A MITEL
PRODUCT
GUIDE

Mitel OpenScape Business

OpenScape Business X1/X1W

OpenScape Business V4

Installation Guide

06/2026

A31003-P3030-J105-06-7631

Mitel

Notices

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

Trademarks

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

Contents

1 History of changes

Changes mentioned in the following list are cumulative.

Changes in V3R2 FR1

Impacted chapters	Change description
How to Configure the Sending of E-mails on page 105	Support for OAuth 2.0 authentication
How to Connect the Admin PC to the Communication System on page 48	Removed note concerning LAN port admin

Changes in V3R1

Impacted chapters	Change description
• Warnings: Warning on page 10 • Lightning Protection Requirements on page 16	Added note about grounding
• Protective Grounding on page 26 • How to Provide Protective Grounding for OpenScape Business X1 on page 27 • How to Check the Grounding on page 32 • How to Insert the M.2 SATA / NVMe SSD (system with OCCSB Mainboard) on page 37	New chapters
Connecting Phones and Devices on page 34	Removed ISDN devices

2 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. Before you begin with the installation and startup of the communication system, make sure that you have carefully read the safety information and warnings as well as the important notes.

INFO: The safety information and requirements inform you about the safety and other requirements to be observed. The important notes contain information on the emergency behavior, the standards and guidelines for the installation, and the radio frequency interference of the communication system. In addition, you will also find details on and the proper disposal and recycling of the communication system here.

2.1 About this Documentation

This documentation informs you about the hardware installation and initial setup of the OpenScape Business X1 hardware models.

The information contained in this documentation should only be considered a guideline and does not replace any training.

This document is intended for administrators and service technicians.

For more information beyond the contents of this document, please refer to the *OpenScape Business Service Documentation* and *OpenScape Business Administrator Documentation*.

2.1.1 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 X1, Service Documentation

  This documentation describes the hardware of OpenScape Business X1.

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 @work, User Guide

  This documentation describes the configuration and operation of the UC client myPortal @work.
- UC Smart Telephone User Interface (TUI), Quick Reference Guide

  This documentation describes the voicemail phone menu of the UC solution UC Smart.

2.1.2 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 ...**.

2.1.3 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>`

2.2 Safety Information and Warnings

Safety information and warnings indicate situations that can result in death, injury, property damage, and/or data loss.

Work on the communication systems and devices should **only** be performed by personnel with proper qualifications.

Within the context of this safety information and these warnings, qualified personnel are people who are authorized to ground and label systems, devices, and trunks and put them into operation in compliance with the applicable safety regulations and standards.

Make sure you have read and noted the following safety information and warnings before installing and starting up the communication system:

Make sure you also read carefully and follow all safety information and warnings printed on the communication system and devices.

Familiarize yourself with emergency numbers.

Types of Safety Information and Warnings

This documentation uses the following levels for the different types of safety information and warning:

DANGER: Indicates an immediately dangerous situation that will cause death or serious injuries.

WARNING: Indicates a universally dangerous situation that can cause death or serious injuries.

CAUTION: Indicates a dangerous situation that can cause injuries.

NOTICE: Indicates situations that can cause property damage and/or data loss.

Additional symbols for specifying the source of danger more exactly

The following symbol is generally not used in this documentation, but may appear on the devices or packaging.

ESD - electrostatically sensitive devices

2.2.1 Warnings: Danger

"Danger" warnings indicate immediately dangerous situations that will cause death or serious injury.

DANGER: Risk of electric shock through contact with live wires

- Note: Voltages over 30 VAC (alternating current) or 60 VDC (direct current) are dangerous.
- Only personnel with proper qualifications or qualified electricians should perform work on the low-voltage network (<1000 VAC), and all work must comply with the national/local requirements for electrical connections.

2.2.2 Warnings: Warning

"Warnings" indicate universal dangerous situations that can cause death or serious injury.

WARNING: Risk of electric shock through contact with live wires

- Only use systems, tools and equipment which are in perfect condition. Do not use equipment with visible damage.
- Replace any damaged safety equipment (covers, labels and ground wires) immediately.
- Replace the power cable immediately if it appears to be damaged.
- The communication systems and servers should only be operated with outlets that have connected ground contacts.
- During a thunderstorm, do not connect or disconnect lines and do not install or remove boards.
- Disconnect all power supply circuits if you do not require power for certain activities (for example, when changing cables).

  Before starting any work, make sure that the communication system is de-energized. Never take it for granted that all circuits have reliably been disconnected from the power supply when a fuse or a main switch has been switched off.

- Expect leakage current from the telecommunications network. Disconnect all telecommunication cables from the communication system.
- So long as the power supply is switched on, always observe the greatest caution when performing measurements on powered components and maintenance work on boards and covers.

  Metallic surfaces such as mirrors are conductive. If you touch them, there is a risk of electric shocks or short circuits.
- Use separate ground wires to provide protective grounding for the OpenScape Business X1 communication system. Before you start up the system and connect the phones and phone lines, connect the communication system with a permanent earthing conductor.

2.2.3 Warnings: Caution

"Caution" warnings indicate a dangerous situation that can result in injury.

CAUTION: Risk of explosion caused by the incorrect replacement of batteries

- The lithium battery should only be replaced with an identical battery or one recommended by the manufacturer.

CAUTION: Fire hazard

- Only use communication lines with a conductor diameter of 0.4 mm (AWG 26) or more.

CAUTION: General risk of injury or accidents in the workplace

- After completing test and maintenance work, make sure that all safety equipment is re-installed in the right place and that all covers and the housing are closed.
- Install cables in such a way that they do not pose a risk of an accident (tripping), and cannot be damaged.
- When working on an open communication system or server, make sure that it is never left unattended.
- Use appropriate tools to lift heavy objects or loads.
- Check your tools regularly. Only use intact tools.
- When working on the systems, never wear loose clothing and always tie back long hair.
- Do not wear jewelry, metal watchbands or clothes with metal ornaments or rivets.
- Always wear the necessary eye protection whenever appropriate.
- Always wear a hard hat where there is a risk of injury from falling objects.
- Make sure that the work area is well lit and tidy.

2.2.4 Warnings: Note

"Note" warnings are used to indicate situations that could result in property damage and/or data loss.

The following contains important information on how to avoid property damage and/or data loss:

- Before placing the system into operation, check whether the nominal voltage of the mains power supply corresponds to the nominal voltage of the communication system or server (type plate).
- Follow these ESD measures to protect the electrostatically sensitive devices:
  - Always wear the antistatic wristband in the prescribed manner before performing any work on PC boards and modules.
  - Always place PC boards and modules on a grounded conductive base.
  - Make sure that the components of the communication system (e.g., the boards) are transported and shipped only in the appropriate packaging.
- Use only original accessories. Failure to comply with this safety information may damage the system equipment or violate safety and EMC regulations.
- Sudden changes in temperature can result in condensing humidity. If a communication system or server is transported from a cold environment to warmer areas, for example, this could result in the condensation of humidity. Wait until the communication system or server has adjusted to the ambient temperature and is completely dry before starting it up.
- Connect all cables only to the specified connection points.
- If no emergency backup power supply is available or if no switchover to emergency analog phones is possible in the event of a power failure, then no emergency calls can be made via the communication system following a power failure.
- Before starting wall mounting, check that the wall has sufficient load bearing capacity. Always use suitable installation and mounting materials to mount the communication systems and devices securely.
- Do not allow easily flammable materials to be stored in or near the room where the communication system is installed.

2.2.5 Country-specific Safety Information

Here, you will find information on the specific safety precautions to be observed when installing, starting up and operating the communication systems in certain countries.

2.3 Important Notes

The important notes inform you about emergency procedures and the proper disposal, recycling, intended use and operating conditions of the communication systems and servers. In addition, they also include details concerning the standards and guidelines for the installation, the radio interference characteristics of the communication systems, and data protection and data security.

2.3.1 Emergencies

This section provides information on how to proceed in an emergency.

What To Do In An Emergency

First Aid

Calling for Help

Reporting Accidents

- In the event of an accident, remain calm and controlled.
- Always switch off the power supply before you touch an accident victim.
- If you are not able to immediately switch off the power supply, only touch the victim with non-conductive materials (such as a wooden broom handle), and first of all try to isolate the victim from the power supply.
- Be familiar with basic first aid procedures for electrical shock. A fundamental knowledge of the various resuscitation methods if the victim has stopped breathing or if the victim's heart is no longer beating, as well as first aid for treating burns, is absolutely necessary in such emergencies.
- If the victim is not breathing, immediately perform mouth-to-mouth or mouth-to-nose resuscitation.
- If you have appropriate training, immediately perform heart massage if the victim's heart is not beating.

Immediately call an ambulance or an emergency physician. Provide the following information in the following sequence:

- Where did the accident happen?
- What happened?
- How many people were injured?
- What type of injuries?
- Wait for questions.
- Immediately report all accidents, near accidents and potential sources of danger to your manager.
- Report all electrical shocks, no matter how small.

2.3.2 Proper Use

The communication systems and servers may only be used as described in this documentation and only in conjunction with add-on devices and components recommended and approved by Unify Software and Solutions GmbH & Co. KG.

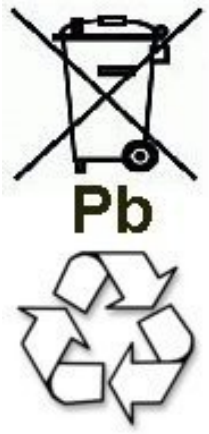
The prerequisites for the proper use of the communication systems and servers include proper transportation, storage, installation, startup, operation and maintenance of the system.

NOTICE: Clean the housing of the communication system and server only with a soft, slightly damp cloth. Do not use any abrasive cleaners or scouring pads.

2.3.3 Correct Disposal and Recycling

Please read the information on the correct disposal and recycling of electrical and electronic equipment and old batteries.

All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities. The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment. For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service, the shop where you purchased the product or your sales representative. The statements quoted above are only fully valid for equipment which is installed and sold in the countries of the European Union and is covered by the directive 2012/19/EU. Countries outside the European Union may have other regulations regarding the disposal of electrical and electronic equipment.



Old batteries that bear this logo are recyclable and must be included in the recycling process. Old batteries that are not recycled must be disposed of as hazardous waste in compliance with all regulations.

2.3.4 Installation Standards and Guidelines

This section provides information on the specifications you must comply with when connecting the communication systems and servers to the power supply circuit and when using shielded cabling for LAN and WAN connectors.

2.3.4.1 Connecting OpenScape Office X to the Power Supply Circuit

The OpenScape Business X communication systems have been approved for connection to TN-S power supply systems. They can also be connected to a TN-C-S power supply system in which the PEN conductor is divided into a

ground wire and a neutral wire. TN-S and TN-C-S systems are defined in the IEC 60364-1 and IEC60364-5-51 standard.

