and Time**.
6) Click **Change**.
7) Activate the **Synchronize with NTP Server** option.
8) Specify an NTP server:
   - **SNTP server on the internal network** (recommended)

     Enter the IP address, URL or DNS name of the SNTP server directly into the list box.
   - **SNTP Server on the Internet**

     Select the desired SNTP server from the **NTP Server Address** list or enter the URL or DNS name of the SNTP server directly into the list box.
   - **OpenScape Business X3/X5/X8 as SNTP server (only for OpenScape Business UC Booster Server)**

     Enter the IP address of the OpenScape Business X3/X5/X8 communication system directly in the list box.
9) Select the **Save NTP configuration** check box.
10) Click **Configure**.
11) Activate the **Now and On Boot** option.
12) Click **OK** followed by **Accept**.
13) Close the window with **OK**.
14) Close the **YaST2Control Center**.

3.7 Updates

To receive updates, it is necessary to register directly with Novell.

The installation and operation of the commercial SLES 11 SP4 64 Bit version is possible without registration. However, it is still important to register with Novell in order to obtain security patches and software updates.

A Novell Activation Code (registration code) can be procured via the order item "OpenScape Business SLES Upgrade Key". When ordering, you will receive a LAC (License Activation Key). Using this LAC, you can download the activation code at the CLS (Central License Server), with which you can then create an account with Novell. It is recommended that the customer account be set up before the Linux installation.

The following update variants are possible: Registering with Novell is a prerequisite.

- **Updates during the Linux installation (recommended)**
  During the Linux installation, updates and patches can be downloaded online from the Novell Download Server.
  Exception: Service Packs may not be installed.
- **Updates after installing Linux and before installing the communication software**
  After the Linux installation, updates and patches can be downloaded manually from the Novell Download Server using YaST (Software - Online Updates).
  Exception: Service Packs may not be installed.
- **Updates after installing the communication software**
  After the installation of the communication software, updates and patches can be downloaded automatically from the Novell Download Server. When performing these updates, any updates and patches that require a reboot of the Linux server (interactive updates) must be skipped. After every 2 or 3 update processes, it is recommended that a manual be started so that the skipped, interactive updates are also installed.
  The corresponding settings are made using YaST (Software - Online Updates).

Deviations from the previously mentioned variants are possible and are described in the Release Notice of the communication software.

3.7.1 How to Enable Automatic Online Updates

Step by Step

1) Click on **Computer** in the task bar.

2) In the menu tree, click on **System > YaST**.

3) Enter the password for the root user and click **Continue**. The YaST2 Control Center is opened.

4) Click on **Software** in the menu tree.

5) Click on **Online Update Configuration**.

6) Enable the **Automatic Online Update** check box and then select **daily**, **weekly** or **monthly** as the interval.

7) Select the **Skip Interactive Patches** check box.

8) Click **Finish**.

9) Close the **YaST2Control Center**.

3.7.2 How to Enable Online Updates Manually

Step by Step

1) Click on **Computer** in the task bar.

2) In the menu tree, click on **System > YaST**.

3) Enter the password for the root user and click **Continue**. The YaST2 Control Center is opened.

4) Click on **Software** in the menu tree.

5) Click on **Online Update** You will see a list of the available patches (**Needed Patches**) that are required. If you already have all the latest patches installed, this list will be empty.

6) Click on **Accept** to start the manual online update. The window will close automatically after the update.

7) Close the **YaST2Control Center**.

3.8 Backup and Restore

It is essential to back up the Linux operating system so it can be restored in an emergency.

After the initial startup and before each manual update, it is strongly recommended that an appropriate tool be used to create a full backup of the server PC and the affected partitions. If a fatal error occurs after an update, for example, the server PC would to be completely restored.

In a virtual environment, the entire virtual machine is to be copied.

If the entire server PC is backed up, the data of the communication software will be included in this backup. If only the operating system is backed up, the data of the communication software will also need to be backed up cyclically.

4 Initial Setup for OpenScape Business S

The initial setup of OpenScape Business S (also referred to as the Softswitch in short) is described here. This includes the integrating the softswitch and related components into the existing customer LAN as well as setting up Internet access for Internet telephony and configuring the connected stations.

For OpenScape Business S, the OpenScape Business communication software is installed on the Linux operating system SLES 11 SP4 64 Bit. The communication software can be operated directly on a Linux server or in a virtual environment with VMware vSphere or Microsoft Hyper-V. The installation of the Linux operating system is described in the installation guide *OpenScape Business, Installing the Linux Server*.

The initial setup of OpenScape Business S is carried out using the OpenScape Business Assistant administration program (web-based management, also called WBM in short).

This section describes the configuration of the most common components. Not all of these components may be used by you. During the initial setup, you may need to choose between multiple options in some places or even skip some configurations entirely, depending on which components you use.

The detailed administration of any features that are not covered by the initial setup is described in subsequent chapters.

The initial setup requires the creation of an IP address scheme and a dial plan.

Summary of the most important installation steps:

- System settings
- System Phone Numbers and Networking
- Internet Telephony
- Station configuration
- Licensing
- Data backup

4.1 Prerequisites for the Initial Setup

Meeting the prerequisites for the initial setup ensures the proper operation of OpenScape Business S.

General

Depending on the used hardware (phones, ...) and the existing infrastructure, the following general conditions apply:

- The LAN infrastructure (Internet routers, switches, etc.) is present and usable.
- The IP phones are connected to the customer LAN.

- The Linux server required for OpenScape Business S was installed as per the instructions in the *OpenScape Business Linux Server Installation Guide*, was integrated into the customer LAN, and is ready for use.
- All licenses required for OpenScape Business S are present (e.g., UC clients, Gate View, Directory Services, etc.).
- An IP address scheme exists and is known.
- A dial plan (also called a numbering plan) is present and known.

Software

The following software is required for the installation of OpenScape Business S:

- DVD or .ISO image with the OpenScape Business communication software
  Contains the OpenScape Business communication software. This DVD or .ISO image is included in the delivery package.
- DVD with Linux operating system SLES 11 SP4 64 bit
  The Linux DVD may be needed during the installation of the OpenScape Business communication software, since some software packages (RPM) required for the communication software may need to installed later from this DVD or .ISO image.

Administration

For the initial setup of OpenScape Business S with the OpenScape Business Assistant (WBM), the Linux server or the Admin PC can be used. The WBM is browser-based and is thus independent of the operating system.

- Web browsers:
  The following HTML 5-enabled web browsers are supported:
  - Microsoft Internet Explorer Version 11 and later (Admin PC).
  - Mozilla Firefox Version 37.x and 38.x
  - Mozilla Firefox ESR Version 24.x and 31.x
  - Google Chrome

  If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.
- Oracle Java:
  The latest version of Oracle Java must be installed. If an older version is installed, you will need to update it to the latest version before you can start setting up the system for the first time.
- Screen resolution: 1024x768 or higher

Firewall

When connected to the Internet, a firewall is needed for the Linux server to prevent unauthorized access from outside. After installing Linux, the Linux firewall is enabled. The installer of the communication software adjusts the firewall settings so that the communication software can be operated properly. The ports for the communication software are opened, and all other ports are closed.

If an external firewall is used in the network, the Linux firewall must be disabled, and the addresses and ports required for the communication software must be opened (see *Used Ports*).

Internet Access

The Server PC must have broadband Internet access for:

- Security patches and general Linux software updates

OpenScape Business requires an Internet connection for:

- OpenScape Business software updates
- OpenScape Business features such as Internet telephony, for example
- OpenScape Business Mobility Clients such as myPortal to go, for example
- Remote Service (SSDP)

E-mail Server (Optional)

OpenScape Business requires access to an e-mail server in order to send e-mails. For this purpose, the access data to the E-mail server must be entered in OpenScape Business, and the relevant accounts (IP address, URL, login data of the E-mail server) must be set up in the E-mail server.

If the e-mail functionality is not used within OpenScape Business, this data need not be entered.

Internet Telephony, VoIP (Optional)

If Internet telephony is used within OpenScape Business, then OpenScape Business will require broadband access to the Internet and to an Internet Telephony Service Provider (ITSP, SIP Provider) for SIP telephony over the Internet. To do this, the appropriate accounts must be obtained from the ITSP, and the access data for the ITSP (IP address, URL, login data of the SIP Provider) must be set up in OpenScape Business.

Second LAN Port

If OpenScape Business S (or the Linux server) has a second LAN port, you can use this as a WAN interface for Internet access and Internet telephony via an ITSP. The first LAN port is used as usual as a LAN interface for the internal phones and PCs. The configuration of Internet access occurs in the external Internet router of the customer LAN. The setup of the second LAN port occurs directly during the initial setup of Linux or can be performed later using YaST. In the WBM, the second LAN port only needs to be activated as a WAN interface.

Fax as PDF

If faxes are to be saved in PDF format, the server PC requires at least 4 GB RAM. If OpenScape Business S is being operated in a virtual environment, the virtual machine must also be assigned 4GB RAM.

4.2 Components

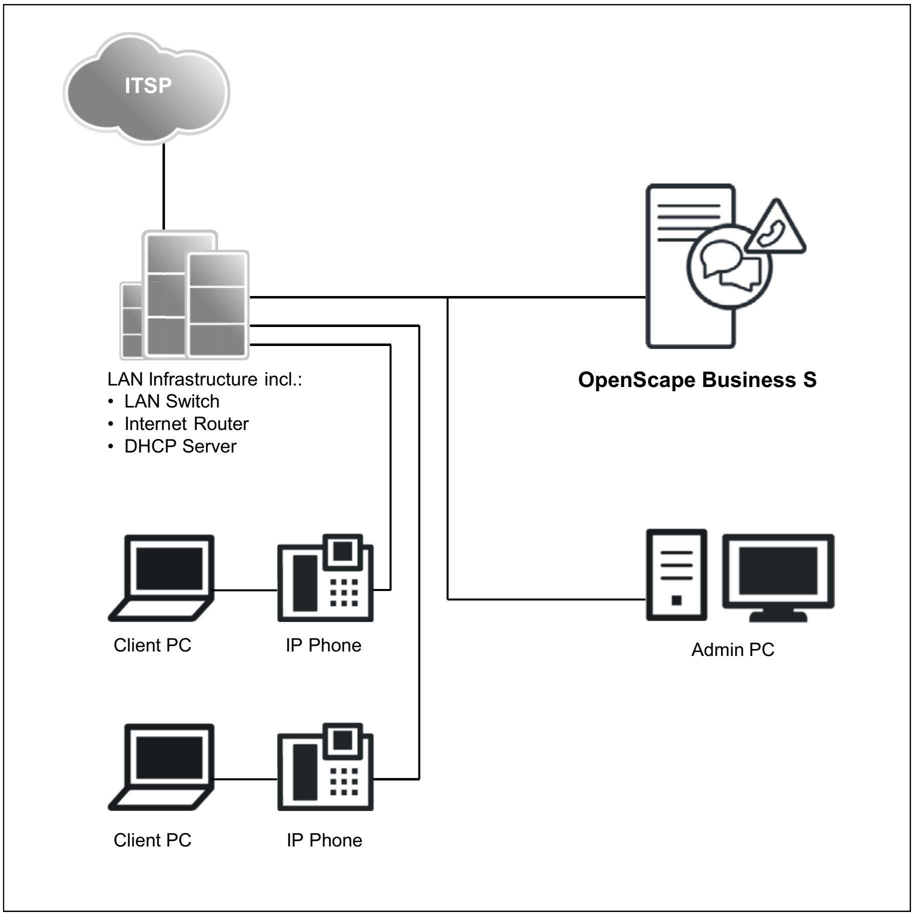
The various components of the installation example are described and outlined below.

The installation example includes the following components:

- OpenScape Business S
  The Linux server with the OpenScape Business S communication software is integrated in the existing customer LAN via its LAN interface.
- Admin PC
  The admin PC is also integrated in the existing customer LAN via its LAN interface.
- IP stations (IP clients)
  The IP stations (IP system phones, client PCs, WLAN Access Points, etc.) are integrated in the LAN via one or more switches.

The IP clients obtain their IP addresses dynamically from an internal DHCP server (DHCP server of the Linux server) or from an external DHCP server (DHCP server of the Internet router, for example).

Internet access is configured in the Internet router.



4.3 IP Address Scheme

An IP address scheme is a definition of how the IP addresses are used in the customer LAN. It includes the IP addresses of PCs, servers, Internet routers, IP phones, etc.

To provide a better overview of the assignment of IP addresses, an IP address scheme should be created.

Example of an IP address scheme with the IP address range `192.168.5.x`:

IP address range	Clients
192.168.5.1 through **192.168.5.49**	Clients with a fixed IP address
192.168.5.1	Internet router (gateway)
192.168.5.10	Server PC (OpenScape Business S)
192.168.5.20	E-mail server
192.168.5.100 to **192.168.5.254**	Client PCs & IP phones, also the IP address range of the DHCP server; IP addresses are assigned automatically to the clients

4.4 Dial Plan

A dial plan is a list of all phone numbers available in the communication system. It comprises internal phone numbers, DID numbers, and group station numbers.

Default Dial Plan

The internal call numbers are preassigned default values. These values can be adapted to suit individual requirements as needed (e.g., to create individual dial plans).

Extract from the default dial plan:

Type of call numbers	Default call numbers
Internal station numbers	100-349, 500-709
User direct inward dialing numbers	100-349, 500-709
Group station numbers	350-439
Voicemail call number	71
Announcement Player call number	72
Seizure codes (external codes): Central Office ITSP	 855-858
Call number for conferences	7400-7404
Call number for parking	7405
Call number for AutoAttendant	7410-7429
Call number for MeetMe conference	7430

Individual Dial Plan

An individual dial plan can be imported in the WBM via an XML file during the basic configuration.

The XML file contains several tabs. Besides the names and phone numbers of subscribers, the "Customer" tab also includes additional subscriber data such as the subscriber types and e-mail addresses of the subscribers.

A sample XML file with the appropriate explanations can be found in the WBM under **Service Center > Documents > Templates > CSV Templates**. You can also use the XML file stored there as a template for your data. It can be edited with Microsoft Excel, for example.

4.5 Installing the Communication Software

The OpenScape Business S communication software is installed on the Linux server.

Make sure that the IP addresses and network masks to be configured are appropriate for the customer LAN.

DHCP Server

A DHCP server automatically assigns a unique IP address to each IP station (IP phones, PCs, etc.) and provides the IP stations with network-specific data such as the IP address of the default gateway, for example.

Either an external DHCP server (e.g., the DHCP server of the Internet router or of the communication system) or the DHCP server of the Linux server can be used as a DHCP server. If the DHCP server of the Linux server is used, the external DHCP server must be disabled. The configuration of the Linux DHCP server can be performed during the installation of the OpenScape Business communication software.

Virtual Environment

The communication software can run in a virtual environment. There are two ways to perform the installation:

- Separate installation of Linux and the communication software
  To do this, the virtualization software (host operating system) must be first installed and configured on the server PC. Linux is installed in the virtual environment as a guest operating system. Within the Linux operating system, the communication software is installed last with the help of the OpenScape Business DVD or .ISO file (see *OpenScape Business Linux Server, Installation Guide* for more details).
- Combined installation of Linux and the communication software (VMWare only)
  To do this, the virtualization software (host operating system) must be first installed and configured on the server PC. An OVA image (Open Virtualization Appliance), which includes Linux and the communication software, is installed

in the virtual environment. The OVA image is provided through the software supply server (SWS).
For more than 50 users, the home partition must be resized after the installation to 100 GB (for 50 to 100 users) or 200 GB (for up to 500 users or for OpenScape Business Contact Center) or 500 GB (for more than 500 users).
For Linux updates, you will also need the OpenScape Business SLES upgrade key in order to be able to register with Linux.

Use of snapshots on virtual machines (VM):

Snapshots can be a valuable maintenance mechanism, for example, to perform a fast rollback to a predefined operating state of the VM after a mass distribution script has failed.