Only qualified electricians should perform any work that may be required on the low-voltage network. These installation activities to connect the communication systems must be performed in compliance with IEC 60364-1 and IEC 60364-4-41 or any corresponding legal norms or national regulations.

2.3.4.2 Shielded Cabling for LAN and WAN Connections of OpenScape Business X

Compliance with CE requirements on electromagnetic compatibility in the OpenScape Business X communication systems and their LAN and WAN connections is subject to the following conditions:

- The communication systems should only be operated using shielded connection cables. This means that a shielded Category 5 (CAT.5) cable with a length of at least 3 m should be used between the shielded LAN and WAN sockets of the communication systems and the building installation port or the external active component port. The cable shield must be grounded at the building installation end or the external active component end (connection to the building's potential equalization terminal).
- A shielded Category 5 (CAT.5) cable should also be used for shorter connections with external active components (LAN switch or similar). However, the active component must feature a shielded LAN connection with a grounded shield connection (connection to the building's potential equalization terminal).
- The shield properties of the cable components should at least satisfy the requirements of the European standard EN 50173-1*) "Information technology - Generic cabling systems" (and all references specified).***)
- Building installations that are fitted with shielded symmetrical copper cables throughout in accordance with the Class-D requirements**) of EN 50173-1 satisfy the above condition.***)

2.3.4.3 Fire Safety Requirements

Fire safety requirements are defined on a country-specific basis in the building regulations. Please follow the valid regulations for your country.

To ensure the legal fire protection and EMC requirements, operate the OpenScape Business X communication systems only when closed. The system may only be opened temporarily for installation and maintenance purposes.

---

*) The European standard EN 50173-1 is derived from the international standard ISO/IEC 11801.

**) Class-D is reached, for instance, if Category-5 (CAT.5) components (cables, wall outlets, connection cables, etc.) are installed.

***) UTP cables (U.S. standard EIA/TIA 568 A/B) are the most widely used cables on the North American market; this has the following implications for the LAN and WAN connections in communication systems: The systems may only be operated with shielded connection cables. This means that a shielded Category 5 (CAT.5) cable with a length of at least 3 m should be used between the shielded LAN and WAN sockets of the communication systems and the building installation port or the external active component port. The cable shield must be grounded at the building installation end or the external active component end (connection to the building's potential equalization terminal).

OpenScape Business system cables comply with the requirements of international norm IEC 60332-1 regarding flammability. The following norms contain similar requirements regarding cables:

IEC 60332-1 Note: IEC 60332-1 is equivalent to test method UL VW-1	EN 60332-1-1 and EN 60332-2-1	DIN EN 60332-1-1 (VDE 0482-332-1-1) and DIN EN 60332-2-1 (VDE 0482-332-2-1)

The division responsible for project planning and service must check whether the IEC 60332-1 norm complies sufficiently with the relevant building regulation and any other applicable regulations.

2.3.4.4 Lightning Protection Requirements

The protection of communication systems against high-energy surges requires a low-impedance ground connection in accordance with the specifications in the *OpenScape Business Installation Guide*.

INFO: Once a communication system has been grounded, check the low-impedance ground connection of the system using the ground conductor of the mains power supply circuit and the low-impedance connection (of the additional permanently-connected protective ground conductor) to the building's potential equalization bus.

NOTICE: Fire hazard due to surge voltage

Telecom lines which are over 500m in length or which must leave the building must be conducted through an additional external lightning protection.

Lightning protection of this kind is known as additional primary protection. The additional primary protection is guaranteed by the professional installation of ÜSAGs (surge arresters, gas filled) in the main distribution frame, the patch panel or at the entry point of the pipe in the building. A gas-filled surge arrester with 230 V nominal voltage is switched to ground from each wire that is to be protected.

Without this additional primary protection, lightning could irreparably damage the boards. This can cause the entire communication system to fail or result in components overheating (fire hazard).

2.3.4.5 Markings for OpenScape Business X

The compliance of the equipment according to EU directives is confirmed by the CE mark. This Declaration of Conformity and, where applicable, other existing declarations of conformity as well as further information on regulations that restrict the usage of substances or affect the declaration of substances used in products can be found in the Unify Expert WIKI at http://wiki.unify.com under the section “Declarations of Conformity”.

2.3.5 Notes on Electromagnetic and Radio Frequency Interference of OpenScape Business X

The OpenScape Business X communication systems are Class B devices in accordance with EN 55032.

2.3.6 Data Protection and Data Security

Please note the details below with respect to protecting data and ensuring privacy.

The communication systems and servers described in this documentation process and use personal data for purposes such as call detail recording, displays, and customer data acquisition.

In Germany, the processing and use of such data is subject to various regulations, including those of the General data Protection Regulation (GDPR) and the Federal Data Protection Law (Bundesdatenschutzgesetz, BDSG). For other countries, please follow the appropriate national laws.

The aim of data protection is to protect the rights of individuals from being adversely affected by use of their personal data.

In addition, the aim of data protection is to prevent the misuse of data when it is processed and to ensure that one’s own interests and the interests of other parties which need to be protected are not affected.

INFO: The customer is responsible for ensuring that the communication systems and servers are installed, operated and maintained in accordance with all applicable labor laws and regulations and all laws and regulations relating to data protection, privacy and safe labor environment.

Employees of Unify Software and Solutions GmbH & Co. KG are bound to safeguard trade secrets and personal data under the terms of the company’s work rules.

In order to ensure that the statutory requirements are consistently met during service – whether on-site or remote – you should always observe the following

rules. You will not only protect the interests of your and our customers, you will also avoid personal consequences.

A conscientious and responsible approach helps protect data and ensure privacy:

- Ensure that only authorized persons have access to customer data.
- Take full advantage of password assignment options; never give passwords to an unauthorized person orally or in writing.
- Ensure that no unauthorized person is able to process (store, modify, transmit, disable, delete) or use customer data in any way.
- Prevent unauthorized persons from gaining access to storage media such as backup CDs and DVDs or log printouts. This applies to service calls as well as to storage and transport.
- Ensure that storage media which are no longer required are completely destroyed. Ensure that no sensitive documents are left unprotected.
- Work closely with your customer contact; this promotes trust and reduces your workload.

2.3.7 Technical Regulations and Conformity of OpenScape Business X

Details on how the OpenScape Business X communication systems meet conformity requirements can be found here.

2.3.7.1 CE Conformity

The CE certification is based on: 2014/35/EU - Low Voltage Directive (LVD); (Official Journal of the EU L96, 29.03.2014, p. 357-374) 2014/30/EU - Electromagnetic Compatibility Directive (EMC); (Official Journal of the EU L96, 29.03.2014, p. 79-106) 2011/65/EU - Restriction of the use of certain Hazardous Substances Directive (RoHS); (Official Journal of the EU L174, 01.07.2011, p. 88–110)

	Standards reference
Safety	EN 62368-1
Electromagnetic Compatibility EMC	EN55032 (EMC Emission) EN55024 (EMC Immunity Residential)

2.3.7.2 Conformity with International Standards

	Standards reference
Safety	IEC 60950-1 and IEC 62368-1
EMC Emission	CISPR 32

2.3.8 Operating Conditions

Note the environmental and mechanical conditions for operating OpenScape Business X1.

Environmental Operating Conditions

Operating limits:

- Room temperature: + 5 to + 40 °C (41 to 104 °F)
- Absolute humidity: 1 to 25 g H_2O/m^3
- Relative humidity: 5 to 80%

Ventilation of the communication system is by convection only.

NOTICE: Damage caused by local temperature increases

Avoid exposing the communication systems to direct sunlight and other sources of heat.

NOTICE: Damage caused by condensation due to humidity

Avoid any condensation of humidity on or in the communication systems before or during operation under all circumstances.

A communication system must be completely dry before you put it into service.

Mechanical Operating Conditions

The communication systems are intended for stationary use.

3 Preparing for the Installation of OpenScape Business X1

Before the OpenScape Business X1 communication system can be set up and put into operation for the first time, a suitable installation site must be found, and some preparatory activities must be performed.

3.1 Prerequisites for the Installation

A number of different tools and resources are required for the installation of OpenScape Business X1. Certain requirements must be observed when selecting the installation site.

OpenScape Business X1 can only be wall-mounted.

Warning: Only authorized service personnel should install and start up the communication system.

Tools and Resources

The following tools and resources are required:

- Diagonal cutting pliers, telephone pliers, wire stripper, flat-nosed pliers
- Slotted screwdriver set
- Phillips or Pozidriv screwdriver set
- TORX screwdriver set
- Electric drill, hammer
- Level, tape measure
- Digital multimeter for testing ground connections and partial voltages

Prerequisites for Selecting the Installation Site

Make sure that the installation site meets the following requirements:

- The following minimum clearances to the housing must be maintained to guarantee sufficient ventilation for the communication system:
  - Left side: 10 cm (for the Service Board)
  - Top: 20 cm
  - Right side and bottom: 30 cm each
- The power cable connector must be readily accessible for quick disconnection from the power source at any time.
- Do not expose the communication system (and the 19" rack) to direct sources of heat (for example, direct sunlight, radiators, etc).
- Do not expose the communication system (and the 19" rack) to extremely dusty environments.
- Avoid any contact between the communication system (and the 19 " rack) and chemicals.
- Avoid all condensation of humidity on or in the communication system during operation under all circumstances.

  The communication system must be completely dry before putting it into service.
- Avoid standard carpeting, as it tends to produce electrostatic charges.

- Note the environmental and mechanical conditions for operating the communication system.
- Allow sufficient space for a main distribution frame or other additional equipment.

Special Prerequisites for Selecting the X1 Installation Site

Make sure that the installation site meets the following requirements:

- The following minimum clearances to the housing must be maintained to guarantee sufficient ventilation for the communication system:
  - Left side: 10 cm (for the Service Board)
  - Top: 20 cm
  - Right side and bottom: 30 cm each

3.2 Preparatory Steps

Unpack and check the supplied components before starting the installation. The housing cover must be removed.

3.2.1 How to Unpack the Components

Proceed as follows to unpack the communication system and parts supplied:

Step by Step

1) Open the packaging without damaging the contents.
2) Check the components delivered against the packing slip to make sure nothing is missing.
3) Report any shipping damage to the address indicated on the packing slip.
4) All packaging material must be disposed of in compliance with the relevant country-specific requirements.

WARNING:

Risk of electric shock through contact with live wires

Only use communication systems, tools and equipment which are in perfect condition. Do not use equipment with visible damage.