- Snapshots cannot be created during normal operation. The current operating state of the virtual machine is frozen while taking a snapshot. Consequently, connected terminals and applications such as IP phones or the UC clients may lose the connection to the server.
- Snapshots can cause internal server processes to lose their synchronization, which means that the stable operation of the communication system can then no longer be guaranteed. A server reboot following the snapshot should therefore also be planned within the maintenance timeframe.
- Previous snapshots should not remain on the production environment during normal operation.
- Snapshots can be taken during a planned maintenance window or within the framework of the installation.
- Snapshots are used internally by backup tools such as VDP or VDR. It must be ensured that these backup operations are schedules outside of business hours and that the snapshots generated by these tools are deleted at the end of the operation.

More information regarding snapshots can be found in the VMware knowledge base (KB). A good starting point is the KB article 1025279 – Best Practices for virtual machine snapshots in the VMware environment (`http://kb.vmware.com/kb/1025279`).

All information about snapshots in Microsoft Hyper-V can be found in the technet library at technet.microsoft.com within the Hyper-V chapter.

4.5.1 How to Install the Communication Software

Prerequisites

- The SLES 11 SP4 64 bit operating system has been correctly installed and started on the Linux server.
- DVD or .ISO file with OpenScape Business communication software.
- DVD or .ISO file with the Linux operating system SLES 11 SP4 64 bit for any subsequent installation of software packages (RPM) that may be required.
- The root access data (user name and password) for logging into the Linux server is available.

IMPORTANT: The OpenScape Business communication software overwrites any existing configuration files (e.g., for DHCP, FTP, Postfix, etc.) during the installation.

Step by Step

1) Log into the Linux server with root privileges.

2) Insert the OpenScape Business DVD or .ISO file into the DVD drive.

3) Confirm the message with **Run**. The "Welcome" window appears.

4) Select the desired setup language (e.g., **English**) and click **Start**. The rest of the installation is described here for the English language.

5) Select the desired product from the list and click on **Select**. A check is performed to determine whether the hardware meets all the requirements for the installation. A warning is displayed for minor shortfalls in meeting the requirements. After confirmation, the installation can then be continued. For severe shortfalls, the installation is canceled automatically.

6) A check is performed to determine whether additional RPM packages need to be installed. If yes, confirm this with **Confirm**. If this occurs, you will need to switch back to the SLES 11 DVD or .ISO file later.

7) A window with the terms of the license (i.e., the End User License Agreement or EULA) appears. Read the terms of the license and accept the license agreement with **Yes**.

8) If a DHCP server is already present in the customer LAN (e.g., the DHCP server of the Internet router), stop the configuration of the Linux DHCP server here with **No** and proceed to step 12 to continue.

INFO: In order to ensure that the software of system telephones can be updated automatically even when using an external DHCP server, you have two options:

a) The IP address of the Linux server must be entered as the DLS address at each system telephone.

b) The network-specific data must be entered at the external DHCP server. The parameters for this can be found under `/var/log/OPTI.txt`.

---

9) If you want to use the Linux DHCP server, click on **Yes** to enable and configure the Linux DHCP server.

10) Enter the following values (preset with default values):

- **Default Route**: IP address of the default gateway; as a rule, the IP address for the Internet router, e.g., `192.168.5.1`.
- **Domain** (optional): the domain specified during the Linux installation, e.g., `<customer>.com`
- **DNS-Server** (optional): IP address of the DNS server specified during the Linux installation. If no DNS server is available in the internal network, you can enter the IP address of the Internet router (e.g., `192.168.5.1`) here.
- **SNTP Server**: IP address of the internal or external NTP server.
- **DLS/DLI Server**: IP address of DLS server, i.e., the IP address of the Linux server (e.g.: `192.168.5.10`).
- **Subnet**: appropriate subnet for the IP address range, e.g.: `192.168.5.0`.
- **Netmask**: Subnet mask of the Linux server that was specified during the Linux installation, e.g.: `255.255.255.0`.
- **IP range begin** and **IP range end**: IP address range from which the DHCP server may assign IP addresses, e.g.: `192.168.5.100` to `192.168.5.254`.

11) Click on **Continue**.

12) After the installation, the Linux operating system needs to be restarted. Select the check box **PC Reboot** and confirm with **Continue**.

13) If additional RPM packages need to be installed, you will be prompted to insert the SLES 11 DVD or .ISO file. Insert the DVD or .ISO file and confirm with **Continue**. Following the successful installation of the RPM packages, reinsert the OpenScape Business DVD or .ISO file and confirm this with **Continue**, followed by **Run**.

14) The OpenScape Business communication software is installed. The operating system then automatically performs a restart.

15) After the restart, log in with the user account that was set up earlier during the Linux installation.

16) Right-click on the DVD drive icon on the desktop and select the menu item **Eject**. Remove the OpenScape Business DVD from the DVD drive.

> ***INFO:*** It takes a few minutes until all components of the OpenScape Business communication software are active. Using the OpenScape Observer, you can check when the OpenScape Business communication software is ready for use.

4.6 Function Check with the OpenScape Observer

The OpenScape Observer program can be used to check whether OpenScape Business is operational.

OpenScape Observer can be started from the Admin PC or from a client PC in the internal network. To do this, the program must be copied from the Service Center of the WBM to the PC.

4.6.1 How to Copy OpenScape Observer to the PC

Prerequisites

- The OpenScape Business communication software is installed.
- The latest Oracle Java version is installed on the PC.

Step by Step

1) Start the web browser on the PC and open the login page of the WBM at the following address:

`https://<IP address of the Linux server>`, e.g., `https://192.168.5.10`.

2) If the browser reports a problem with a security certificate, install the certificate (using the example of Internet Explorer V10).

a) Close the web browser.

b) Open the web browser with administrator rights by clicking the right mouse button on the web browser icon and selecting the menu item **Run as administrator** from the context menu.

c) Allow the User Account Control.

d) Open the login page of the WBM at the following address:

`https://<IP address of the Linux server>`, e.g., `https://192.168.5.10`.

e) Click on **Continue to this website**.

f) Click on the message **Certificate Error** in the navigation bar of the web browser.

g) Click on **View Certificates**.

h) Click on **Install Certificate** (only visible with administrator rights).

i) Select the option **Local Computer** and confirm with **Next**.

j) Select the option **Place all certificates in the following store**, click **Browse** and specify **Trusted Root Certification Authorities**.

k) Confirm with **OK** and then with **Next** and **Finish**.

l) Confirm the certificate import with **OK** and close the certificate window **OK**.

m) Close the web browser.

n) Start the web browser again (without administrator rights) and open the login page of the WBM at the following address:

`https://<IP address of the Linux server>`, e.g., `https://192.168.5.10`.

3) Click on the language code at the top right and select the language in which the user interface of the WBM is to be displayed from the menu. The Login page will be displayed in the selected language.

4) In the field under **Login**, enter the default user name `administrator@system` for access as an administrator.

> ***INFO:*** If you press the tab key after entering `administrator`, `@system` will be added automatically.

5) In the second field under **Login**, enter the default password `administrator` for access as an administrator.

6) Click **Login**.

7) You are prompted to change the default password.

a) Reenter the default password **administrator** in the `Password` field.

b) Enter a new password in the **New Password** and **Confirm New Password** fields to protect the system against misuse. Note case usage and the status of the **Num** key. The password is displayed as a string of asterisks (*).

> ***INFO:*** The password must be at least 8 characters long and include a digit. Make sure that you remember your new password.

8) Click **Login**.

9) Click **Service Center** on the navigation bar.

10) Click in the **Software** area on the item **OpenScape Observer**.

11) Save the file `OsoObserver.jar` on the PC in a directory of your choice.

4.6.2 How to Start OpenScape Observer from the PC

Prerequisites

- The file `OsoObserver.jar` is stored on the client PC.

Step by Step

1) Navigate on the PC to the storage path of OpenScape Observer.
2) Double-click on the file `OsoObserver.jar`. OpenScape Observer opens as a small window in the upper left corner of the screen.
3) Enter the IP address of the Linux server on which the OpenScape Business communication software is installed (e.g., `192.168.5.10`) in the field of the OpenScape Observer.
4) Click on **Connect OSO**.
5) Another window opens with the following contents:
   - IP address of the Linux server (in the header)
   - Version number of the installed OpenScape Business communication software
   - Version of the Linux server operating system
   - Utilization of the home partition (`HD`) and memory (`RAM`) of the Linux server as a percentage
   - Abbreviation of the installed product (e.g., `S` for OpenScape Business S and `B` for the UC Booster Server)
6) In the window you will also be informed about the status of OpenScape Business with an LED display:
   - Red LED: The OpenScape Business system components cannot be started - OpenScape Business is not ready for use
   - Yellow LED: The OpenScape Business system components have started - OpenScape Business is not yet ready for use
   - Green LED: The OpenScape Business system components have started - OpenScape Business is ready for use

4.7 Starting Up

The basic settings are made using the **Initial Installation** wizard of the WBM.

4.7.1 How to Start the Initial Installation Wizard

Prerequisites

- The WBM has been started.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) Click on **Edit** to start the **Initial Installation** wizard.

> ***INFO:*** If the size of the browser window cannot display the workspace in its entirety at low screen resolutions, a horizontal or vertical scroll bar appears at the sides and can be used to scroll to the required section.

Next steps

Perform initial installation as described in the following step-by-step instructions. Fields that are not described here are preset for the default scenario and should only be changed if they are not appropriate for your network data. For detailed information, refer to the descriptions provided in the Administrator documentation for the individual wizards.

4.7.2 System Settings

The **System Settings** window is used to configure the system settings of the communication system.

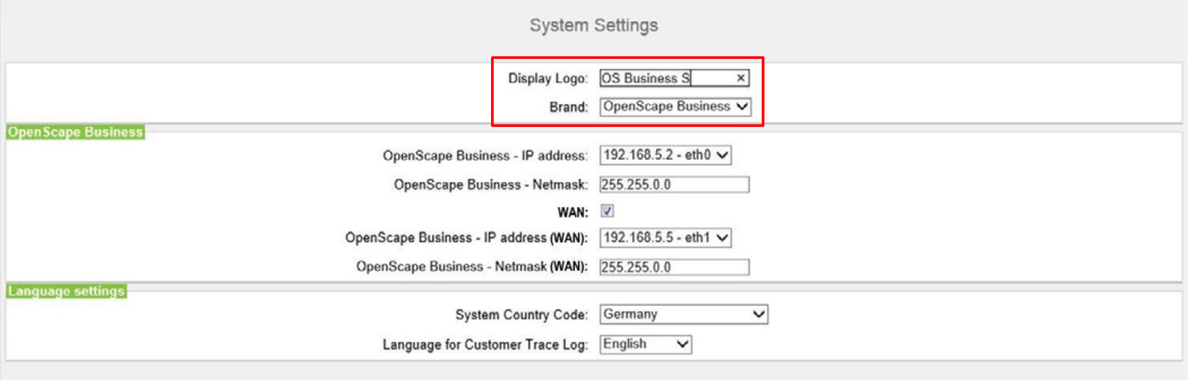
Proceed as follows:

1. Set the display logo and the product name
   Specify a display text to be displayed on the display of the system phones. Additionally, you can also select the product name.
2. Select the country code and the language to be used for event logs
   For country initialization to work correctly, you must select the country in which the communication system is operated. In addition, you can select the language in which the event logs (system event logs, errors logs, etc.) are to be stored.
3. Only if required: Activate another LAN port as a WAN interface
   If OpenScape Business S (or the Linux server) has a second LAN port, you can use this as a WAN interface for Internet access and Internet telephony via an ITSP. The first LAN port is used as usual as a LAN interface for the internal phones and PCs.

4.7.2.1 How to Set the Display Logo and the Product Name

Prerequisites

- You are in the **System Settings** window.



System Settings

Display Logo: OS Business S

Brand: OpenScape Business

OpenScape Business

OpenScape Business - IP address: 192.168.5.2 - eth0

OpenScape Business - Netmask: 255.255.0.0

WAN: ☑

OpenScape Business - IP address (WAN): 192.168.5.5 - eth1

OpenScape Business - Netmask (WAN): 255.255.0.0

Language settings

System Country Code: Germany

Language for Customer Trace Log: English

Step by Step

1) In the **Display Logo** field, enter a text of your choice (e.g., OS Business S). The text can contain up to 16 characters. Avoid the use of diacritical characters such as umlauts and special characters.

2) Select the desired time product name in the **Brand** drop-down list.

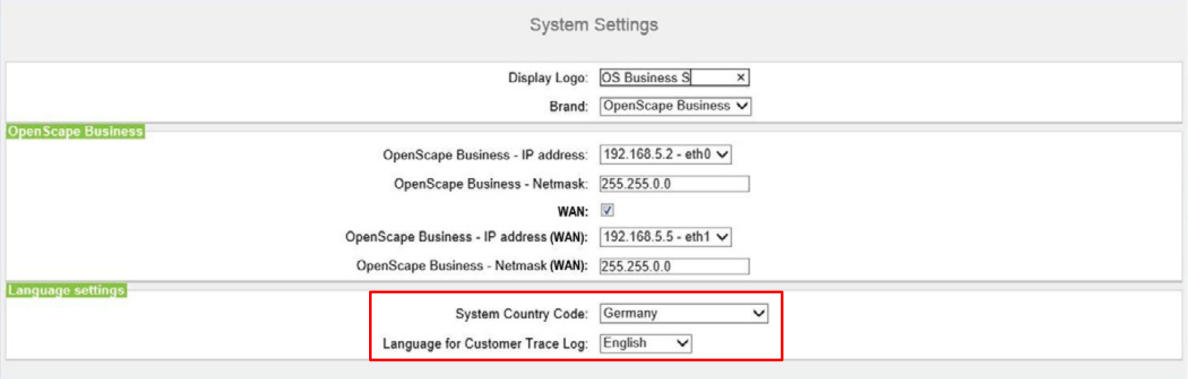
Next steps

Select the country code and language to be used for the event logs.

4.7.2.2 How to Select the Country Code and the Language for Event Logs

Prerequisites

- You are in the **System Settings** window.



System Settings

Display Logo: OS Business S

Brand: OpenScape Business

OpenScape Business

OpenScape Business - IP address: 192.168.5.2 - eth0

OpenScape Business - Netmask: 255.255.0.0

WAN: ☑

OpenScape Business - IP address (WAN): 192.168.5.5 - eth1

OpenScape Business - Netmask (WAN): 255.255.0.0

Language settings

System Country Code: Germany

Language for Customer Trace Log: English

Step by Step

1) In the **System Country Code** drop-down list, select the country where the communication system is operated.

2) In the **Language for Customer Event Log** field, enter the language in which the event logs (system event logs, error logs, etc.) are to be output.

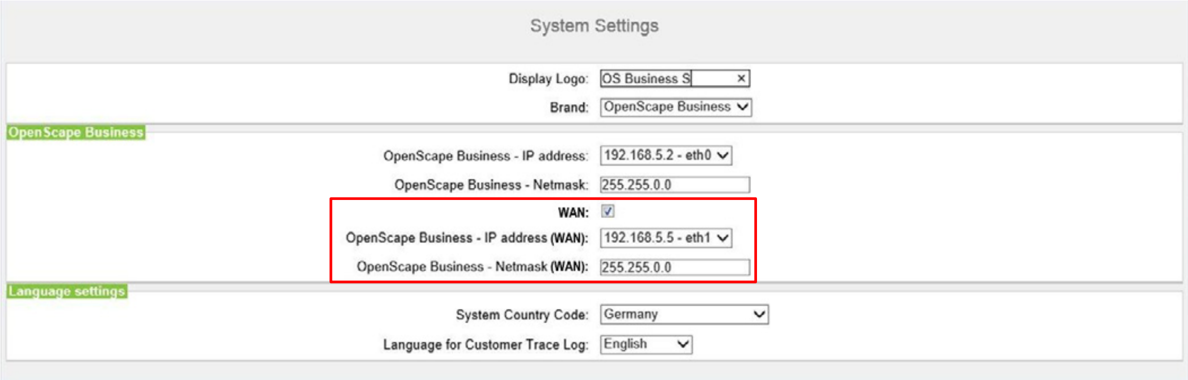
Next steps

Start the basic configuration.