3.2.2 How to Remove the X1 Housing Cover

DANGER:

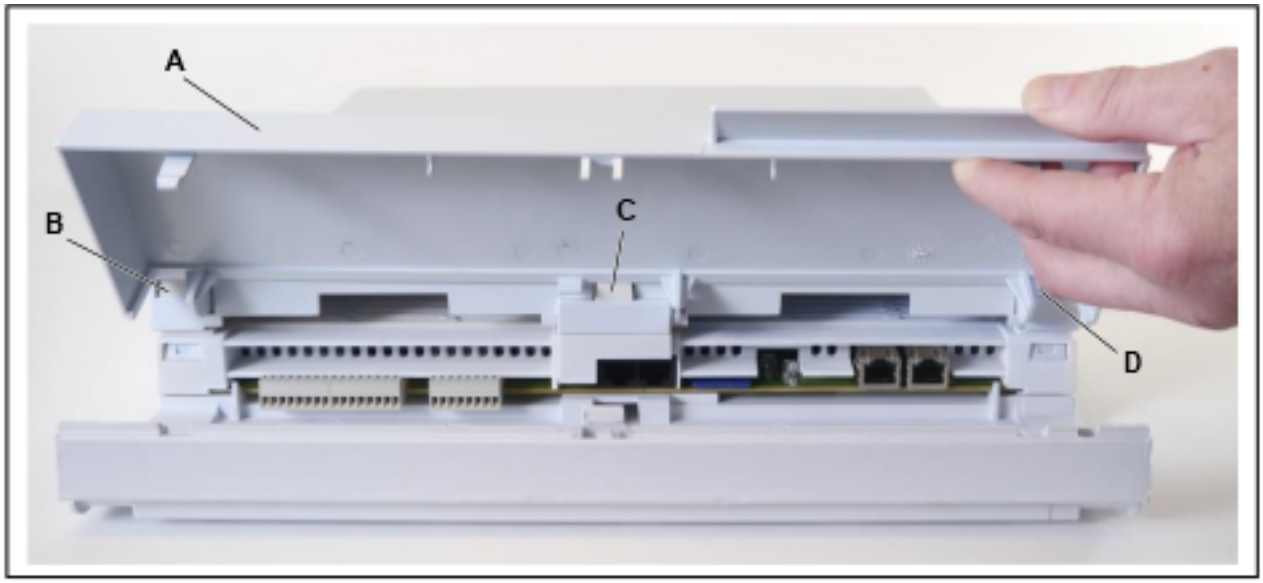
Risk of electric shock through contact with live wires

Make sure that the communication system is de-energized.

Step by Step

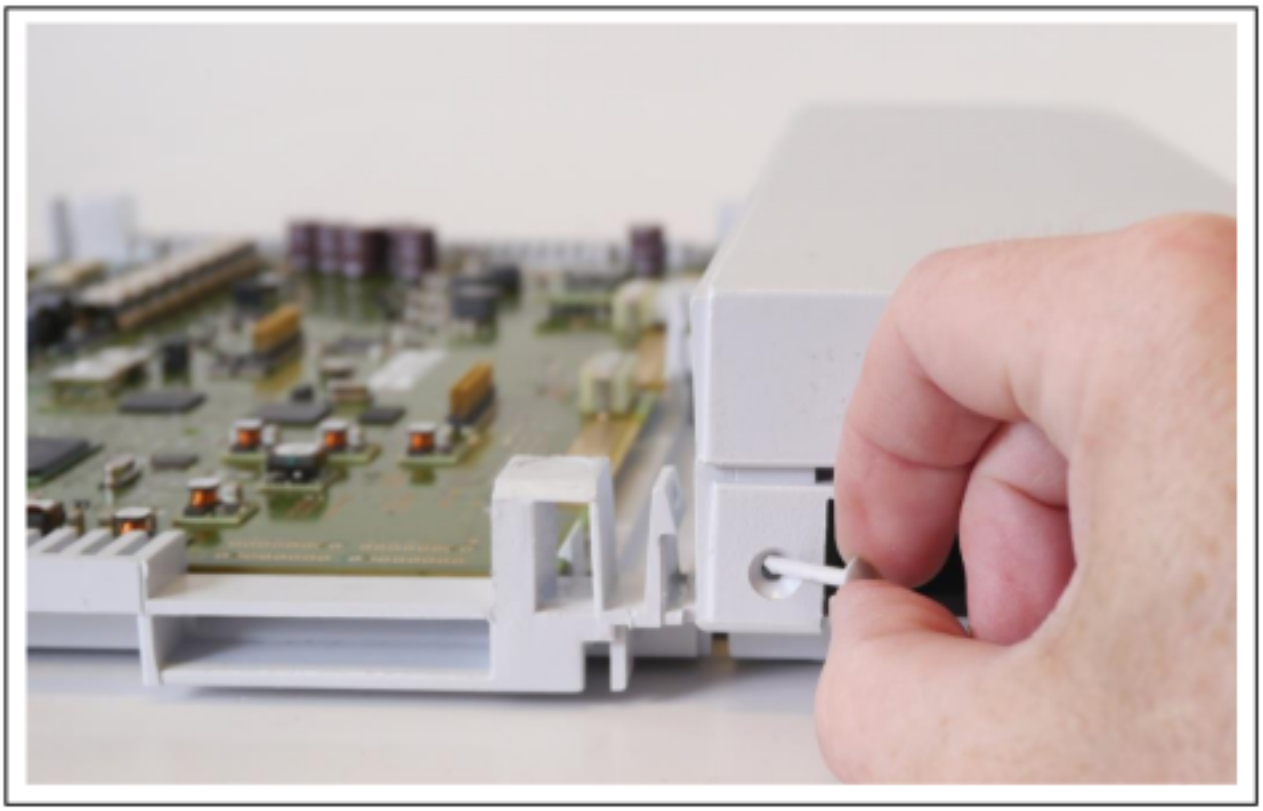
1) Disconnect the power plug of the communication system.

2) Lift open the left housing cover (A) and remove it. You have access to the connections of the communication system.

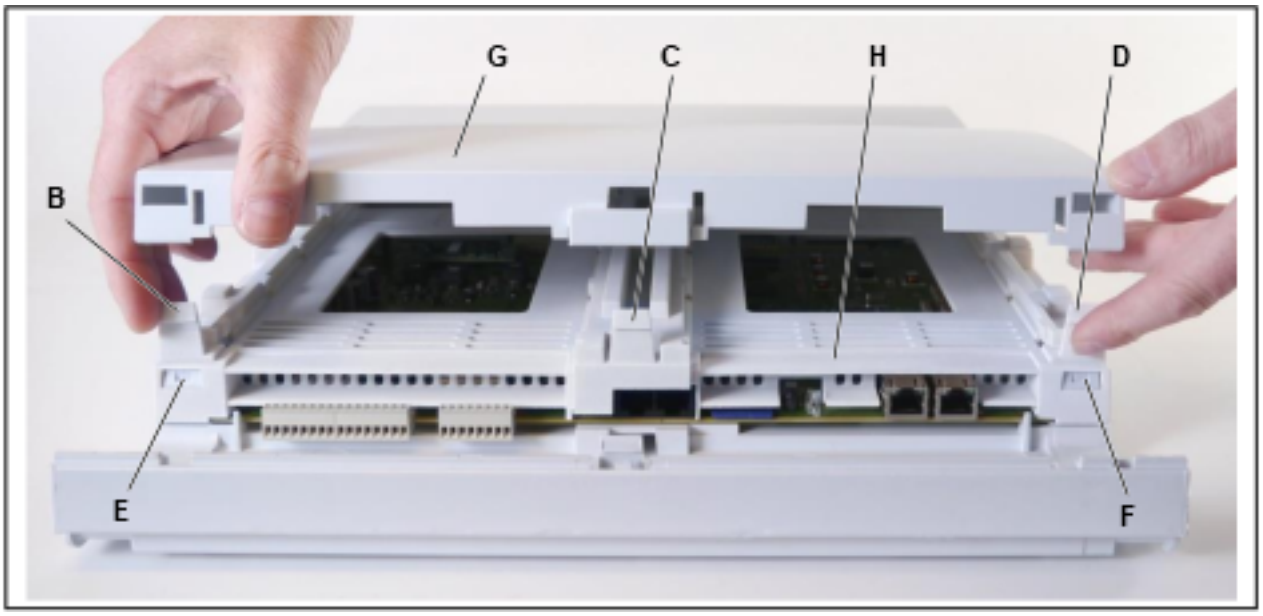


3) You may also need access to the mainboard. To do this, proceed as follows:

a) Pull out the two retaining pins at the top and bottom of the right housing cover (includes power supply) and slide the right housing cover slightly to one side.



b) Use a small slotted screwdriver to press the 3 latches (B, C and D) of the middle housing cover (G) inward and remove the middle cover (G).



c) Use a small slotted screwdriver to press the two front latches (E and F) of the middle frame (H) inward. Then press the three rear latches of the middle frame (H) inward and remove the middle frame.

4 Installing the Hardware for OpenScape Business X1

This section covers the standard installation procedure for the OpenScape Business X1 communication system.

OpenScape Business X1 can only be wall-mounted.

WARNING:

Risk of electric shock through contact with live wires

- Work on the housing must only be performed in the de-energized state.
- Before starting any work, make sure that all circuits are de-energized. Never take it for granted that all circuits have reliably been disconnected from the power supply when a fuse or a main switch has been switched off.

4.1 Type of Installation

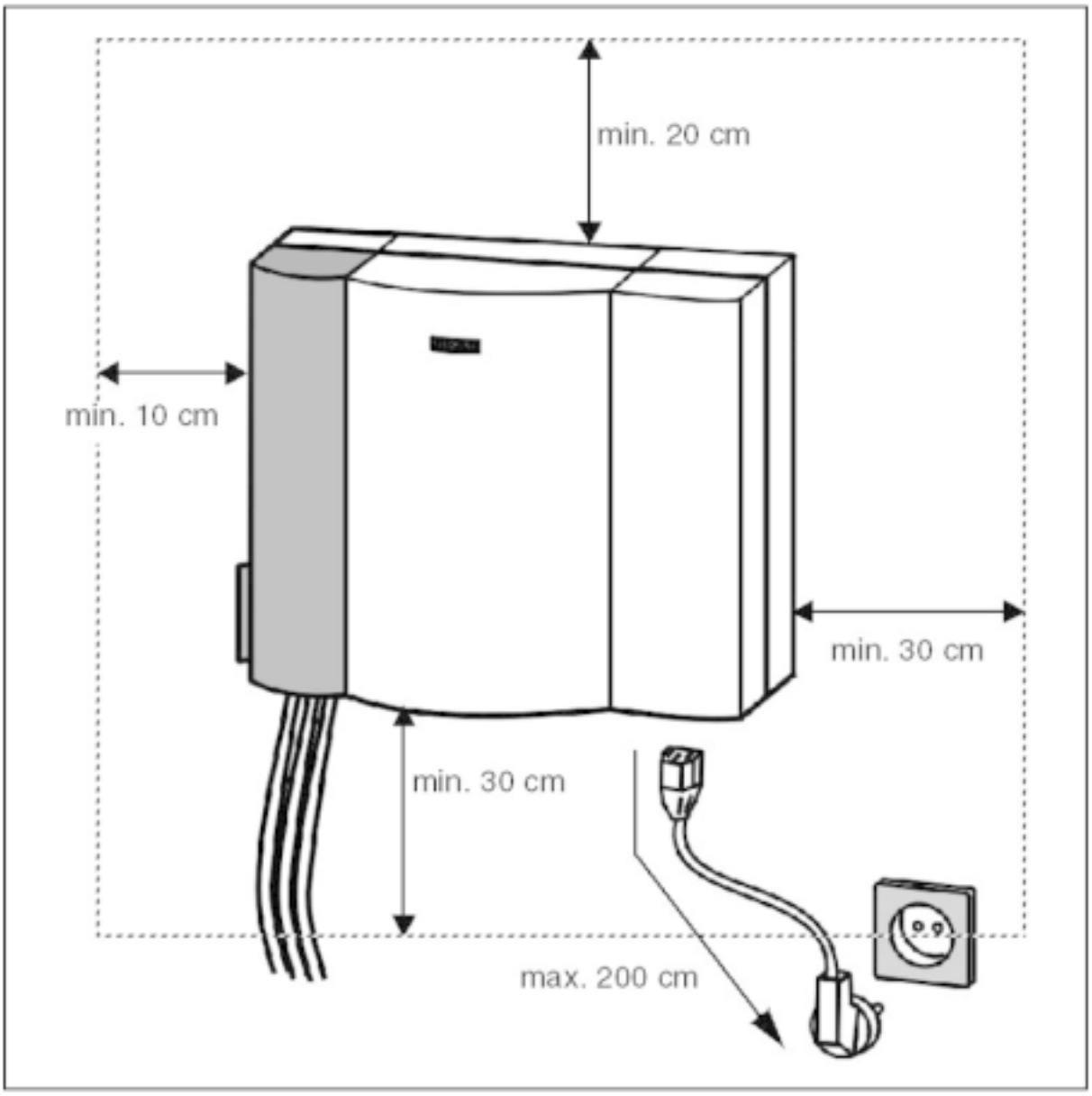
The OpenScape Business X1 communication system is released exclusively for wall mounting.

4.1.1 How to Mount the Communication System to a Wall

Prerequisites

The prerequisites for selecting the installation site were taken into account (see Prerequisites for the Installation on page 20).

A strong wall with enough space for the installation of the communication system is available.


min. 20 cm
min. 10 cm
min. 30 cm
min. 30 cm
max. 200 cm

Step by Step

1) Drill a dowel hole for mounting hole A.

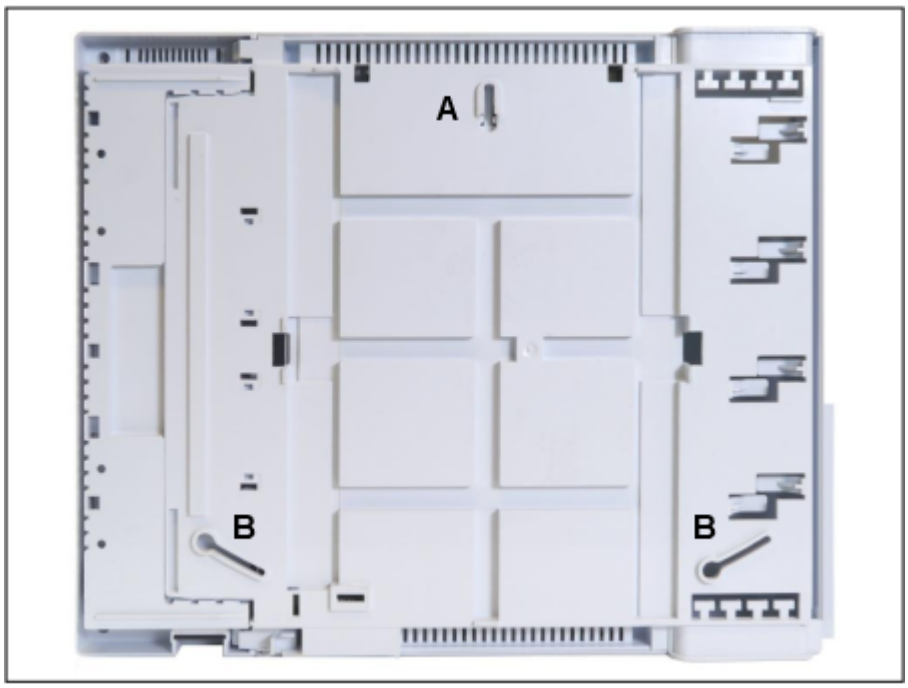


Figure 1: OpenScape Business X1 - Mounting Holes in the Rear Wall of the Housing

2) Insert the wall anchor into the drilled hole and screw in the screw, leaving approx. 5 mm projecting.

3) Hang the communication system on the screw at the mounting hole A and align it.

4) Draw two more dowel holes for the two mounting holes B and remove the communication system again.

5) Drill the two holes for the wall anchors.

6) Insert the wall anchors into the drill holes and screw in the screws, leaving approx. 5 mm projecting.

7) Hang the communication system on the screws at the mounting holes and align it.

8) Tighten all three screws.

4.2 Protective Grounding

The protective grounding provides a secure connection to the ground potential to protect against dangerously high touch voltages in the event of a malfunction.

The mainboard used in OpenScape Business X1 dictates if the protective grounding is required or not.

- Systems with built-in OCCS mainboard need not be connected to protective ground.
- Systems with built-in OCCSB mainboard require connection to protective ground.

The subsequent description referes to OpenScape Business systems with built-in OCCBS maniboard only. These systems are equipped with a protective ground connector at the right side of the power supply housing.

WARNING:

Risk of electric shock through contact with live wires

- Use separate ground wires to provide protective grounding for the OpenScape Business X1 communication system and possibly any main distribution frames being used. Connect your communication system and your main distribution frame to the ground wire before starting up the system and connecting telephones and lines.
- Make sure that the ground wires laid are protected and strain-relieved.

WARNING:

Assembly of Protection Ground Terminal

In case of a migration from HiPath 500 or from OpenScape Business X1 with OCCB mainboard to OpenScape Business X1 with OCCBS mainboard, the protection ground terminal has to be installed as shown in Figure 2: Assembly of the protection ground terminal on page 27.

Afterwards, the protection ground wire has to be connected as described in How to Provide Protective Grounding for OpenScape Business X1 on page 27.

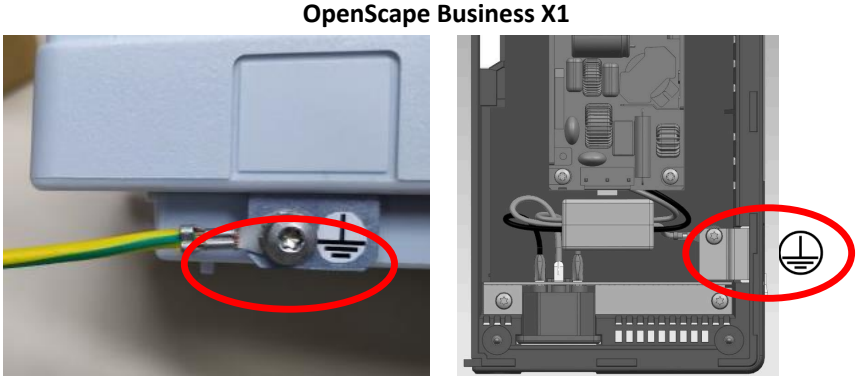


Figure 2: Assembly of the protection ground terminal

4.2.1 How to Provide Protective Grounding for OpenScape Business X1

Prerequisites

A low-impedance ground connection is available.

DANGER:

Risk of electric shock through contact with live wires

Only personnel with proper qualifications or qualified electricians should perform work on the low-voltage network (<1000 VAC) and all work must comply with the national/local requirements for electrical connections.

WARNING:

Risk of electric shock through contact with live wires

- Use separate ground wires to provide protective grounding for the OpenScape Business X1 communication system and possibly any main distribution frames being used. Connect your communication system and your main distribution frame to the ground wire before starting up the system and connecting telephones and lines.
- Make sure that the ground wires laid are protected and strain-relieved.

The grounding of the communication system and the external main distribution frame must be performed from the grounding point in a star configuration.

The implementation rules specified in IEC 60364, IEC 60950-1 and IEC 62368-1 must be complied with during the installation.

Proceed as follows to ensure protective grounding:

Step by Step

1) Attach a separate ground wire to the communication system's ground terminal.

2) Provide strain relief for the ground wire by securing it to of the communication system with a cable tie.

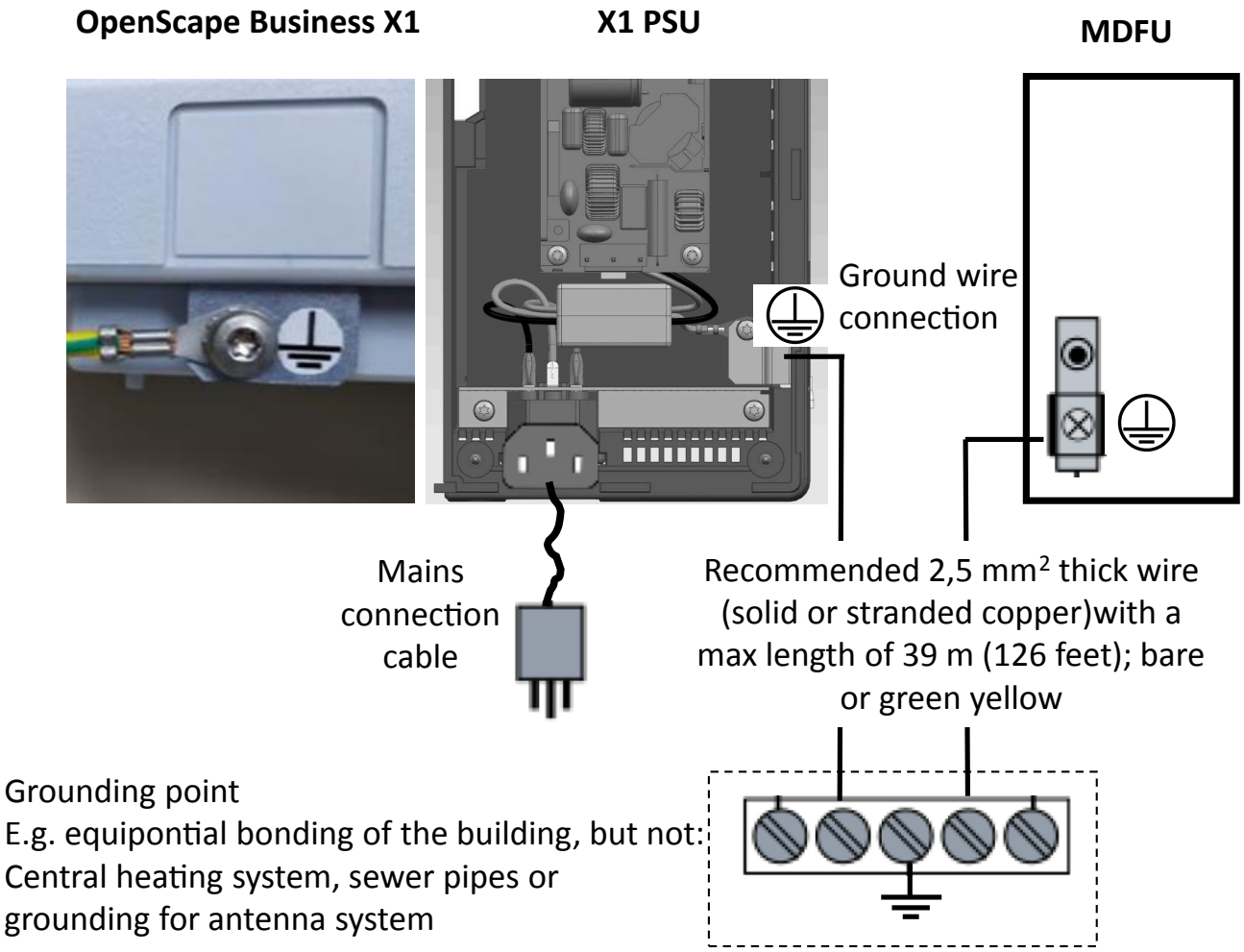
3) If an MDFU is present: Attach a separate ground wire to the ground terminal of the MDFU main distribution frame.