4.7.2.3 How to Activate an Additional LAN Port as a WAN Interface

Prerequisites

- You are in the **System Settings** window.



System Settings

Display Logo: OS Business S ×
Brand: OpenScape Business

OpenScape Business

OpenScape Business - IP address: 192.168.5.2 - eth0
OpenScape Business - Netmask: 255.255.0.0
WAN: ☑
OpenScape Business - IP address (WAN): 192.168.5.5 - eth1
OpenScape Business - Netmask (WAN): 255.255.0.0

Language settings

System Country Code: Germany
Language for Customer Trace Log: English

Step by Step

1) Select the **WAN** check box.

2) Select the desired LAN port (e.g., `eth1` or `eth2`) from the **OpenScape Business - IP Address (WAN)** drop-down list. If only two LAN ports are available, the second LAN port `eth1`is activated automatically.

> ***INFO:*** The assignment of IP addresses and subnet masks to the LAN ports is done during the initial installation of Linux or subsequently via YaST.

Next steps

Specify UC solution.

4.7.3 UC Solution

In the **Change application selection** window, select the UC solution to be used.

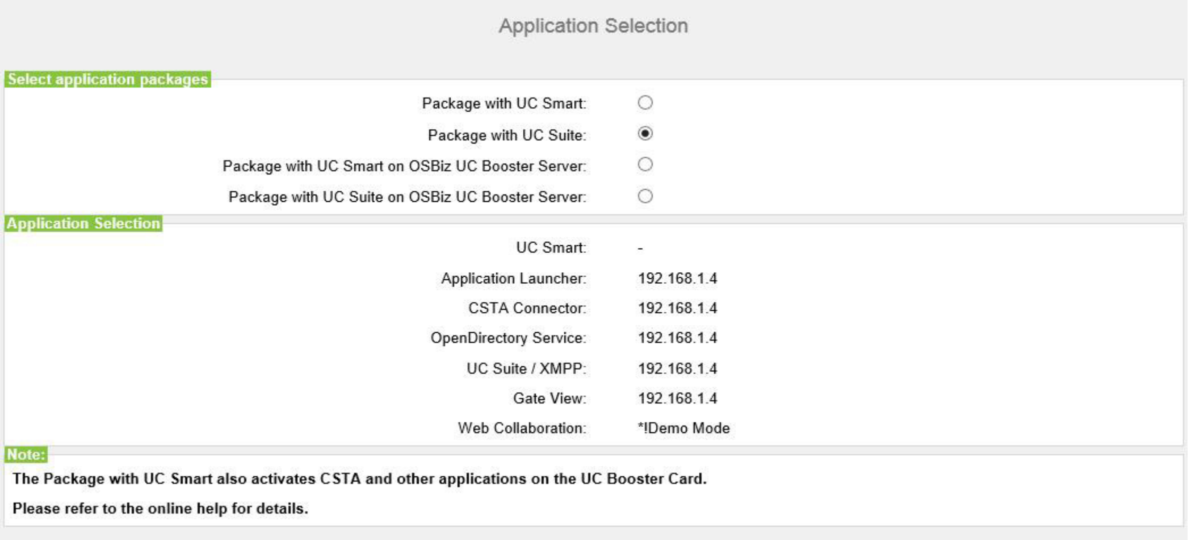
You have the following options:

- **Package with UC Smart**
  The UC solution UC Smart is integrated in OpenScape Business S.
- **Package with UC Suite**
  The UC solution UC Suite is integrated in OpenScape Business S.

4.7.3.1 How to Define the UC Solution

Prerequisites

- You have purchased licenses for either of the UC solutions, UC Smart or UC Suite.
- You are in the **Change application selection** window.



Application Selection

Select application packages

Package with UC Smart:	○
Package with UC Suite:	●
Package with UC Smart on OSBiz UC Booster Server:	○
Package with UC Suite on OSBiz UC Booster Server:	○

Application Selection

UC Smart:	-
Application Launcher:	192.168.1.4
CSTA Connector:	192.168.1.4
OpenDirectory Service:	192.168.1.4
UC Suite / XMPP:	192.168.1.4
Gate View:	192.168.1.4
Web Collaboration:	*!Demo Mode

Note:

The Package with UC Smart also activates CSTA and other applications on the UC Booster Card.

Please refer to the online help for details.

Step by Step

1) If you use the UC solution UC Smart, click **Package with UC Smart**.
2) If you are using the UC solution UC Suite, click on **Package with UC Suite**.
3) Click on **OK & Next**.
4) The **Initial installation** wizard is closed. Click on **Finish**.

Next steps

Start the basic configuration.

4.8 Basic Configuration

The **Basic Installation** wizard is used for basic configuration. Basic configuration includes the most important settings for operating the communication system.

The Basic Installation Wizard includes a progress indicator showing the current step, as well as the steps that follow.

4.8.1 How to Start the Basic Installation Wizard

Prerequisites

- The **Initial installation** has been completed.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) Click on **Edit** to start the **Basic Installation** wizard.

Next steps

Perform basic installation as described in the following step-by-step instructions. Fields that are not described here are preset for the default scenario and should only be changed if they are not appropriate for your network data. For detailed information, refer to the descriptions provided in the Administrator documentation for the individual wizards.

4.8.2 System Phone Numbers and Networking

Enter the system phone numbers (PABX number, country and area code, international prefix) in the **Overview** window and specify whether OpenScape Business is to be networked with other OpenScape Business systems.

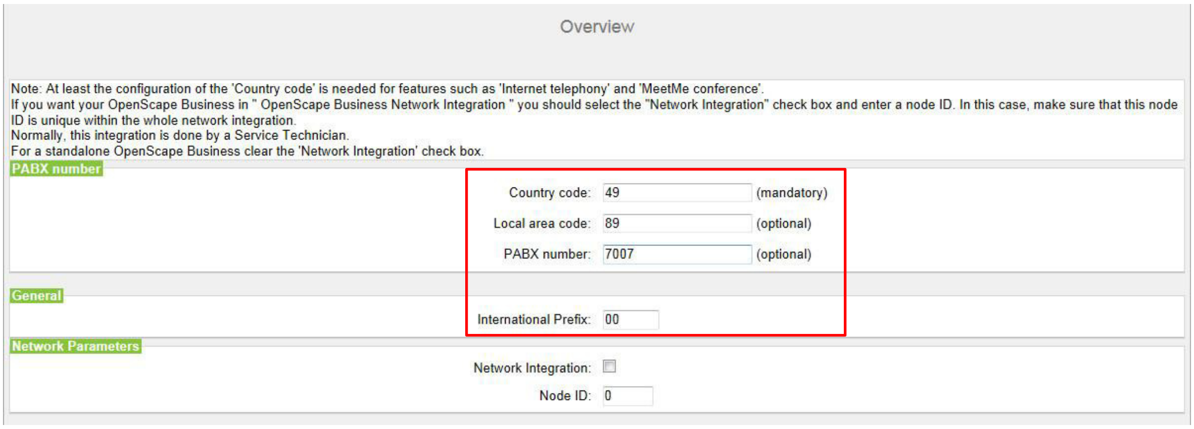
Proceed as follows:

1. Enter system phone numbers
   - Enter system phone numbers for point-to-point connection
     Here you enter the system phone number for your point-to-point connection and the country code and area code.
     The entry of the country code is mandatory for Internet telephony and conference server functionality.
     The international prefix is preset, depending on the previously dialed country code.
   - Enter system phone numbers for point-to-multipoint connection
     Here you enter the country code and area code for your point-to-multipoint connection.
     The entry of the country code is mandatory for Internet telephony and Meet-Me conferences.
     The international prefix is preset, depending on the previously dialed country code.
2. Activate or deactivate networking
   If OpenScape Business is to be networked with other OpenScape Business systems, networking must be enabled, and OpenScape Business must be assigned a node ID. Every OpenScape Business must have a unique node ID in the network.

4.8.2.1 How to Enter the System Phone Numbers for a Point-to-Point connection

Prerequisites

- You have a point-to-point connection.
- You are in the **Summary** window.



Overview

Note: At least the configuration of the 'Country code' is needed for features such as 'Internet telephony' and 'MeetMe conference'.
If you want your OpenScape Business in " OpenScape Business Network Integration " you should select the "Network Integration" check box and enter a node ID. In this case, make sure that this node ID is unique within the whole network integration.
Normally, this integration is done by a Service Technician.
For a standalone OpenScape Business clear the 'Network Integration' check box.

PABX number

Country code: 49 (mandatory)
Local area code: 89 (optional)
PABX number: 7007 (optional)

General

International Prefix: 00

Network Parameters

Network Integration: □
Node ID: 0

Step by Step

1) In the **Country Code** field, enter the country code prefix, e.g., `49` for Germany or `1` for the U.S.

2) Enter the local area code, e.g., `89` for Munich, in the **Local area code** field.

3) Enter the system phone number of your trunk connection, e.g., `7007` (your connection number), in the **PABX number** field.

4) Change the **International Prefix** field only if required. The applicable values for Germany and the United States are `00` and `011`, respectively.

   For international calls, the phone number is preceded by the international prefix and the country code, e.g., "00-1-..." for calls from Germany to the USA and "011-49-..." for calls from the USA to Germany.

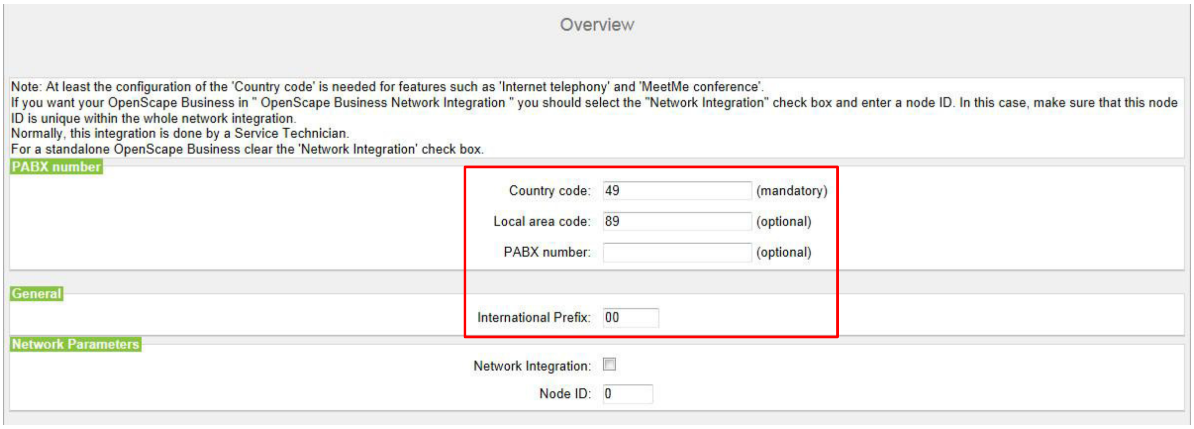
Next steps

Activate or deactivate networking

4.8.2.2 How to Enter the System Phone Numbers for a Point-to-Multipoint Connection

Prerequisites

- You have a point-to-multipoint connection.
- You are in the **Summary** window.



Overview

Note: At least the configuration of the 'Country code' is needed for features such as 'Internet telephony' and 'MeetMe conference'.
If you want your OpenScape Business in " OpenScape Business Network Integration " you should select the "Network Integration" check box and enter a node ID. In this case, make sure that this node ID is unique within the whole network integration.
Normally, this integration is done by a Service Technician.
For a standalone OpenScape Business clear the 'Network Integration' check box.

PABX number

Country code: 49 (mandatory)
Local area code: 89 (optional)
PABX number: (optional)

General

International Prefix: 00

Network Parameters

Network Integration: □
Node ID: 0

Step by Step

1) In the **Country Code** field, enter the country code prefix, e.g., `49` for Germany or `1` for the U.S.

2) Enter the local area code, e.g., `89` for Munich, in the **Local area code** field.

3) Leave the **PABX number** field empty.

4) Change the **International Prefix** field only if required. The applicable values for Germany and the United States are `00` and `011`, respectively.

   For international calls, the phone number is preceded by the international prefix and the country code, e.g., "00-1-..." for calls from Germany to the USA and "011-49-..." for calls from the USA to Germany.

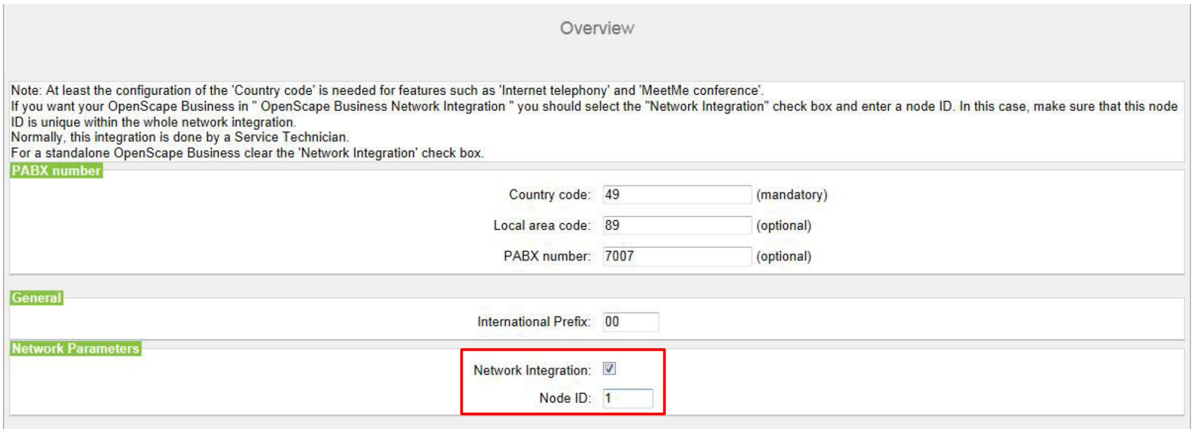
Next steps

Activate or deactivate networking

4.8.2.3 How to Activate or Deactivate Networking

Prerequisites

- You are in the **Summary** window.



Overview

Note: At least the configuration of the 'Country code' is needed for features such as 'Internet telephony' and 'MeetMe conference'.
If you want your OpenScape Business in " OpenScape Business Network Integration " you should select the "Network Integration" check box and enter a node ID. In this case, make sure that this node ID is unique within the whole network integration.
Normally, this integration is done by a Service Technician.
For a standalone OpenScape Business clear the 'Network Integration' check box.

PABX number

Country code: 49 (mandatory)
Local area code: 89 (optional)
PABX number: 7007 (optional)

General

International Prefix: 00

Network Parameters

Network Integration: ☑
Node ID: 1

Step by Step

1) If the communication system is to be networked with other communication systems:
   a) Select the **Network Integration** check box.
   b) In the **Node ID** field for the communication system, enter a node ID that is unique in the internetwork (digits from `1` through `100` are possible).
2) If the communication system is not to be networked with other communication systems, leave the **Network Integration** check box disabled.
3) Click on **OK & Next**.

Next steps

Configure the station data.

4.8.3 Station Data

If necessary, you can configure your own individual dial plan instead of the predefined default dial plan in the **Central Functions for Stations** window and import additional station data. In an internetwork, the default dial plan must be adapted to the dial plan of the internetwork.

The default dial plan contains predefined numbers for different types of stations (IP phones, analog phones, ...) and for special functions (Internet telephony, voicemail box, AutoAttendant, ...).

The station data includes the internal call numbers, DID numbers and names of the stations. This data and other station data can be imported into the communication system during the basic configuration via an XML file in UTF-8 format.

> ***INFO:*** An XML template with the appropriate explanations can be found in the WBM under **Service Center > Documents > CSV Templates**. You can enter your data in this template by using Microsoft Excel, for example.