4) If an MDFU is present: Provide strain relief for the ground wire by securing it to the housing of the main distribution frame MDFU with a cable tie.

5) Select one of the following options:

- **Not for U.S. and Canada - Equipotential bonding strip**

  Connect the separate ground wire(s) with the grounding point (e.g., the equipotential bonding strip of the building) as illustrated in the conceptual diagram.

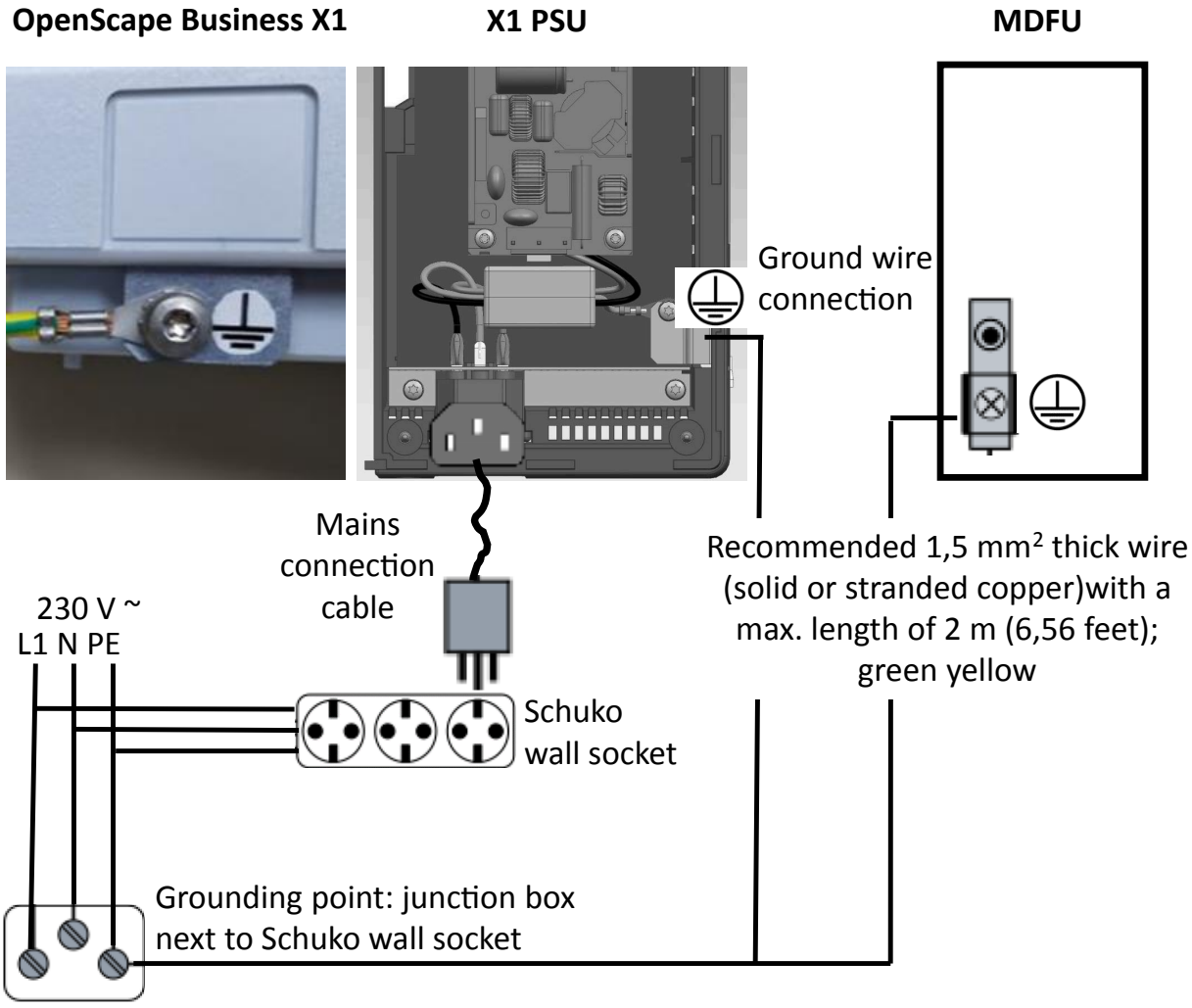


Make sure that all ground wires laid are protected and strain-relieved. The minimum conductor cross-section is 12 AWG/2.5 mm^2. A minimum conductor cross section of 10 AWG/4 mm^2 is needed to block the effects of external factors if the ground wire cannot be protected.

- **Not for U.S. and Canada - Outlet to the low-voltage network**

  Connect a junction box to the low-voltage network close to the Schuko wall socket into which the communication system is plugged. Use a

separate ground wire to set up a fixed connection to the junction box as illustrated in the conceptual diagram.



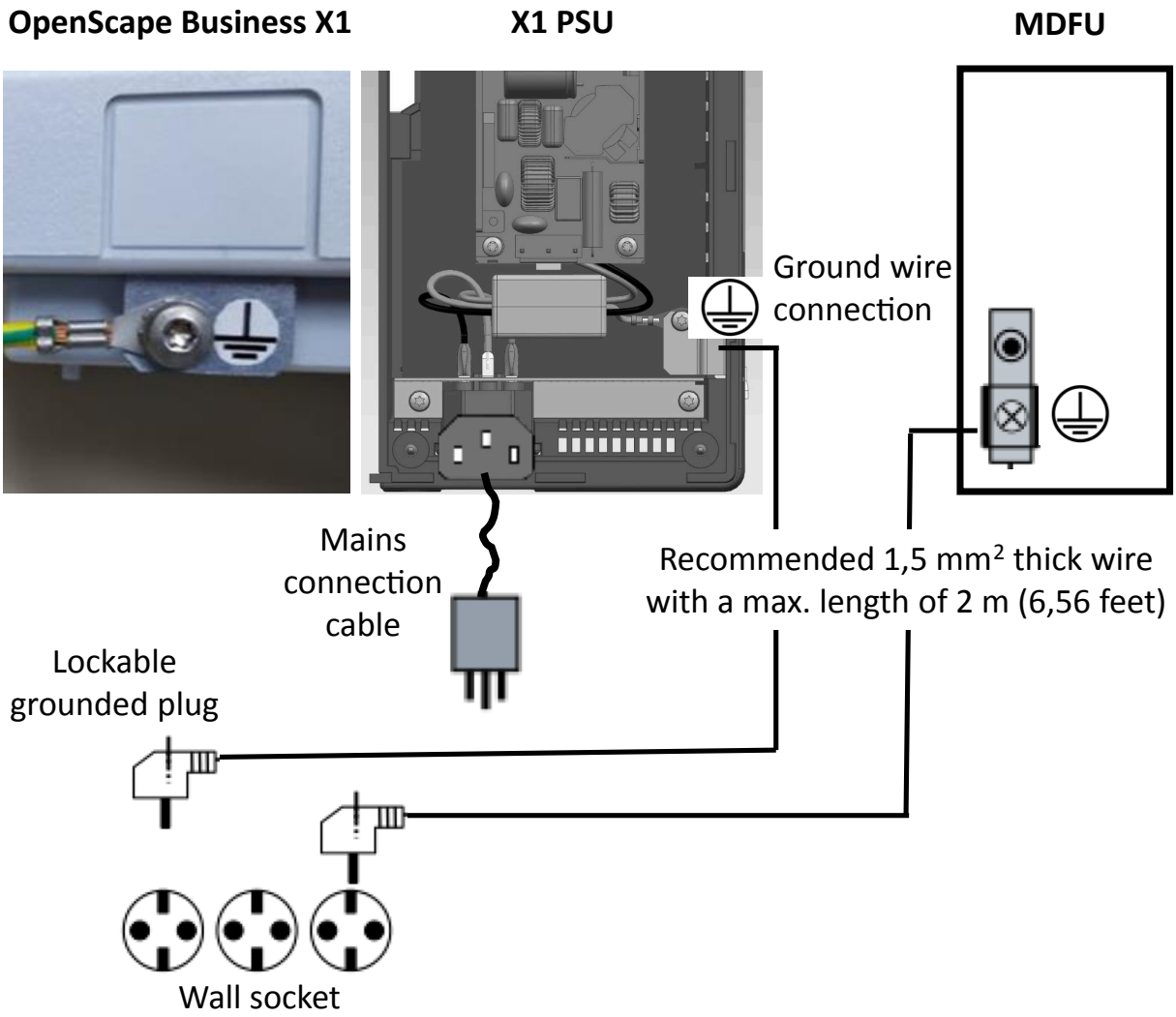
Make sure that all ground wires laid are protected and strain-relieved.

The minimum conductor cross-section is 16 AWG/1.5 mm^2.