You have the following options:

- **Configure station data without an internetwork**
  Proceed as follows:
  a) Display the station data
     You can have all preconfigured station numbers and station data displayed.
  b) Delete all station numbers (optional)
     If you use an individual dial plan, you must delete all preconfigured station numbers.

c) Adapt preconfigured station numbers for the individual dial plan (optional)
If you are using an individual dial plan, you can adapt the preconfigured phone numbers to your own dial plan.

d) Import station data from an XML file (optional)
You can easily import your individual station numbers, including any additional station data, during the basic configuration via an XML file.

- **Configure station data with an internetwork**
  Proceed as follows:

  a) Delete all station numbers
  If the UC Suite is used in an internetwork, a closed numbering plan is required, i.e., all station numbers in the internetwork must be unique. For this reason, any preconfigured station numbers must be deleted and only stations numbers adapted for the internetwork must be used.

  b) Import station data from an XML file
  The station numbers adapted for the internetwork and any additional station data can be easily imported during the basic configuration via an XML file. This file can contain all stations in the internetwork. During import, only the station numbers and the station data assigned to the previously specified node ID of the communication system will be transferred.

4.8.3.1 How to Display the Station Data

Prerequisites

- You are in the **Central Functions for Stations** window.

Step by Step

1) Select the **Display stations configuration** radio button.

2) Click on **Execute function**. A list of stations with the preconfigured phone numbers (default dial plan) is displayed.

3) Click on **OK**. You are taken back to the **Central Functions for Stations** window.

4) If you do not want to change any station data, click **OK & Next**.

4.8.3.2 How to Delete all Call Numbers

Prerequisites

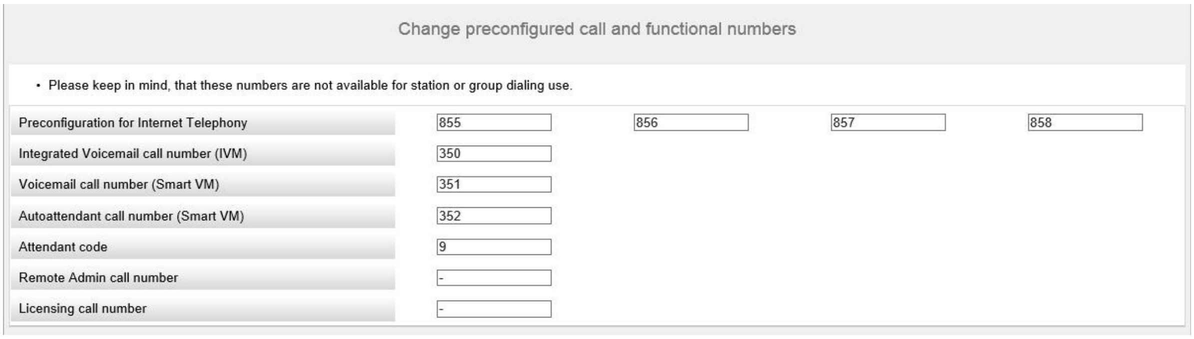
- You are in the **Central Functions for Stations** window.

Step by Step

1) Enable the radio button **Delete all station call numbers**.

2) Enable the check box **Delete All Call Addresses**.

3) Click on **Execute function**. All preset call numbers are deleted. The **Change preconfigured call and functional numbers** window then appears.



Change preconfigured call and functional numbers

- Please keep in mind, that these numbers are not available for station or group dialing use.

Preconfiguration for Internet Telephony	855	856	857	858
Integrated Voicemail call number (IVM)	350			
Voicemail call number (Smart VM)	351			
Autoattendant call number (Smart VM)	352			
Attendant code	9			
Remote Admin call number	-			
Licensing call number	-			

4) Adjust the codes and special call numbers to suit your preferences, and then click **OK**. You are taken back to the **Central Functions for Stations** window.

5) If you do not want to change any further station data, click **OK & Next**.

4.8.3.3 How to Adapt Preconfigured Station Numbers for the Individual Dial Plan

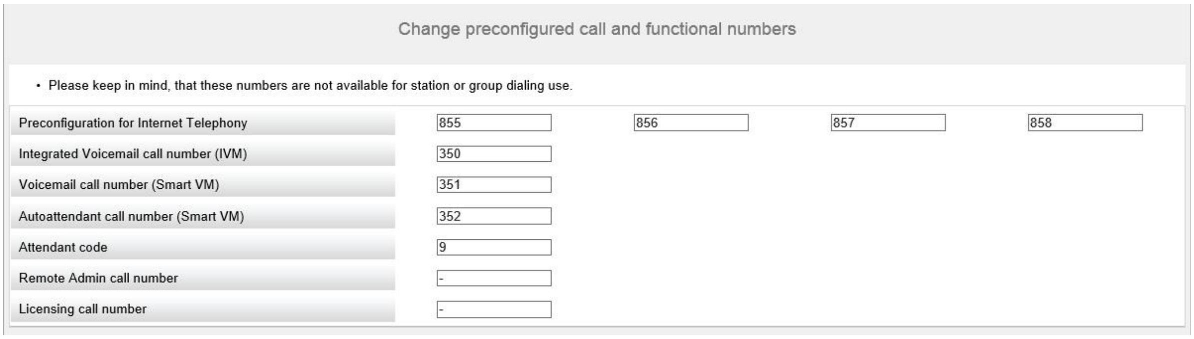
Prerequisites

- You are in the **Central Functions for Stations** window.

Step by Step

1) Enable the radio button **Change pre-configured call and functional numbers**.

2) Click on **Execute function**. The **Change preconfigured call and functional numbers** window appears.



Change preconfigured call and functional numbers

- Please keep in mind, that these numbers are not available for station or group dialing use.

Preconfiguration for Internet Telephony	855	856	857	858
Integrated Voicemail call number (IVM)	350			
Voicemail call number (Smart VM)	351			
Autoattendant call number (Smart VM)	352			
Attendant code	9			
Remote Admin call number	-			
Licensing call number	-			

3) Adjust the preconfigured call numbers to suit your preferences, and then click **OK**. You are taken back to the **Central Functions for Stations** window.

4) If you do not want to change any further station data, click **OK & Next**.

4.8.3.4 How to Import the Station Data from an XML File

Prerequisites

- You are in the **Central Functions for Stations** window.
- An XML file with the entered data is available in UTF-8 format. An XML template can be found under **Service Center > Documents > CSV Templates**.

Step by Step

1) Enable the radio button **Import XML file with station data**.
2) Click **Execute function**.
3) Use **Browse** to select the created XML file and click **Open**.
4) Click **OK** when finished. The station data is imported.
5) Click **OK & Next**.

4.8.4 Internet Telephony

The **Provider configuration and activation for Internet telephony** window is used to configure Internet telephony. You can configure predefined or new Internet Telephony Service Providers (ITSPs). You can configure one or several accounts for each ITSP. Up to 8 ITSPs may be active simultaneously.

You have the following options:

- **Configure a predefined ITSP**
  You can use predefined ITSP templates. To do this, the own access data and phone numbers are entered in the template, and this is then activated.
- **Configure a new ITSP**
  You can also add and activate a new ITSP.
  Configuring a new ITSP is seldom required and can be very time-consuming. This option is therefore not described in the initial installation. Detailed information can be found in the chapter *Administrator Documentation, Connecting to Service Providers*.
- **Disable Internet telephony**
  You can disable Internet telephony.

> ***INFO:*** Configuration examples can be found on the Internet at the **Unify Experts Wiki** under *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Assigning the ITSP Phone Numbers

- In the case of an **Internet Telephony Station Connection**, the ITSP provides individual numbers such as 70005555, 70005556, etc. These individual call numbers are then assigned manually as the internal call numbers of the subscribers.

- In the case of an **Internet telephony point-to-point connection**, the ITSP provides a call number range, e.g., (+49) 89 7007-100 to (+49) 89 7007-147. The call numbers from the range are then assigned manually as the internal call numbers of the subscribers.

These two connection types can be combined as appropriate.

Alternatively, the ITSP phone numbers can be entered as the DID call numbers of the subscriber for both connection types during the station configuration.

Internal call number	Name	DID
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

The ITSP call numbers thus result from the configured PABX number (e.g., country code 49) and the entered DID numbers in long format. This has advantages for the digit analysis and call management, even in an internetwork. The ITSP connection is thus DID-enabled for another node, for example.

A further CO trunk connection via ISDN is only possible to a limited extent in this case (useful for emergency calls, for example).

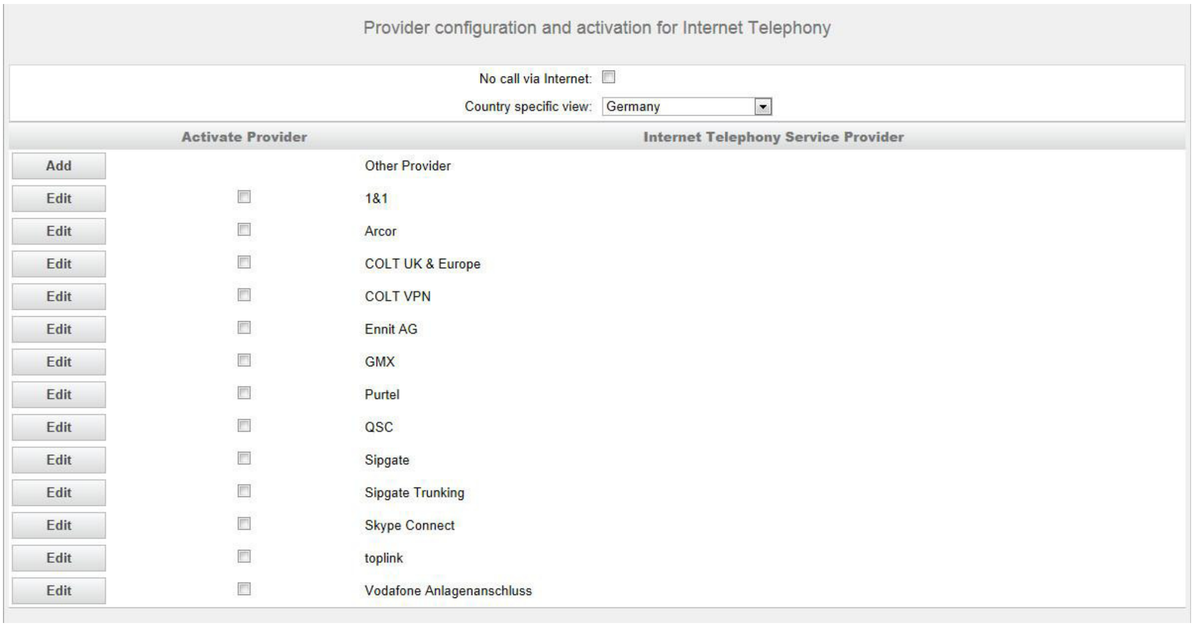
4.8.4.1 How to Configure a Predefined ITSP

Prerequisites

- You are in the **Provider configuration and activation for Internet Telephony** window.
- The Internet connection is operational.
- Your ITSP's Internet telephony access data is available (for example, user account, password and Internet telephony numbers).

Step by Step

1) Clear the **No call via Internet** check box. A country-specific list of the possible ITSPs is displayed. The list contains the predefined ITSPs for the selected country and any already created ITSPs.



Provider configuration and activation for Internet Telephony

No call via Internet: □

Country specific view: Germany

	Activate Provider	Internet Telephony Service Provider
Add		Other Provider
Edit	□	1&1
Edit	□	Arcor
Edit	□	COLT UK & Europe
Edit	□	COLT VPN
Edit	□	Ennit AG
Edit	□	GMX
Edit	□	Purtel
Edit	□	QSC
Edit	□	Sipgate
Edit	□	Sipgate Trunking
Edit	□	Skype Connect
Edit	□	toplink
Edit	□	Vodafone Anlagenanschluss

2) If you want to change the preset country, select the desired country from the **Country specific view** drop-down list to display the ITSPs that are available for this country.

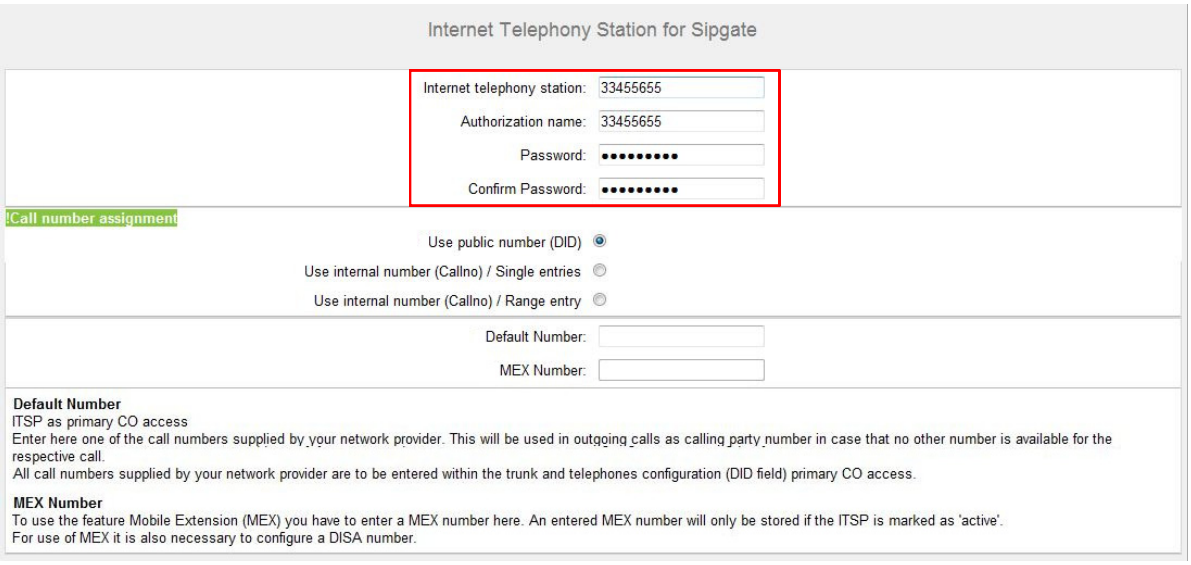
3) If required, click **Display Status** to check which ITSPs have already been activated and which Internet telephony subscribers have already been configured under each ITSP. You can activate a maximum of 8 ITSPs. Click **OK** when finished.

4) To configure Internet telephony stations, click **Edit** in the line associated with the relevant ITSP.

5) Activate the check box **Enable Provider**.

6) Click **OK & Next**.

7) Click **Add** to configure your ITSP accounts with the corresponding Internet telephony numbers. The fields that will then be displayed are provider-specific.



Internet Telephony Station for Sipgate

Internet telephony station: 33455655

Authorization name: 33455655

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

!Call number assignment

Use public number (DID) ●

Use internal number (Callno) / Single entries ○

Use internal number (Callno) / Range entry ○

Default Number:

MEX Number:

Default Number
ITSP as primary CO access
Enter here one of the call numbers supplied by your network provider. This will be used in outgoing calls as calling party number in case that no other number is available for the respective call.
All call numbers supplied by your network provider are to be entered within the trunk and telephones configuration (DID field) primary CO access.

MEX Number
To use the feature Mobile Extension (MEX) you have to enter a MEX number here. An entered MEX number will only be stored if the ITSP is marked as 'active'.
For use of MEX it is also necessary to configure a DISA number.