- **Not for U.S. and Canada - Lockable grounded plug to the low-voltage network**

  Insert the lockable grounded plug (special Schuko with fixed protective earth conductor) into a wall outlet of the low-voltage network and lock the plug. Use the ground wire connected to the plug to set up a fixed connection to the communication system, as illustrated in the conceptual

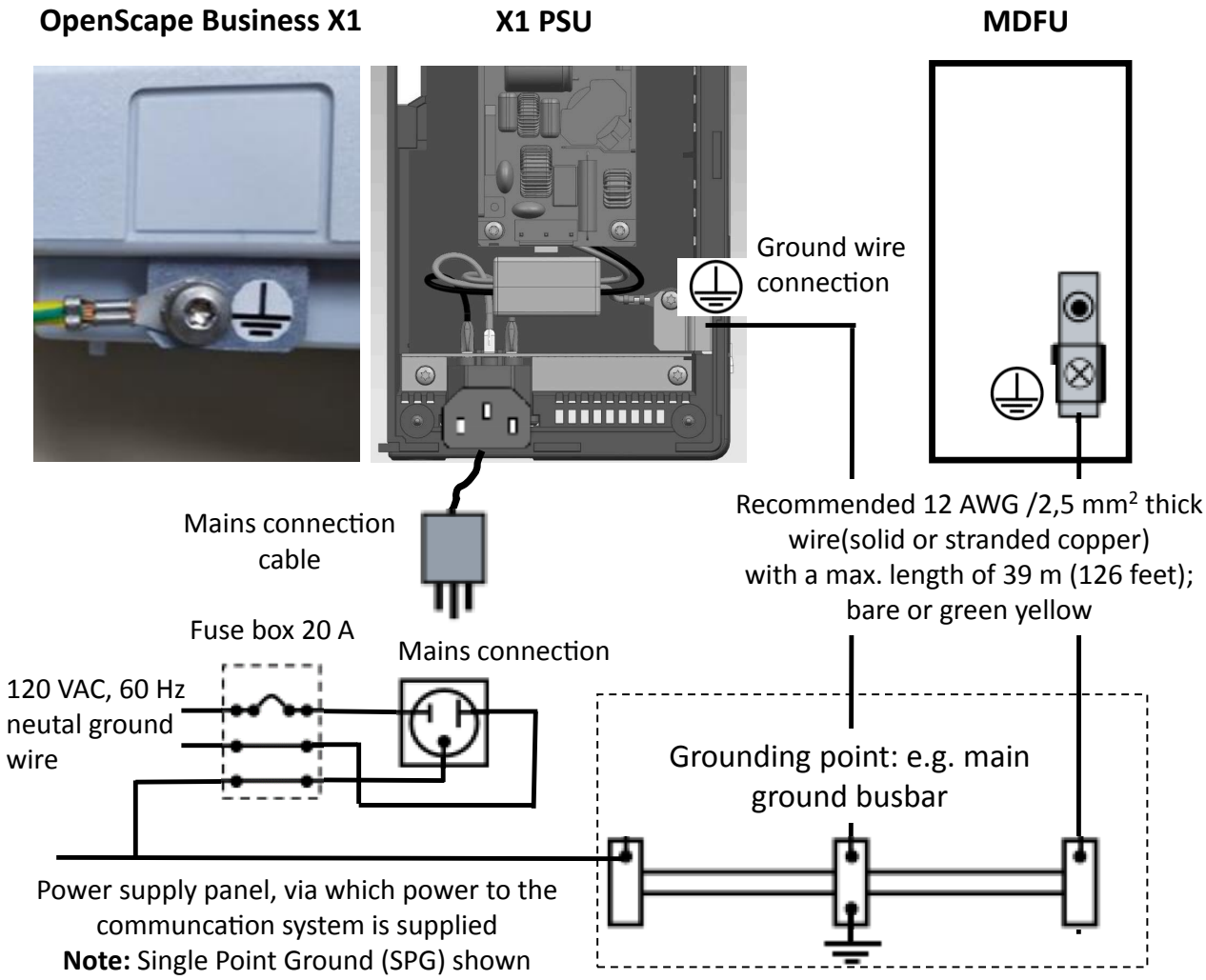
diagram. Use a second lockable grounded plug for a possibly existing MDFU.



Make sure that all ground wires laid are protected and strain-relieved. The minimum conductor cross section is 16 AWG/1.5 mm^2 for up to 2m and at least 12 AWG/2.5 mm^2 for 2m and above.

- **For U.S. and Canada only: Main ground busbar**

  Connect the separate ground wire(s) with the grounding point (e.g., the main ground busbar, ground field) as illustrated in the conceptual diagram.



Make sure that all ground wires laid are protected and strain-relieved. The minimum conductor cross-section is 12 AWG/2.5 mm^2. A minimum conductor cross section of 10 AWG/4 mm^2 is needed to block the effects of external factors if the ground wire cannot be protected.

4.2.2 How to Check the Grounding

Prerequisites

The communication system is **not yet** connected to the low-voltage network via the power cable.

The communication system and the main distribution frame have been properly grounded using separate ground wires.

Run the following test before startup to make sure that the protective grounding for the communication system and the MDF (if any) is working properly.

Step by Step

1) Check the ohmic resistance of the separate ground connection to the communication system:

   The measurement is taken between the ground contact of a grounded power outlet of the home installation (where the communication system is connected) and the housing of the communication system.
2) If a main distribution frame is used, check the ohmic resistance of the separate ground connections to the main distribution frame.

   The measurement is taken between the ground contact of a grounded power outlet of the home installation (where the communication system is connected) and the housing of the main distribution frame.

The result (reference value) of a measurement must be significantly less than 10 Ohms.

If you obtain some other results, contact a qualified electrician. The electrician will need to check the equipotential bonding of the domestic installation and ensure the low resistance grounding (ohmage) of the earthing conductors.

4.3 WAN and LAN Port

OpenScape Business X1 and offer two Ethernet ports (10BaseT/ 1 Gb) for WAN and LAN connections via 8-pin RJ45 sockets, for example, to connect to an Internet router.

4.3.1 How to Set up a WAN or LAN Connection

Prerequisites

CAUTION:

Fire hazard

To reduce the risk of fire, you may only use communication cables with a conductor diameter of at least 0.4mm (AWG 26) or larger. The recommended cable is a shielded Cat.5 cable (multi-element cables characterized up to 100 MHz - horizontal and building backbone cables as per EN 50288). These are specified with a conductor diameter from 0.4 mm to 0.8 mm.

At least one free WAN or LAN port is available.

Step by Step

Connect the desired WAN or LAN port to the device to be connected (LAN switch, Internet router, DSL modem, etc.).

4.4 Connecting Phones and Devices

Different types of phones and devices can be connected to the OpenScape Business X1 offer. The connection is made directly at the board.

You can select the connection(s) required for your communication system from the following options:

- Connection of $U_{P0/E}$ phones
- Connection of analog devices

$U_{P0/E}$ Phones and Analog Devices

For $U_{P0/E}$ telephones and analog devices, edge connectors with Wieland screw clamps are inserted directly onto the X1, X2 and X3 connectors of the mainboard. On these edge connectors, the connection cables of the telephones are either connected directly to the screw clamps or to any other edge connectors that may already be attached to the screw clamps:

- Connectors X1 and X2: $U_{P0/E}$ interfaces for connecting $U_{P0/E}$ telephones
- Connector X3: a/b interfaces for connecting analog devices

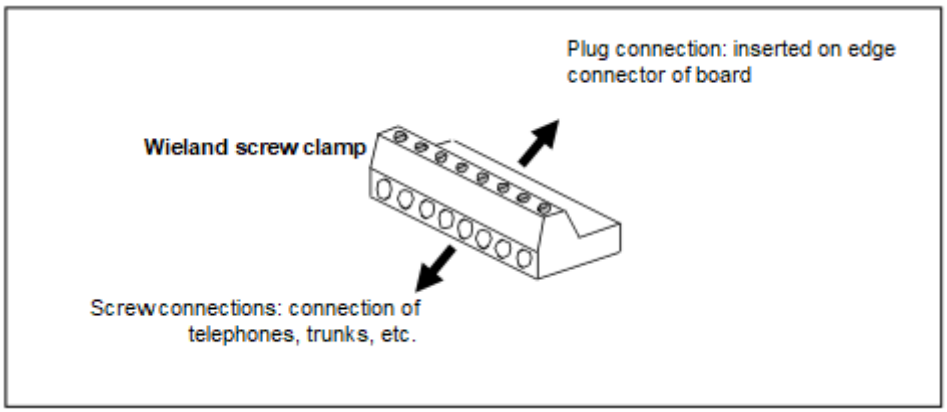


Figure 3: Wieland screw clamp

4.4.1 How to Connect $U_{P0/E}$ Phones

Prerequisites

WARNING: Risk of electric shock through contact with live wires. Use separate ground wires to provide protective grounding for your communication system and any main distribution frames used before connecting telephones and lines.

CAUTION: Fire hazard

To reduce the risk of fire, you may only use communication cables with a conductor diameter of at least 0.4mm (AWG 26) or larger.

NOTICE: Fire hazard due to surge voltage

In the case of line lengths exceeding 500 m and where the lines exit the building, the OCCS or OCCSB mainboard must be protected by external lightning protection.

Lightning protection of this kind is known as additional primary protection. The additional primary protection is guaranteed by installing ÜSAGs (surge arresters, gas filled) in the patch panel or at the entry point of the pipe in the building. A gas-filled surge arrester with 230 V nominal voltage is switched to ground from each wire that is to be protected.

At least one free $U_{P0/E}$ interface is available on an OCCS or OCCSB mainboard.

Step by Step

1) Insert the plug of the connection cable into the $U_{P0/E}$ telephone.
2) Secure the wires of the connection cable to the plug connector and insert it into one of the two edge connectors X2 or X3 of the $U_{P0/E}$ interfaces.

   For more detailed information on cable and pin assignments, see OCCS.

   INFO:

   Refer to the installation instructions of the phone to be connected.
3) If present, connect any further $U_{P0/E}$ phones to the communication system by the same method.

4.4.2 How to Connect Analog Devices

Prerequisites

WARNING: Risk of electric shock through contact with live wires. Use separate ground wires to provide protective grounding for your communication system and any main distribution frames used before connecting telephones and lines.

CAUTION: Fire hazard

To reduce the risk of fire, you may only use communication cables with a conductor diameter of at least 0.4mm (AWG 26) or larger.

NOTICE: Fire hazard due to surge voltage

In the case of line lengths exceeding 500 m and where the lines exit the building, the OCCS or OCCSB mainboard must be protected by external lightning protection.

Lightning protection of this kind is known as additional primary protection. The additional primary protection is guaranteed by installing ÜSAGs (surge arresters, gas filled) in the patch panel

or at the entry point of the pipe in the building. A gas-filled surge arrester with 230 V nominal voltage is switched to ground from each wire that is to be protected.

At least one free a/b interface is available on an OCCS or OCCSB mainboard.

Step by Step

1) Insert the plug of the connection cable into the analog device (telephone, fax, modem, TFE-S, etc.).
2) Secure the wires of the connection cable to the plug connector and insert it into the X3 edge connector of the a/b interfaces.

   For more detailed information on cable and pin assignments, see OCCS.

   INFO:

   Refer to the installation instructions of the phone/device to be connected.

3) If present, connect any further analog telephones to the communication system by the same method.

4.5 Closing Activities

To complete the installation, the SDHC card in case of OCCS mainboard or the M.2 SATA / NVMe SSD in case of OCCSB mainboard must be inserted. A visual inspection must be performed, the housing cover must be reattached, and the system must be connected to the mains power supply.

The communication system can then be put into operation with the OpenScape Business Assistant (WBM). The description of this can be found in the online help of the WBM or in the Administrator Documentation in the section "Initial Installation of OpenScape Business".

NOTICE: During the initial startup of the communication system, the charge state of the battery on the mainboard is undefined. To achieve an adequate charge state, the system must remain connected to the mains for at least 2 days. If the system is disconnected from the mains power supply, the battery may be insufficiently charged and could potentially cause the activation period to be blocked due to time manipulation

4.5.1 How to Insert the SDHC Card (system with OCCS Mainboard)

The SDHC card contains the OpenScape Business communication software and must be inserted before starting up the communication system.

Step by Step

1) Make sure that the write protection of the SDHC card is disabled (switch directed toward metal contacts).

2) Insert the SDHC card into the SDHC slot of the mainboard until it snaps into place. The metal contacts of the SDHC card must point towards the mainboard.

4.5.2 How to Insert the M.2 SATA / NVMe SSD (system with OCCSB Mainboard)

The M.2 SATA SSD contains the OpenScape Business communication software and must be inserted before starting up the communication system. The NVMe SSD is optional and contains media data for UC Suite, further trace capabilities and local backup options.

DANGER:

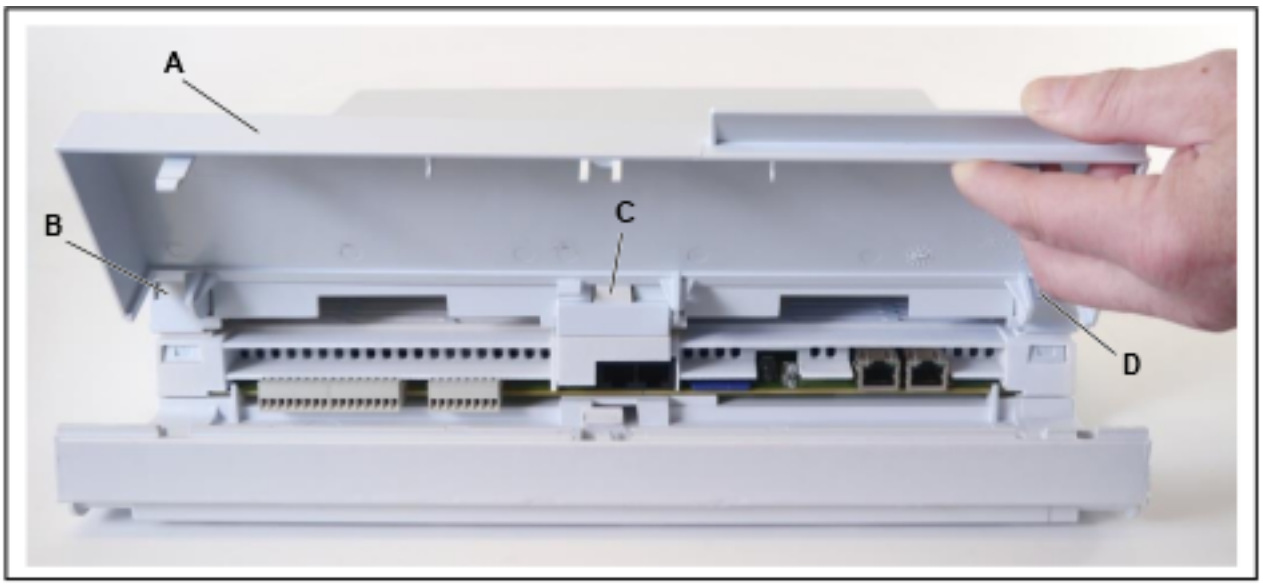
Risk of electric shock through contact with live wires

Make sure that the communication system is de-energized.

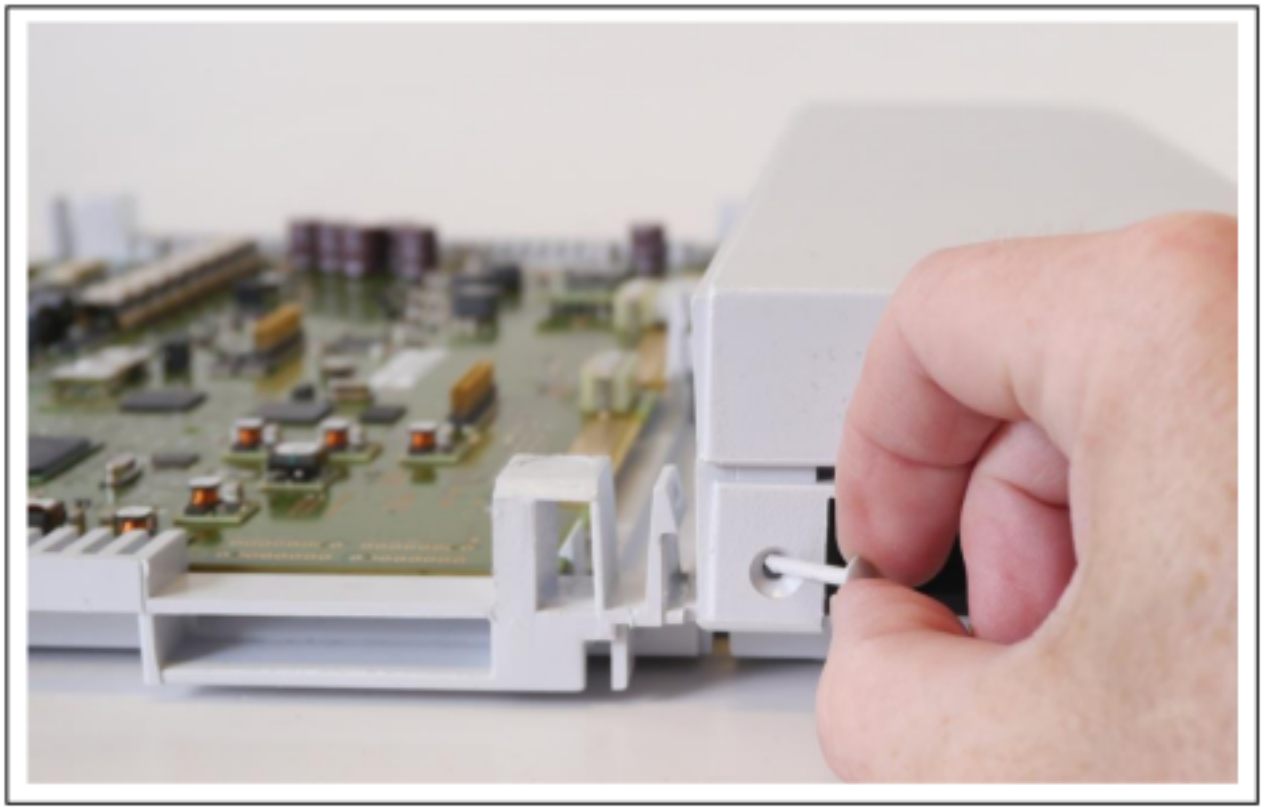
Step by Step

1) Disconnect the power plug of the communication system.

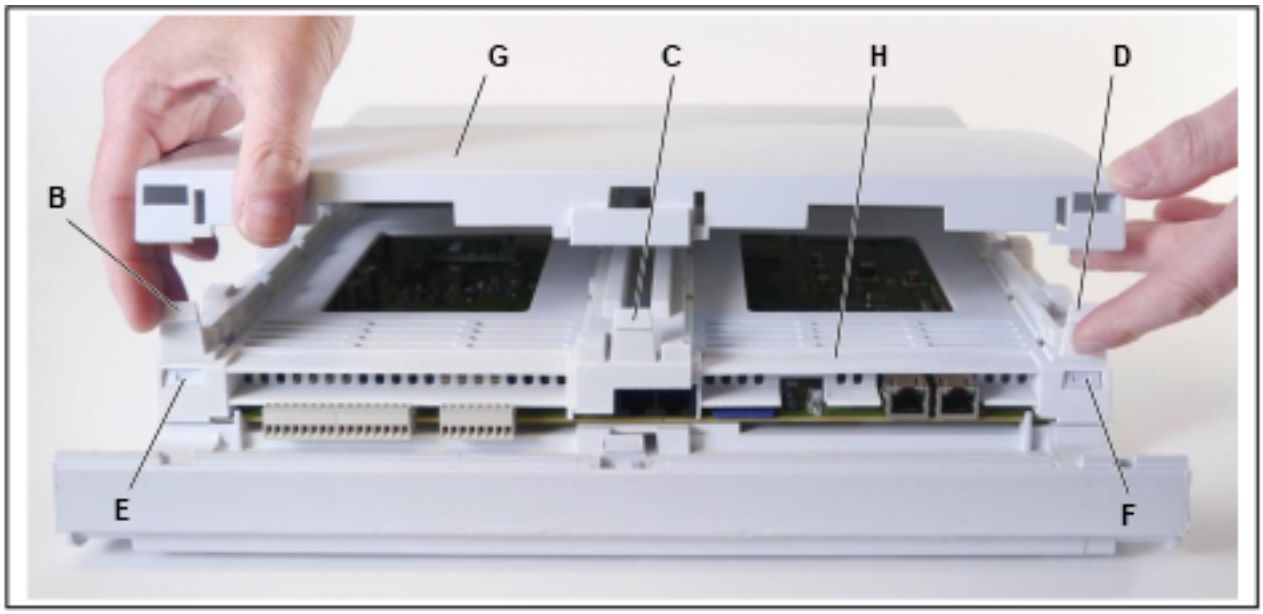
2) Lift open the left housing cover (A) and remove it.



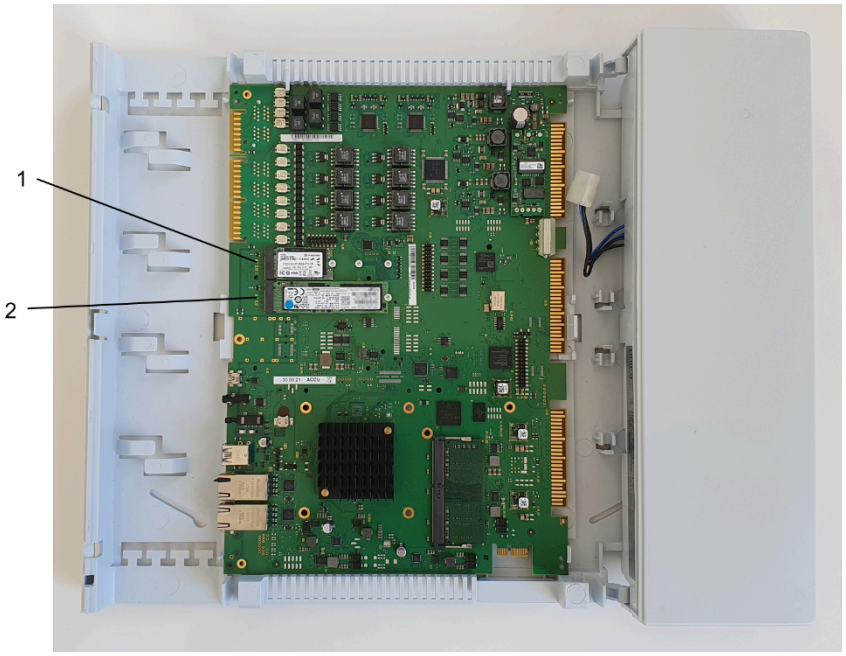
3) Pull out the two retaining pins at the top and bottom of the right housing cover (includes power supply) and slide the right housing cover slightly to one side.