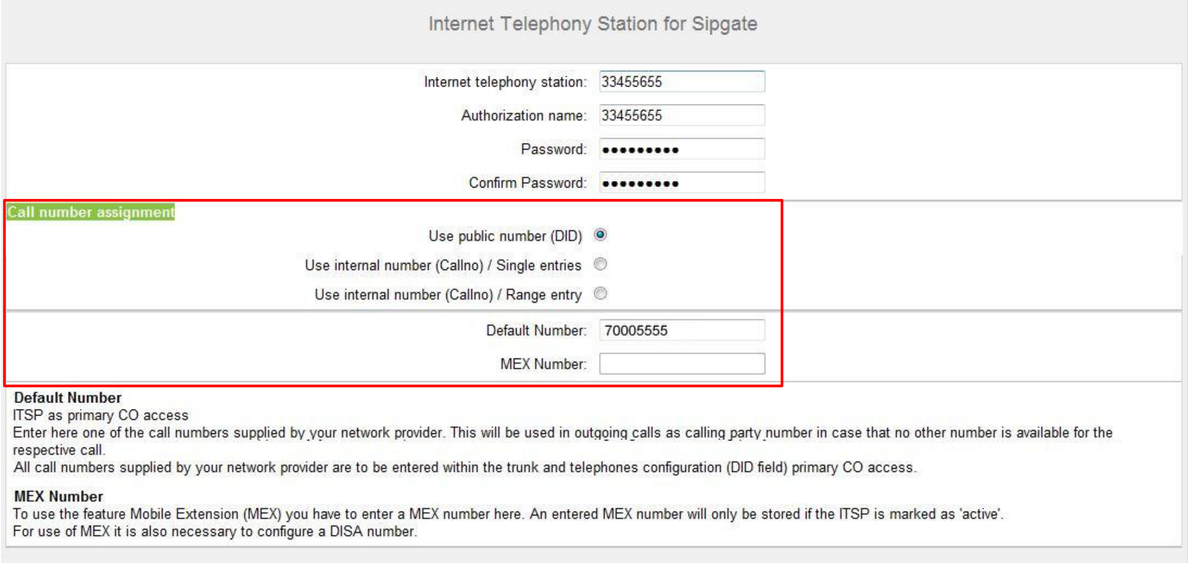
8) Enter the credentials for your account in the **Internet Telephony Station** field. You received this data from your ITSP. Depending on the ITSP, different designations are used for this, for example: SIP User, SIP ID, etc.

9) Enter the authorization name in the **Authorization name** field. You received this data from your ITSP. If you have not received any authorization name, enter the same data you entered under **Internet Telephony Station**.

10) Enter the password you received from the ITSP in the **New Password** and **Confirm Password** fields. Depending on the ITSP, different designations are used for this, for example: Password, SIP Password, etc.

11) Assignment of Internet telephony phone numbers - Option 1:

Use public number (DID): the Internet telephony phone numbers of your Internet telephony station connection or Internet telephony point-to-point connection are not entered here during the ITSP configuration, but when the configuring the stations, i.e. the telephones and subscribers (in the **DID** fields).



Internet Telephony Station for Sipgate

Internet telephony station: 33455655

Authorization name: 33455655

Password: •••••••••

Confirm Password: •••••••••

Call number assignment

Use public number (DID) ●

Use internal number (Callno) / Single entries ○

Use internal number (Callno) / Range entry ○

Default Number: 70005555

MEX Number:

Default Number
ITSP as primary CO access
Enter here one of the call numbers supplied by your network provider. This will be used in outgoing calls as calling party number in case that no other number is available for the respective call.
All call numbers supplied by your network provider are to be entered within the trunk and telephones configuration (DID field) primary CO access.

MEX Number
To use the feature Mobile Extension (MEX) you have to enter a MEX number here. An entered MEX number will only be stored if the ITSP is marked as 'active'.
For use of MEX it is also necessary to configure a DISA number.

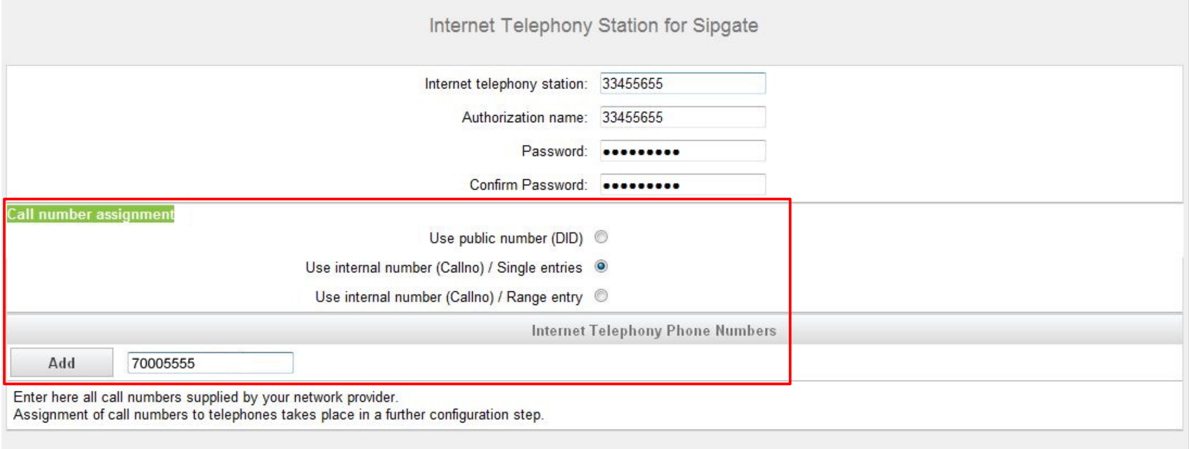
a) Select the option field **Use public number (DID)** in the **Call number assignment** area.

b) Under **Default Number**, enter the phone number to be used for outgoing calls to subscribers who do not have their own phone number.

c) If your ITSP supports the "Mobile Extension (MEX)" feature, enter the MEX number provided by the ITSP (8 positions, digits only) under **MEX Number**.

12) Assignment of Internet telephony phone numbers - Option 2:

Use internal number (Callno) / Single entries: You have an Internet telephony station connection and have received individual call numbers as Internet telephony phone numbers (e.g. 70005555, 70005556,...). Then assign these single numbers to the internal call numbers of the subscribers.



Internet Telephony Station for Sipgate

Internet telephony station: 33455655

Authorization name: 33455655

Password: •••••••••

Confirm Password: •••••••••

Call number assignment

Use public number (DID) ○

Use internal number (Callno) / Single entries ●

Use internal number (Callno) / Range entry ○

Internet Telephony Phone Numbers

70005555

Enter here all call numbers supplied by your network provider.
Assignment of call numbers to telephones takes place in a further configuration step.

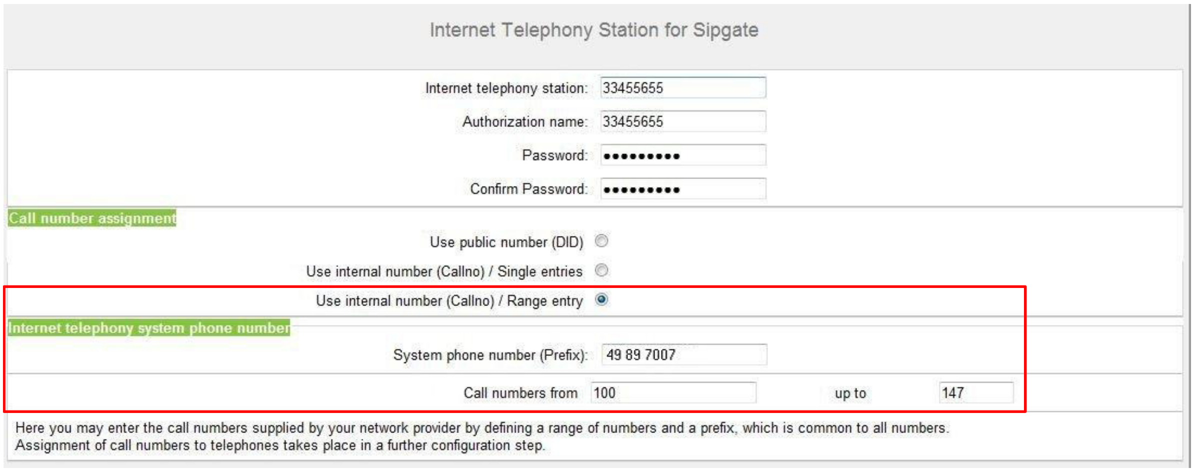
a) Select the option field **Use internal number (Callno) / Single entries** in the **Call number assignment** area.

b) In the **Internet Telephony Phone Numbers** area, enter one of the Internet telephony phone numbers provided by the ITSP in the field next to the **Add** button and then click **Add**.

c) To assign further Internet telephony numbers to the account, repeat step b).

13) Assignment of Internet telephony phone numbers - Option 3:

Use internal number (Callno) / Range entry: You have an Internet telephony point-to-point connection and have received a call number range as Internet telephony phone numbers (e.g., +49) 89 7007-100 to (+49) 89 7007-147. You then assign the call numbers from the call number range as the internal call numbers of the subscribers.



Internet Telephony Station for Sipgate

Internet telephony station: 33455655
Authorization name: 33455655
Password: ●●●●●●●●●
Confirm Password: ●●●●●●●●●

Call number assignment

Use public number (DID) ○
Use internal number (Callno) / Single entries ○
Use internal number (Callno) / Range entry ●

Internet telephony system phone number

System phone number (Prefix): 49 89 7007
Call numbers from 100 up to 147

Here you may enter the call numbers supplied by your network provider by defining a range of numbers and a prefix, which is common to all numbers.
Assignment of call numbers to telephones takes place in a further configuration step.

a) Select the option field **Use internal number (Callno) / Range entry** in the **Call number assignment** area.

b) Enter the system phone number under **System phone number (prefix)**.

c) Enter the desired DID number range for the Internet telephony station in the 'from' **and** 'to **' fields after** Direct inward dialing band. The range entered by default is 100 - 147.

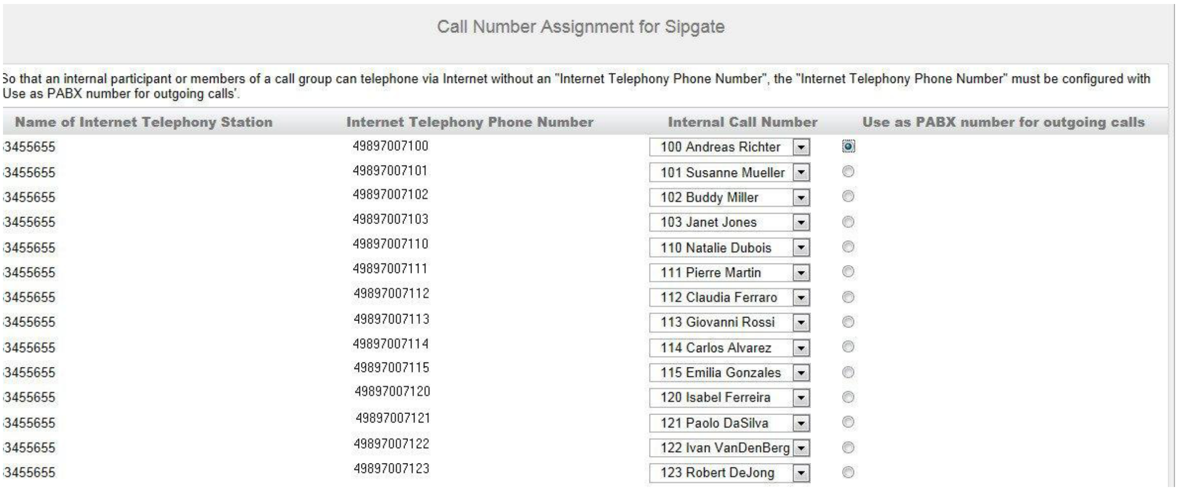
14) Click on **OK & Next**.

15) If you want to configure additional accounts and their associated Internet telephony numbers, repeat steps 7 through 14.

16) Click **OK & Next**. You will see an overview of which Internet telephony phone numbers are assigned to accounts.

17) Assign one internal station number each to every Internet telephony phone number.

This step is not required if you have selected option 1 for the assignment of the Internet telephony phone numbers. In this case, the assignment is made when the configuring the stations (i.e., the telephones and subscribers) in the **DID** field.



Call Number Assignment for Sipgate

So that an internal participant or members of a call group can telephone via Internet without an "Internet Telephony Phone Number", the "Internet Telephony Phone Number" must be configured with Use as PABX number for outgoing calls'.

Name of Internet Telephony Station	Internet Telephony Phone Number	Internal Call Number	Use as PABX number for outgoing calls
3455655	49897007100	100 Andreas Richter	●
3455655	49897007101	101 Susanne Mueller	○
3455655	49897007102	102 Buddy Miller	○
3455655	49897007103	103 Janet Jones	○
3455655	49897007110	110 Natalie Dubois	○
3455655	49897007111	111 Pierre Martin	○
3455655	49897007112	112 Claudia Ferraro	○
3455655	49897007113	113 Giovanni Rossi	○
3455655	49897007114	114 Carlos Alvarez	○
3455655	49897007115	115 Emilia Gonzales	○
3455655	49897007120	120 Isabel Ferreira	○
3455655	49897007121	121 Paolo DaSilva	○
3455655	49897007122	122 Ivan VanDenBerg	○
3455655	49897007123	123 Robert DeJong	○

a) To do this, select an internal call number in the appropriate line from the **Internal Call Number** drop-down list.

b) If subscribers without Internet telephony phone numbers or members of a call group are to be allowed to make external calls via the Internet, the radio button **Use as PABX number for outgoing calls** must be activated. The radio button can be activated for only one single Internet telephony phone number.

18) Click **OK & Next**. Here you see again the list of predefined and newly added ITSPs. The enabled ITSPs are identified with a check mark in the **Enable Provider** column. If you are having connection problems with already activated ITSP, you can register it again with **Restart ITSP**.

19) Click **OK & Next**.

20) Enter the upload speed of your Internet connection in the **Upstream up to (Kbps)** field. Please do not confuse this with the download speed!

> ***INFO:*** The number of simultaneous Internet calls permitted is displayed in the **Number of Simultaneous Internet calls** field. If the voice quality deteriorates due to the network load, you will need to reduce the number.

21) Click **OK & Next**.

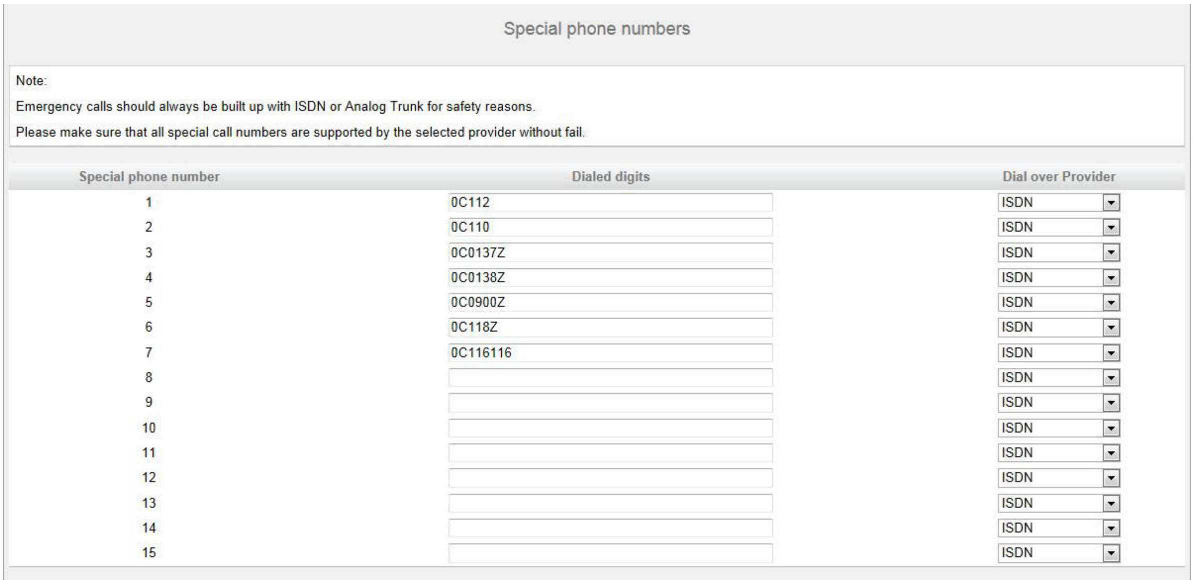
22) If you did not activate the full-time circuit when setting up your Internet access, you can now do this here. Without a permanent connection (full-time circuit), you cannot receive calls over the Internet. If the full-time circuit has already been set up, the fields described under a) to c) will not appear.

a) Enable the radio button **On** under **Full-Time Circuit**.

b) In the **Forced Disconnect at (hour:min)** field, enter the time at which the Internet connection is to be deactivated (e.g., 04:59).

c) Click **OK & Next**.

23) Enter the special numbers you want in the **Dialed digits** column.



Special phone numbers

Note:
Emergency calls should always be built up with ISDN or Analog Trunk for safety reasons.
Please make sure that all special call numbers are supported by the selected provider without fail.

Special phone number	Dialed digits	Dial over Provider
1	0C112	ISDN
2	0C110	ISDN
3	0C0137Z	ISDN
4	0C0138Z	ISDN
5	0C0900Z	ISDN
6	0C118Z	ISDN
7	0C116116	ISDN
8		ISDN
9		ISDN
10		ISDN
11		ISDN
12		ISDN
13		ISDN
14		ISDN
15		ISDN

The following station number entries are valid:

0 to 9: allowed digits

-: Field separator

X: Any digit from 0 to 9

N: Any digit from 2 to 9

Z: One or more digits to follow up to the end of dialing

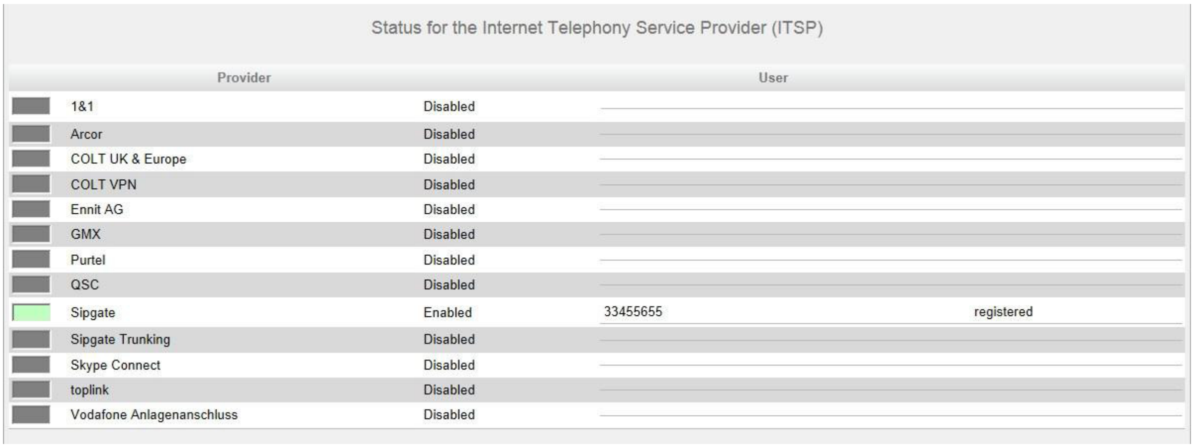
C: Simulated dial tone (can be entered up to three times)

24) Use the **Dial over Provider** column to specify whether the special number should be dialed via ISDN or an ITSP. Only the active ITSP is displayed.

INFO: Ensure that emergency numbers can always be dialed. If you want to dial emergency numbers via an Internet Telephony Service Provider, you must make sure that the ITSP supports this feature.

---

25) Click **OK & Next**. The status of your ITSP will be displayed.



Status for the Internet Telephony Service Provider (ITSP)

Provider			User	
■	1&1	Disabled		
■	Arcor	Disabled		
■	COLT UK & Europe	Disabled		
■	COLT VPN	Disabled		
■	Ennit AG	Disabled		
■	GMX	Disabled		
■	Purtel	Disabled		
■	QSC	Disabled		
🟩	Sipgate	Enabled	33455655	registered
■	Sipgate Trunking	Disabled		
■	Skype Connect	Disabled		
■	toplink	Disabled		
■	Vodafone Anlagenanschluss	Disabled		

The configured ITSPs at which you are already registered are marked in green.

The configured ITSPs at which you are not yet registered are marked in orange.

26) Click **Next** followed by **Finish**.

4.8.4.2 How to Deactivate Internet Telephony

Prerequisites

- You are in the **Provider configuration and activation for Internet Telephony** window.

Step by Step

1) Leave the **No call via Internet** check box selected.

2) Click **OK & Next** twice.

4.8.5 Stations

In the **Select a station - ...** window, you can configure the stations connected to the communication system.

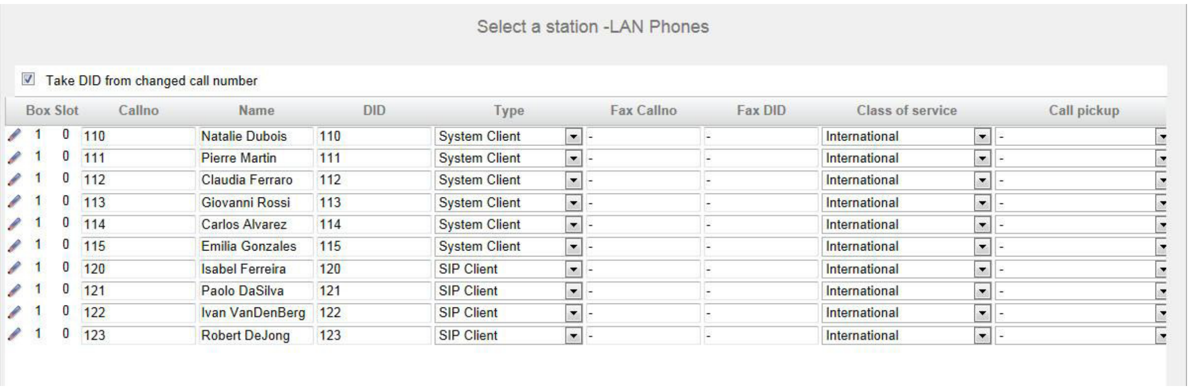
Proceed as follows:

1. Configure the IP and SIP stations
   IP and SIP stations include LAN phones or WLAN phones, for example.

4.8.5.1 How to Configure IP and SIP Stations

Prerequisites

- You are in the **Select a station - LAN Phones** window.
- A functional wireless LAN network is needed to operate WLAN phones.



Select a station -LAN Phones

☑ Take DID from changed call number

	Box	Slot	Callno	Name	DID	Type	Fax Callno	Fax DID	Class of service	Call pickup
✎	1	0	110	Natalie Dubois	110	System Client	-	-	International	-
✎	1	0	111	Pierre Martin	111	System Client	-	-	International	-
✎	1	0	112	Claudia Ferraro	112	System Client	-	-	International	-
✎	1	0	113	Giovanni Rossi	113	System Client	-	-	International	-
✎	1	0	114	Carlos Alvarez	114	System Client	-	-	International	-
✎	1	0	115	Emilia Gonzales	115	System Client	-	-	International	-
✎	1	0	120	Isabel Ferreira	120	SIP Client	-	-	International	-
✎	1	0	121	Paolo DaSilva	121	SIP Client	-	-	International	-
✎	1	0	122	Ivan VanDenBerg	122	SIP Client	-	-	International	-
✎	1	0	123	Robert DeJong	123	SIP Client	-	-	International	-

Step by Step

1) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:

- Only for a point-to-point connection:

  Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.

- Only for a point-to-multipoint connection:

  Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.

- For point-to-point and point-to-multipoint connections:

  Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

2) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.

3) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name`.

INFO: The name can consist of up to 16 characters, but should not include any diacritical characters such as umlauts or special characters. The name specified here will be entered as the Last Name at the UC clients, but can be edited there.

4) Select the type of IP station (e.g., "System Client" or "SIP Client") from the **Type** drop-down list in the row of the desired station.

5) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:

a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.

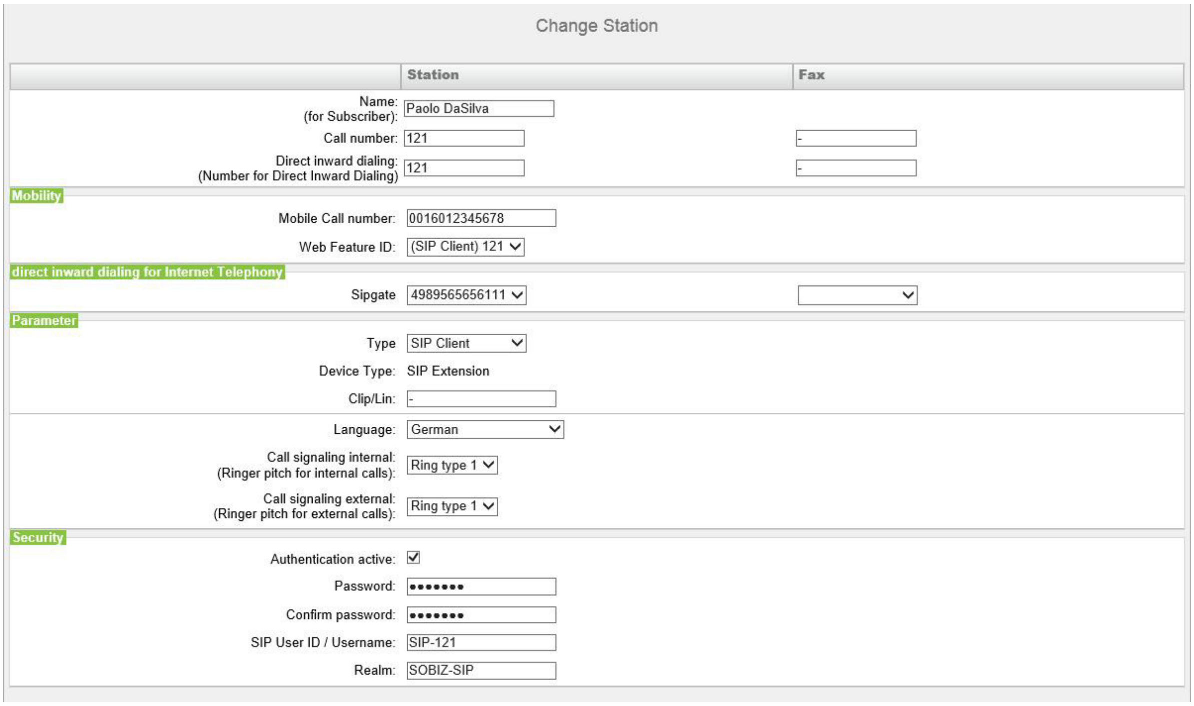
b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.

6) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

7) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

8) Make the settings described under this step only if needed or for a SIP phone:

a) Click in the row of the desired station on the pencil icon **Edit**.



Change Station

	Station	Fax
Name: (for Subscriber):	Paolo DaSilva	
Call number:	121	-
Direct inward dialing: (Number for Direct Inward Dialing)	121	-

Mobility

Mobile Call number: 0016012345678

Web Feature ID: (SIP Client) 121

direct inward dialing for Internet Telephony

Sipgate: 4989565656111

Parameter

Type: SIP Client

Device Type: SIP Extension

Clip/Lin: -

Language: German

Call signaling internal:
(Ringer pitch for internal calls): Ring type 1

Call signaling external:
(Ringer pitch for external calls): Ring type 1

Security

Authentication active: ☑

Password: •••••••

Confirm password: •••••••

SIP User ID / Username: SIP-121

Realm: SOBIZ-SIP

b) For SIP phones: If the SIP phone is to be operated in conjunction with a dual-mode mobile phone, enter the dialout prefix followed by the telephone number of the mobile phone (e.g., **0016012345678**) in the **Mobility** area under `Mobile phone number`. In addition, select this SIP client from the **Web Feature ID** drop-down list. (see *Administrator Documentation, Mobility*).

c) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

INFO: This feature must be released by the network provider.

d) Select the language for the menu controls on the phone from the **Language** drop-down list.

e) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

f) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

g) Only for SIP phones: Enable the **Authentication active** check box.

h) Only for SIP phones: Enter the authentication password in the **Password** and **Confirm password** fields.

i) Only for SIP phones: Enter the user ID for the authentication in the **SIP User ID / Username** field.

j) Only for SIP phones: Enter the associated zone for the authentication in the **Realm** field.

k) Click on **OK & Next**.

l) Change the station flags as needed. For a description of the station flags, see *Expert mode: Station > Station > Station Parameters*.

m) Click on **OK & Next**.

9) If you want to configure another IP station, click on **Store data** and repeat steps 1 through 8.

10) Click on **OK & Next**. A list of all configured stations appears. This list is effectively a dial plan.

11) If required, click **Print** to print out the data of the configured stations.

12) Then click **OK & Next**.

4.8.6 Configuring UC Suite

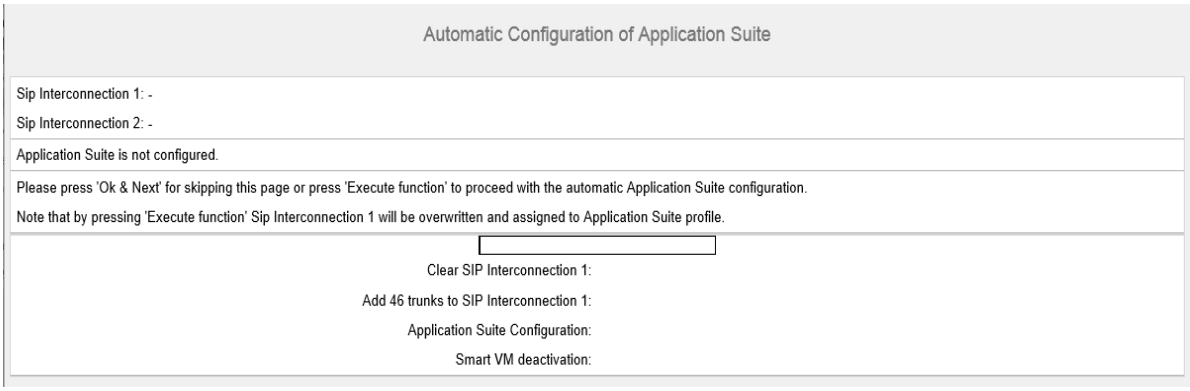
You can perform the automatic configuration of the UC solution UC Suite in the **Automatic Configuration of the Application Suite** window.

> ***INFO:*** This window appears only if **Package with UC Suite** was selected during the application selection in the **Initial Installation** wizard.

4.8.6.1 How to Configure the UC Suite

Prerequisites

- You are in the **Automatic Configuration of Application Suite** window.



Automatic Configuration of Application Suite

Sip Interconnection 1: -

Sip Interconnection 2: -

Application Suite is not configured.

Please press 'Ok & Next' for skipping this page or press 'Execute function' to proceed with the automatic Application Suite configuration.

Note that by pressing 'Execute function' Sip Interconnection 1 will be overwritten and assigned to Application Suite profile.

Clear SIP Interconnection 1:

Add 46 trunks to SIP Interconnection 1:

Application Suite Configuration:

Smart VM deactivation:

Step by Step

› Click on **Execute function**. The UC Suite is configured automatically. Once the progress bar shows 100%, click on **OK & Next**.

4.8.7 Configuring UC Smart Mailboxes

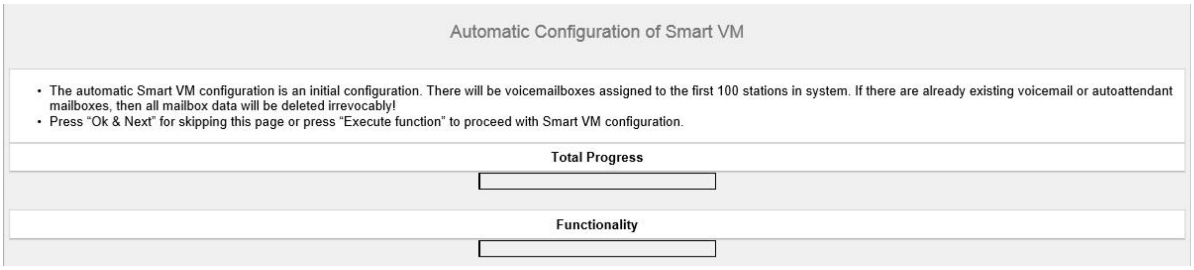
If you are using the UC solution UC Smart, you can perform the automatic configuration of the UC Smart voicemail boxes (Smart VM, Smart VoiceMail) in the **Automatic Configuration of Smart VM** window.

> ***INFO:*** This window appears only if **Package with UC Smart** was selected during the application selection in the **Initial Installation** wizard.

4.8.7.1 How to Configure UC Smart Voicemail Boxes

Prerequisites

- You are in the **Automatic Configuration of Smart VM** window.



Automatic Configuration of Smart VM

- The automatic Smart VM configuration is an initial configuration. There will be voicemailboxes assigned to the first 100 stations in system. If there are already existing voicemail or autoattendant mailboxes, then all mailbox data will be deleted irrevocably!
- Press "Ok & Next" for skipping this page or press "Execute function" to proceed with Smart VM configuration.

Total Progress

Functionality

Step by Step

1) If the UC Smart voicemail boxes are not to be used, click on **OK & Next**. The configuration of the voicemail boxes will be skipped.

2) If the UC Smart voicemail boxes are to be used, click on **Execute function**. Voicemail boxes are then automatically configured for the first 100 subscribers. Once the progress bar shows 100%, click on **OK & Next**.

> ***INFO:*** Existing UC Smart or UC Smart AutoAttendant voicemail boxes are irrevocably deleted in the process.

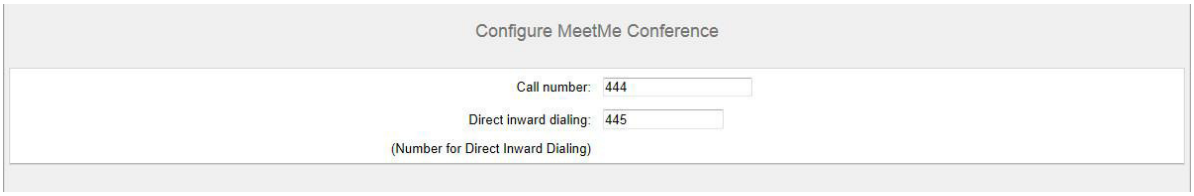
4.8.8 Conference Server Settings

The **MeetMe Conference** settings window can be used to define the call numbers and the dial-in numbers for conferences.

4.8.8.1 How to Edit the Conference Server Settings

Prerequisites

- You are in the **Configure MeetMe Conference** window.



Configure MeetMe Conference

Call number: 444

Direct inward dialing: 445

(Number for Direct Inward Dialing)

Step by Step

1) Enter a phone number for the conference in the **Phone Number** field.

2) Enter the dial-in number for the conference (conference DID) with which subscribers can dial into an existing conference in the **Direct inward dialing** field.

3) Click on **OK & Next**.

4.8.9 E-mail Delivery (Optional)

You can configure the delivery of e-mails in the **Configure E-Mail Forwarding** window. These e-mails notify users of voicemail and fax messages and administrators of system messages.

You have the following options:

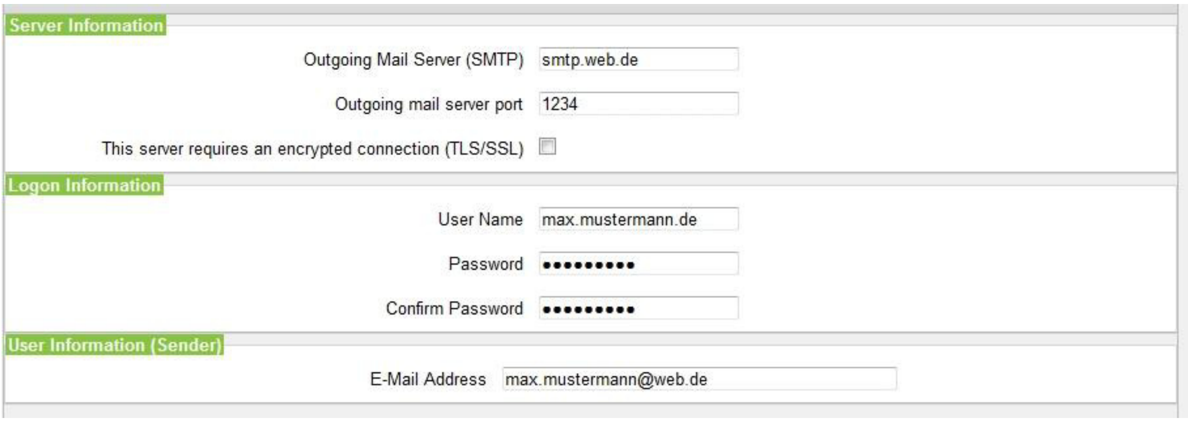
- Configuring the Sending of E-mails
  You can specify an external E-mail server via which the e-mails are to be sent by OpenScape Business. Voicemails, fax messages and internal system messages can then be sent via this E-mail server to one or several different configurable e-mail addresses.

> ***INFO:*** Entering the e-mail server is important if an e-mail with a link to the installation file(s) is to be automatically sent to the users of the UC Suite.

4.8.9.1 How to Configure the Sending of E-mails

Prerequisites

- An e-mail account with a password exists with an e-mail provider, and you know the access data for this account.
- You are in the **Configure E-Mail Forwarding** window.



Server Information

Outgoing Mail Server (SMTP): smtp.web.de

Outgoing mail server port: 1234

This server requires an encrypted connection (TLS/SSL) □

Logon Information

User Name: max.mustermann.de

Password: •••••••••

Confirm Password: •••••••••

User Information (Sender)

E-Mail Address: max.mustermann@web.de

Step by Step

1) Enter the **Outgoing mail server (SMTP)** for the e-mail server to be used for sending e-mails, e.g., `smtp.web.de`. Ask your e-mail provider for the outgoing mail server if required.

> ***INFO:*** Make sure that the name of the outgoing mail server can be resolved. If not, you must start the e-mail sending function via

Service Center > E-mail Forwarding and then enter the IP address of the outgoing mail server instead of its name.

2) If a secure connection is required, enable the corresponding check box. If required, check with your e-mail provider whether this option needs to be enabled.

3) Enter the **User Name** of the e-mail account, e.g.,: `john.doe`.

4) Enter the **Password** for the e-mail account and repeat it in the **Confirm Password** field.

5) Enter the **E-mail Address**, for example: `john.doe@web.de`.

6) If you want to test the entered e-mail settings immediately, proceed as follows:

a) Click on **Test Connection**.

b) Under **Send to e-mail address**, enter the e-mail address of any e-mail box that you can access. The test e-mail will be sent to that e-mail address.

c) Under **Subject in the e-mail**, enter a descriptive text so that you can identify the e-mail in your e-mail inbox.

d) Click on **Send Test E-mail**. The e-mail settings are verified, and the e-mail is sent to the specified e-mail address.

e) Check whether the e-mail has arrived in your e-mail inbox.

f) If the e-mail was sent correctly, proceed to the next step.

g) If the e-mail delivery failed, click **Back** and correct your e-mail settings.

7) Click on **OK & Next** followed by **Finish**. The basic installation is finished. Before you perform the backup mentioned in the wizard, you should activate the licenses.

4.9 Closing Activities

After the initial installation and the basic installation with the WBM have been completed, some important settings must still be made for the operation of OpenScape Business.

Proceed as follows:

1. Activate and assign licenses
   The licenses procured with OpenScape Business must be activated within a period of 30 days. The time period begins the next time you log on to the WBM. After this time period expires, the communication system will only operate in restricted mode. Once the licenses have been activated successfully, they must be assigned to the stations and lines. System-wide features are enabled automatically upon activation.
2. Provision the UC Smart client for installation (only for UC Smart)
   The UC Smart client myPortal Smart is a part of UC Smart. The installation file for myPortal Smart is accessible via the WBM and can be made available

to the IP stations automatically or manually. For more information, see *the section UC Smart - UC Smart Clients in the Administrator Documentation*.

3. Provision the UC Clients for installation

   The UC clients are part of the UC Suite. The installation files for the UC Client are accessible via the WBM and can be made available to the IP stations automatically or manually.

   In addition, the administrator has the option of performing a silent installation. The silent installation/uninstallation is a command-line based method to automatically install, uninstall or modify UC Suite PC clients on a PC without requiring any further user inputs. For more information, see *the section UC Suite - UC Suite Clients in the Administrator Documentation*.

4. Perform a data backup

   All previous changes to OpenScape Business must be backed up. The backup can be stored as a backup set in the internal network, for example.

4.9.1 How to Activate and Assign the Licenses

Prerequisites

- You are logged on to the WBM with the **Advanced** profile.
- You know the LAC (License Authorization Code) for releasing the license and have a user ID and password for accessing the license server.
- You need Internet access to connect to the license server.

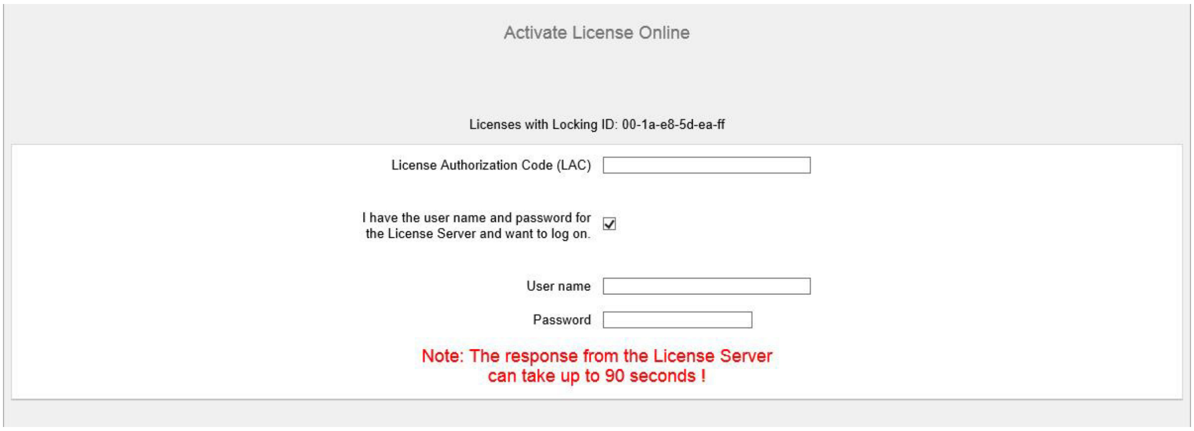
Step by Step

1) Activate license online:

a) In the navigation bar, click on **Expert Mode**.

b) In the navigation tree, click **Wizards > Basic Installation**.

c) Click on **Edit** to start the **Licensing** wizard.



Activate License Online

Licenses with Locking ID: 00-1a-e8-5d-ea-ff

License Authorization Code (LAC)

I have the user name and password for the License Server and want to log on. ☑

User name

Password

Note: The response from the License Server can take up to 90 seconds !

d) Enter the appropriate LAC in the **License Authorization Code (LAC)** field.

e) Select the check box **I have the user name and password for the License Server and want to log on**.

f) Enter the **User Name** and **Password** for logging into the License Server.

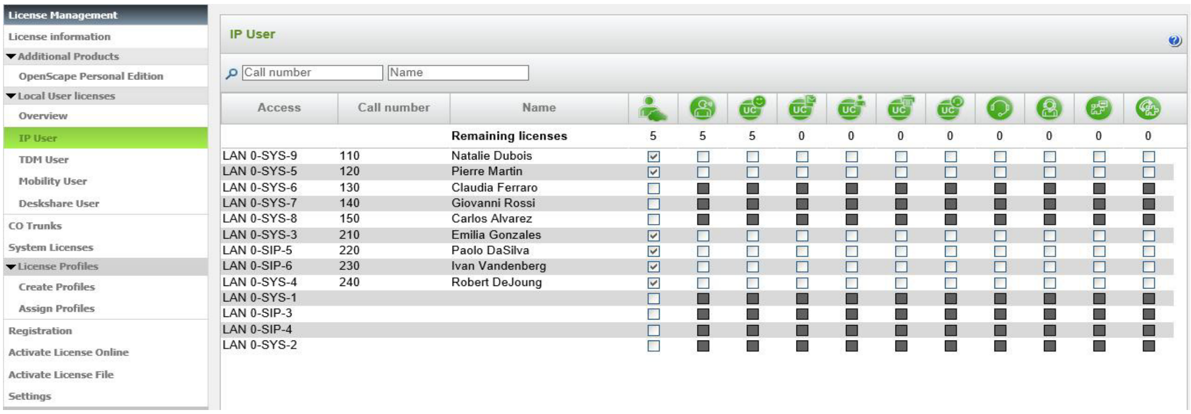
g) Click on **OK & Next**. The connection to the license server is established, and the licenses are released.

2) Assign licenses to stations:

a) Click on **License Management** in the navigation bar.

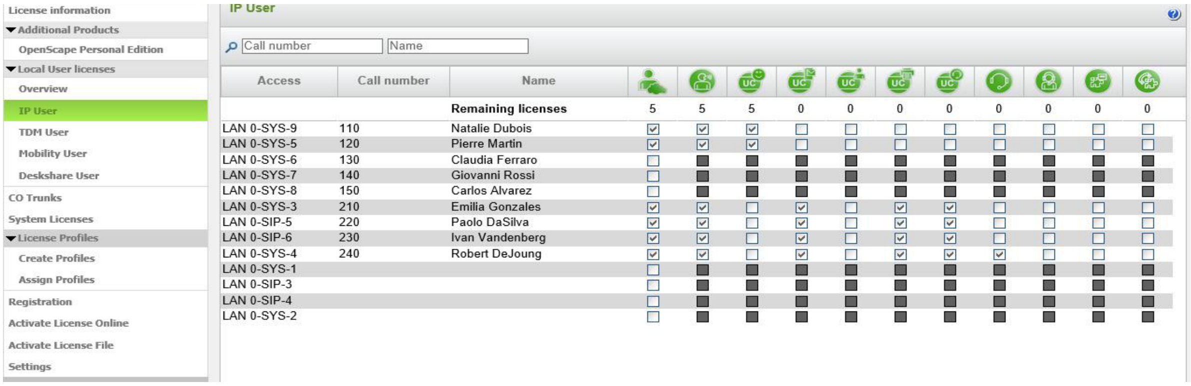
b) In the navigation tree, navigate to the desired type of subscriber under **Local User Licenses > ....** You will be shown a list of all subscribers of the selected subscriber type.

c) In the row of the desired subscriber, select the check box in the **User license** column (first column with check boxes).



Access	Call number	Name											
		Remaining licenses	5	5	5	0	0	0	0	0	0	0	0
LAN 0-SYS-9	110	Natalie Dubois	☑	□	□	□	□	□	□	□	□	□	□
LAN 0-SYS-5	120	Pierre Martin	☑	□	□	□	□	□	□	□	□	□	□
LAN 0-SYS-6	130	Claudia Ferraro	□	■	■	■	■	■	■	■	■	■	■
LAN 0-SYS-7	140	Giovanni Rossi	□	■	■	■	■	■	■	■	■	■	■
LAN 0-SYS-8	150	Carlos Alvarez	□	■	■	■	■	■	■	■	■	■	■
LAN 0-SYS-3	210	Emilia Gonzales	☑	□	□	□	□	□	□	□	□	□	□
LAN 0-SIP-5	220	Paolo DaSilva	☑	□	□	□	□	□	□	□	□	□	□
LAN 0-SIP-6	230	Ivan Vandenberg	☑	□	□	□	□	□	□	□	□	□	□
LAN 0-SYS-4	240	Robert DeJoung	☑	□	□	□	□	□	□	□	□	□	□
LAN 0-SYS-1			□	■	■	■	■	■	■	■	■	■	■
LAN 0-SIP-3			□	■	■	■	■	■	■	■	■	■	■
LAN 0-SIP-4			□	■	■	■	■	■	■	■	■	■	■
LAN 0-SYS-2			□	■	■	■	■	■	■	■	■	■	■

d) Activate the user-oriented licenses in the row of the desired subscriber by selecting the appropriate check boxes.



Access	Call number	Name											
		Remaining licenses	5	5	5	0	0	0	0	0	0	0	0
LAN 0-SYS-9	110	Natalie Dubois	☑	☑	☑	□	□	□	□	□	□	□	□
LAN 0-SYS-5	120	Pierre Martin	☑	☑	☑	□	□	□	□	□	□	□	□
LAN 0-SYS-6	130	Claudia Ferraro	□	■	■	■	■	■	■	■	■	■	■
LAN 0-SYS-7	140	Giovanni Rossi	□	■	■	■	■	■	■	■	■	■	■
LAN 0-SYS-8	150	Carlos Alvarez	□	■	■	■	■	■	■	■	■	■	■
LAN 0-SYS-3	210	Emilia Gonzales	☑	☑	□	☑	□	☑	☑	□	□	□	□
LAN 0-SIP-5	220	Paolo DaSilva	☑	☑	□	☑	□	☑	☑	□	□	□	□
LAN 0-SIP-6	230	Ivan Vandenberg	☑	☑	□	☑	□	☑	☑	□	□	□	□
LAN 0-SYS-4	240	Robert DeJoung	☑	☑	□	☑	□	☑	☑	☑	□	□	□
LAN 0-SYS-1			□	■	■	■	■	■	■	■	■	■	■
LAN 0-SIP-3			□	■	■	■	■	■	■	■	■	■	■
LAN 0-SIP-4			□	■	■	■	■	■	■	■	■	■	■
LAN 0-SYS-2			□	■	■	■	■	■	■	■	■	■	■

INFO: User-oriented licenses can be assigned to a subscriber only if a station license (user license) was assigned to the subscriber earlier (step c).

e) Click on **OK & Next**. A check is performed to determine whether there are enough licenses for your assignment.

If sufficient licenses are available, the licensing of the subscriber is completed.

f) If licenses are missing, the errors are indicated by displaying a check box shaded in red. Correct these errors and repeat step e.

3) Assign licenses to trunks:

a) In the navigation tree, click **CO trunks**. The number of trunk licenses purchased will be displayed in the **CO trunks** area.

b) For SIP trunks: In the **License demand for number of simultaneous Internet calls in this node** area, enter the number of Internet calls that can be conducted simultaneously via an ITSP.

c) Click on **OK & Next**.

4.9.2 How to Provision the UC Smart Client for Installation

Prerequisites

- You are logged on to the WBM with the **Advanced** profile.
- The hardware and software for using UC Smart are available.

INFO: Licenses are required to use the UC Smart client myPortal Smart.

Step by Step

1) Click on **Service Center** in the navigation bar.

2) Click on **Software** in the navigation tree.

3) Click on the Download icon of **myPortal Smart** and save the installation file on a shared network drive.

4) Click on the link icon for **Adobe AIR** and download the installation file to a shared network drive.

5) Send the two installation files to the users of myPortal Smart.

6) Alternatively, you can also send the users of myPortal Smart two links with which they can access the installation files:

```
https://<IP address of the communication system>/
management/downloads/SmartClient.air
```

```
http://www.adobe.com/air
```

4.9.3 How to Provision the UC Suite Clients for Installation

Prerequisites

- You are logged on to the WBM with the **Advanced** profile.
- The hardware and software for using the UC Suite are available.

INFO: Licenses are required to use the UC Suite clients.

Step by Step

1) To enable the installation files to be provided automatically to a station, make sure that the following steps have been performed:

a) The e-mail addresses of the stations and the associated subscriber data must have either been already imported via an XML file or entered later under **Setup > UC Suite > User Directory**.

b) An e-mail server must have been specified.

INFO: You can also enter an E-mail server later under **Service Center > E-mail Forwarding**.

All subscribers whose e-mail addresses are known receive an e-mail with a link to the installation directory of the UC clients and Getting Started Instructions. The installation folder also includes a Readme file with information on installing the software on client PCs.

2) If the required steps for automatic notification are not fulfilled, you can also make the installation files available manually. To do this, proceed as follows:

a) Click on **Service Center** in the navigation bar.

b) Click on **Software** in the navigation tree.

c) Click on the desired UC client and save the zipped installation file on a shared network drive.

d) Click in the navigation tree on **Documents** and select **User Guide** from the drop-down list.

e) Click on the documentation of the desired UC client and save the documentation file on a shared network drive.

f) Send the zipped installation file and the documentation file to the users of the UC clients by e-mail or inform the users about the storage location of these files.

g) The zip file with the installation files also includes a Readme file. Notify the users that the installation of the UC clients must be performed in accordance with the installation notes in the Readme file.

3) Alternatively, you can also send the UC users links through which they can directly access the installation files of the UC clients.

- ***a)*** Click on **Service Center** in the navigation bar.
- ***b)*** Click on **Software** in the navigation tree.
- ***c)*** Click on the **Show Application Links** button. You will be presented with multiple links, depending on the used operating system and the desired UC client. For example:

```
https://<IP address of the communication system>/
management/downloads/install-common.zip
```

4.9.4 How to Perform a Data Backup

Prerequisites

- You are logged on to the WBM with the **Advanced** profile.

> ***INFO:*** For more information on backing up data, see *Administrator Documentation, Maintenance*.

Step by Step

1) Click on **Backup and Restore** in the navigation bar.

2) In the navigation tree, click **Backup - Immediate**.

3) Enter a comment for the backup set in the **Comment** field in the **Name** area so that the backup set can be easily identified if needed later for a restore. Avoid the use of diacritical characters such as umlauts and special characters in your input.

4) Activate the target drive on which the backup set is to be saved (e.g., a network drive) in the **Devices** area.

5) Click on **OK & Next**. The progress of the backup process is displayed in a separate window.

6) The backup was successful if the message **Backup completed successfully!** appears. Click on **Finish**.

7) This completes the initial startup with WBM. Exit the WBM by right-clicking the **Logout** link on the top right of the screen and then close the window.

4.10 Commissioning of IP Phones

The commissioning of IP phones can be facilitated by the existence of a DHCP server that supplies an IP phone with important (network-specific) data that is needed to log into the communication system.

Network-Specific Data

In order to log into the communication system, an IP phone requires some network-specific data. This data can be stored in the DHCP server or be entered directly at the IP phone. The advantage of a DHCP server is that all connected IP phones are automatically supplied with the relevant data.

The following data is required by the IP phone:

- IP address of the communication system
- IP address of DLS server

In addition, the IP phone needs its own call number. This must be entered manually when logging in at the phone.

Registration of SIP Phones

For security reasons, it is recommended that SIP phones register at the communication system. To do this, the registration information on the IP phone and the communication system must match.

The following data is required for the login:

- SIP user ID
- SIP password
- SIP realm (optional)

Use a non-trivial SIP password that complies with the following rules:

- At least 8 characters
- At least one uppercase letter (A - Z)
- At least one lowercase letter (a - z)
- At least one digit (0-9)
- At least one special character

Use a SIP user ID that does not include the phone number.

> ***INFO:*** More information on configuring SIP telephones can be found at `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Using the Internal DHCP Server

If the internal DHCP server of the communication system is used, the network-specific data will already be stored there. In order to enable an IP phone to register at the communication system, only the specified call number must be entered at the IP phone. In the case of SIP phones, the SIP registration data at the SIP phone and at the communication system must match.

Using an External DHCP Server with Network-specific Data

If an external DHCP server is used, the network-specific data must be stored there. In order to enable an IP phone to register at the communication system, only the specified call number must be entered at the IP phone. In the case of SIP phones, the SIP registration data at the SIP phone and at the communication system must match.

Using an External DHCP Server without Network-specific Data

If an external DHCP server in which the network-specific data cannot be stored is used, this must be entered at the IP phone. To enable an IP phone to register at the communication system, the defined call number and IP address of the communication system must be entered at the phone, and the settings for the Deployment Service may need to be changed. In the case of SIP phones, the SIP registration data at the SIP phone and at the communication system must match.

4.10.1 How to Configure an IP Phone

Prerequisites

- The IP phone is connected to the internal network and operational.

> ***INFO:*** The sample configuration described here uses an OpenStage 40/60/80 IP system telephone. The same settings must also be made for any other IP phone. For more information, refer to the manual supplied with your IP phone.

Step by Step

1) To reach the administration mode of the IP system telephone, press the appropriate key for the Settings/Applications menu on the phone.

2) Scroll through the `Settings` options until `Admin` and confirm this with the OK key.

3) Enter administrator password (`123456` by default) and confirm your selection with the OK key.

4) If you are using the DHCP server of the communication system in the internal network, skip the next step.

5) If you are not using the DHCP server of the communication system in the internal network, you will need to enter the IP addresses of the Deployment Server (DLS) and the communication system so that the software of the IP system telephone can be updated automatically. This applies only to IP system telephones. Proceed as follows:

   a) Scroll to `Network` and confirm your selection with the OK key.

   b) Scroll to `Update service (DLS)` and confirm your selection with the OK key.

   c) Scroll to `DLS address` and confirm your selection with the OK key.

   d) Specify the IP address of the communication system (`192.168.1.2` by default) as the Deployment Server and confirm your entry with the OK key.

- ***e)*** Scroll to `Save & Exit` and confirm your selection with the OK key.
- ***f)*** Scroll to `IPv4 configuration` and confirm your selection with the OK key.
- ***g)*** Scroll to `Route (default)` and confirm your selection with the OK key.
- ***h)*** Specify the IP address of the communication system (`192.168.1.2` by default) and confirm your entry with the OK key.
- ***i)*** Scroll to `Save & Exit` and confirm your selection with the OK key.
- ***j)*** Navigate one menu level back with the Back key.

6) Specify the call number of the phone:

- ***a)*** Scroll to `System` and confirm your selection with the OK key.
- ***b)*** Scroll to `Identity` and confirm your selection with the OK key.
- ***c)*** Scroll to `Terminal number` and confirm your selection with the OK key.
- ***d)*** Enter the set phone number (e.g., `120`) and confirm your selection with the OK key.
- ***e)*** Scroll to `Save & Exit` and confirm your selection with the OK key.

7) Navigate one menu level back with the Back key.

8) If the system telephone needs to be restarted due to the changes made, the menu item `Restart` will appear in the `Admin` menu. Confirm the `Restart` with the OK key and then also confirm `Yes` with the OK key. The system telephone performs a reboot and logs in to the communication system.

4.10.2 How to Configure a SIP Phone

Prerequisites

- The SIP phone is connected to the customer LAN and operational.

> ***INFO:*** The configuration described here uses an OpenStage 40/60/80 SIP system telephone as an example. The same settings must also be made for another SIP phone. For more information, refer to the manual supplied with your SIP phone.

Step by Step

1) To reach the administration mode of the SIP system telephone, press the appropriate key for the Settings/Applications menu on the phone.

2) Scroll through the `Settings` options until `Administrator (Admin)` and confirm this with the OK key.

3) Enter administrator password (`123456` by default) and confirm your selection with the OK key.

4) If you are using the DHCP server of the communication system in the internal network, skip the next step.

5) If you are not using the DHCP server of the communication system in the internal network, you will need to enter the IP addresses of the Deployment Server (DLS) and the communication system so that the software of the SIP system telephone can be updated automatically. This applies only to SIP system telephones. Proceed as follows:

  a) Scroll to `Network` and confirm your selection with the OK key.

  b) Scroll to `Update service (DLS)` and confirm your selection with the OK key.

  c) Scroll to `DLS address` and confirm your selection with the OK key.

  d) Specify the IP address of the communication system (`192.168.1.2` by default) as the Deployment Server and confirm your entry with the OK key.

  e) Scroll to `Save & Exit` and confirm your selection with the OK key.

  f) Scroll to `IPv4 configuration` and confirm your selection with the OK key.

  g) Scroll to `Route (default)` and confirm your selection with the OK key.

  h) Specify the IP address of the communication system (`192.168.1.2` by default) and confirm your entry with the OK key.

  i) Scroll to `Save & Exit` and confirm your selection with the OK key.

  j) Navigate one menu level back with the Back key.

6) Specify the SNTP time settings:

  a) Scroll to `Date and time` and confirm your selection with the OK key.

  b) Scroll to `Time source` and confirm your selection with the OK key.

  c) Scroll to `SNTP IP address` and confirm your selection with the OK key.

  d) Specify the IP address of the communication system (`192.168.1.2` by default) and confirm your entry with the OK key.

  e) Scroll to `Timezone offset` and confirm your selection with the OK key.

  f) Enter the deviation between the local time and UTC (Universal Time Coordinated) in hours (Germany: `1`) and confirm this with the OK button.

  g) Scroll to `Save & Exit` and confirm your selection with the OK key.

  h) Navigate one menu level back with the Back key.

7) Specify the call number of the phone:

  a) Scroll to `System` and confirm your selection with the OK key.

  b) Scroll to `Identity` and confirm your selection with the OK key.

  c) Scroll to `Terminal number` and confirm your selection with the OK key.

  d) Enter the set phone number (e.g., `120`) and confirm your selection with the OK key.

  e) Scroll to `Save & Exit` and confirm your selection with the OK key.

8) Specify the SIP authentication data:

  a) Scroll to `Registration` and confirm your selection with the OK key.

  b) Scroll to `SIP Session` and confirm your selection with the OK key.

  c) Note the `Realm`, or enter a new realm (e.g., `OSBIZ-SIP`), if necessary.

  d) Note the `User ID`, or enter a new user ID (e.g., `SIP-120`), if necessary.

  e) Specify a `Password` for registering at the SIP server.

  f) Scroll to `Save & Exit` and confirm your selection with the OK key.

9) Use the Back key to go back to the `Admin` menu.

10) If the system telephone needs to be restarted due to the changes made, the menu item `Restart` will appear in the `Admin` menu. Confirm the `Restart` with the OK key and then also confirm `Yes` with the OK key. The system telephone performs a reboot and logs in to the communication system.

4.11 Uninstalling the Communication Software

The software communication can be uninstalled via a text console.

4.11.1 How to Uninstall the Communication Software

Step by Step

1) Open a terminal (e.g., a GNOME terminal).

2) Enter the command `su` (for superuser = root) in the shell interface and confirm it by pressing the Enter key.

3) Enter the password for the "root" user in the shell interface and confirm it by pressing the Enter key.

4) Enter the command `oso_deinstall.sh` in the shell interface and confirm it by pressing the Enter key. Follow the instructions of the uninstallation program.

4.12 Used Ports

The OpenScape Business system components use different ports, which may need to be opened in the firewall as required. For the ports of the web-based clients (e.g., myPortal to go), port forwarding must be configured in the router.

INFO: The ports identified with "O" in the list below are optional, i.e., are not permanently open in the firewall (e.g., the TFTP port is open only when Gate View is activated).

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
System components							
Admin Portal (https)	X		443	X	X	X	X
CAR Update Registration	X		12061	X		X	
CAR Update Server	X		12063	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
Csta Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
Csta Service Provider (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000:40040	O		O	
Gate View	X		8000:8010		O	O	O
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
LDAP server	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
OSBiz Multisite	X		8778		X	X	X

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
OSBiz myReports (http)	X		8101		X	X	X
OsBiz status server	X		8808	X		X	X
OSBiz user portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (embedded)		X	29100:30530	X	X	X	X
RTP (server)		X	29100:30888	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (traps)		X	162	X		X	
SSDP	X		3011	X		X	X
TFTP		X	69		O	O	O
VSL	X		8770		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
XMPP Connection Manager	X		5262		X	X	X
XMPP server	X		5269		X	X	X
Web-based clients							
Web-based clients (http)	X		8801	X	X	X	X
Web-based clients (https)	X		8802	X	X	X	X

INFO: For security reasons, we recommend that only https be used for the web-based clients and that port forwarding be set up from external TCP/443 to internal TCP/8802.

Index

C
concept 7

D
dial plan 37
Display Conventions 7

I
installation 33
Internet Telephony Service Provider (ITSP) 55
IP address scheme 37

J
Java Runtime Environment (JRE) 34

L
license server (CLS)
  edit the IP address 72

O
operating instructions 7

R
remote access
  enable via Internet access with a fixed IP address 71, 73, 74, 75

T
topics, types 7