4) Use a small slotted screwdriver to press the 3 latches (B, C and D) of the middle housing cover (G) inward and remove the middle cover (G).



5) Use a small slotted screwdriver to press the two front latches (E and F) of the middle frame (H) inward. Then press the three rear latches of the middle frame (H) inward and remove the middle frame.



6) Lift the mainboard carefully out of the brackets to get access to the backside of the mainboard.
7) Remove the pre-assembled screw on the M.2 SATA slot (1) of the OCCBS mainboard.
8) Insert the M.2 SATA SSD into the M.2 SATA slot (1) of the mainboard.
9) Optional: Remove the pre-assembled screw on the NVMe slot (2) of the OCCBS mainboard.
10) Optional: Insert the NVMe SSD into the NVMe slot (2) of the mainboard.
11) Fasten the M.2 SATA SSD (optional NVMe SSD) to the mainboard with the screw you removed before.
12) Reinstall the mainboard.
13) Lock the middle frame back into its brackets.
14) Slide the right housing cover (power supply) back and insert the two retaining pins at the top and bottom in the right housing cover.
15) Lock the middle housing cover in its brackets.
16) Place back the left housing cover and close it.
17) Place the communication system back into operation.

4.5.3 How to Perform a Visual Inspection

Before starting up the communication system, you must perform a visual inspection of the hardware, cables, and the power supply.

Prerequisites

DANGER:

Risk of electric shock through contact with live wires

Make sure that the communication system is de-energized.

NOTICE:

Always wear an antistatic wristband when handling boards.

The ESD measures for protecting electrostatically sensitive devices must be observed and followed.

The housing cover of the communication system is not mounted.

Step by Step

1) Disconnect all power supply circuits of the communication system.
2) Verify that the SDHC or M.2 SATA SSD card is properly seated. In case of an SDHC card, the write protection of the card must be disabled (switch directed toward metal contacts).
3) Check that all boards are secure.
4) Ensure that all connection cables have been correctly laid and secured. Is there any risk of tripping over a cable, for example?

   If required, make sure that the connection cables are properly installed.
5) Check that a separate ground wire is connected to the communication system's ground terminal. (Only applicable for systems with OCCSB mainboard.)

   If required, ground the communication system using a separate ground wire (see How to Provide Protective Grounding for OpenScape Business X1 on page 27)
6) Check whether the nominal voltage of the mains power supply corresponds to the nominal voltage of the communication system (type plate).

Next steps

Close the housing cover of the communication system.

4.5.4 How to Close the Communication System

Step by Step

1) If you needed access to the mainboard, you must first attach the middle frame and the middle housing cover. To do this, proceed as follows:
   a) Lock the middle frame back into its brackets.
   b) Slide the right housing cover back and insert the two retaining pins at the top and bottom in the right housing cover.
   c) Lock the middle housing cover in its brackets.
2) Place back the left housing cover and close it.

4.5.5 How to Connect the System to the Mains

Step by Step

Plug the power cord into the socket of the power supply. The communication system boots up.

NOTICE: Leave the system connected to the mains for at least 2 days so that the mainboard battery is adequately charged. If the charge state is insufficient, it is possible that repeated booting of the system could cause the activation period to be blocked due to time manipulation.

---

5 Initial Setup for OpenScape Business X

This chapter describes the initial setup of OpenScape Business X1/X3/X5/X8. The communication system and its components are integrated into an existing infrastructure consisting of a customer LAN and a TDM telephony network. Internet access and the trunk connection are set up and the connected stations are configured.

The initial setup of OpenScape Business X1/X3/X5/X8 (i.e., the communication system) is carried out using the OpenScape Business Assistant administration program (web-based management, also called WBM).

The standard initial setup of commonly used components is described here. The specific installation steps depend on the communication system and the components (e.g., the UC Booster Card) involved. During the initial setup, you may need to choose between multiple options in some places or even skip some configurations entirely. It is also possible that the installation steps described here do not appear in your communication system.

The detailed configurations of features not covered by the standard initial setup are described in subsequent chapters.

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

The most important installation steps are as follows:

- IP addresses and DHCP settings
- Country and Time Settings
- System Phone Numbers and Networking
- ISDN Configuration
- Internet access
- Internet telephony
- Station configuration
- Licensing
- Data backup

5.1 Prerequisites for the Initial installation

Meeting the prerequisites for the initial installation ensures the proper operation of the communication system.

General

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

- The infrastructure (LAN, TDM telephony network) is available and usable.
- The hardware is installed and connected properly.
- One LAN port each is required to integrate the mainboard and the UC Booster Card in the customer LAN.
- The communication system has not yet been connected to the LAN.
- If the UC Booster Card is used, it should be inserted prior to the initial installation.
- Internet access is available through an Internet Service Provider.

- An ISDN S_0 or ISDN Primary Rate Interface is required for using ISDN outside lines.
- A CAS trunk connection is required for using a CAS outside line.
- An analog trunk connection is required for using an analog outside line.
- An IP address scheme exists and is known (see *Administrator Documentation, Initial Installation of X3/X5/X8*).
- A dial plan (also called a numbering plan) is present and known (see *Administrator Documentation, Initial Installation of X3/X5/X8*).

Admin PC

The following prerequisites must be fulfilled for the Administration PC (Admin PC) that is used for initially setting up the system and for the subsequent administration of the communication system:

- Network interface:

  The admin PC requires an available LAN port.
- Operating system:

  Configuring the communication system with the Manager E is only possible on a Windows operating system (Windows XP and later).

  WBM configuration, however, is browser-based and therefore platform-independent.
- Web browser:

  The following web browsers are supported:

  – Microsoft Internet Explorer Version 10 and later.
  – Microsoft Edge
  – Mozilla Firefox Version 17 and later.
  – 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 setting up the system.
- Java:

  Oracle Java 8 or higher or alternatively OpenJDK 8 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.

5.2 Components

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

The installation example includes the following components:

- OpenScape Business X

  The communication system is integrated in the existing customer LAN via the LAN interface.
- Admin PC

  The admin PC is also connected to the communication system via a LAN interface.

- IP stations (IP clients)

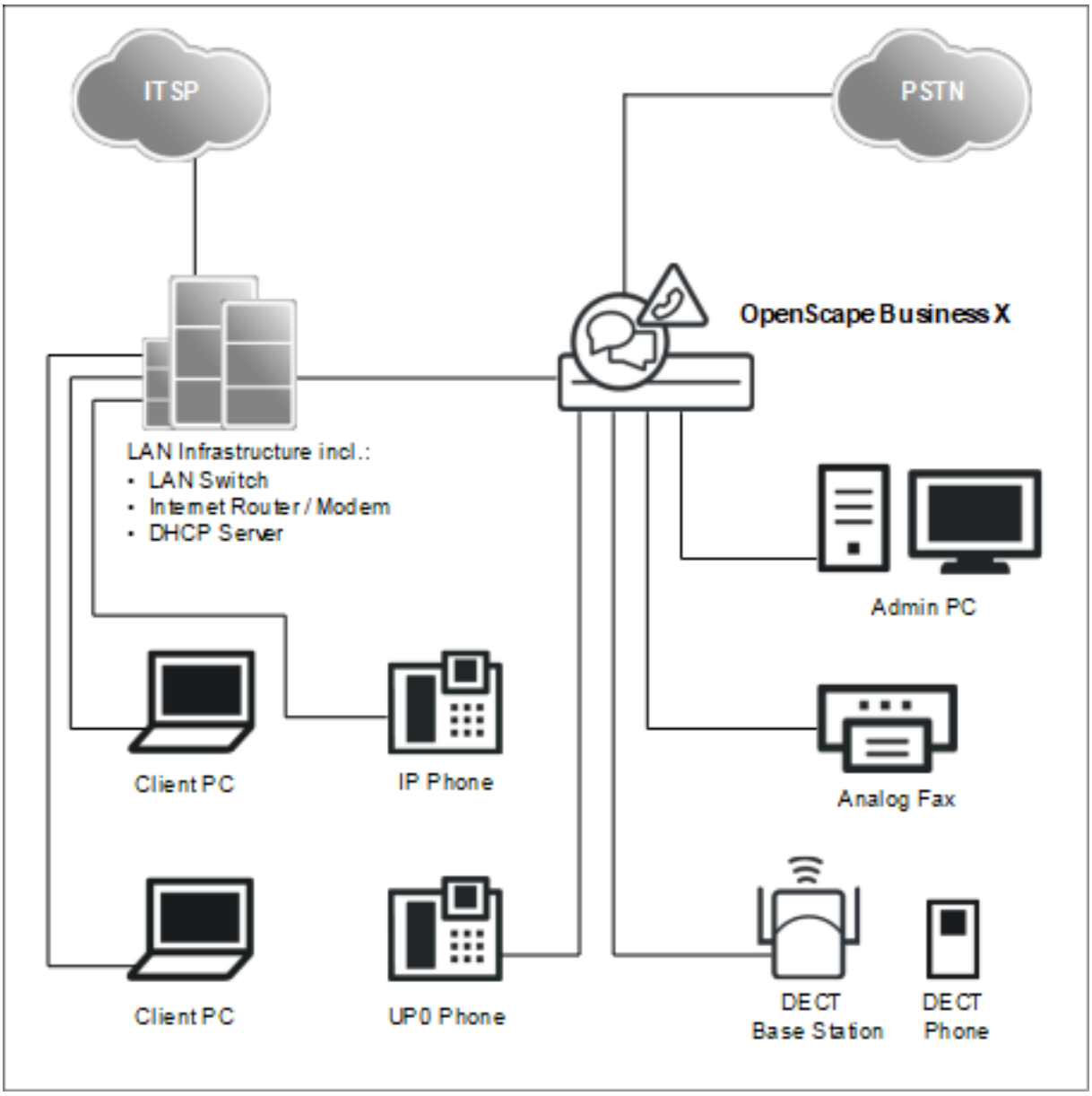
  The IP stations (IP system phones, client PCs, WLAN Access Points, etc.) are integrated in the LAN via one or more switches.
- UP0 stations

  UP0 stations (e.g., OpenStage 60 T TDM system telephones) are connected directly to the communication system.
- Analog stations

  Analog stations (e.g., analog fax devices) are connected directly to the communication system.
- DECT stations

  DECT stations are logged on to the communication system via a base station.

The IP clients receive their IP addresses dynamically from an internal or external DHCP server (e.g., an Internet router).



5.3 Dial Plan

A dial plan is a list of all phone numbers available in the communication system. It includes, among other things, the internal call numbers, DID numbers and group call 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	**X1**	X3/X5/X8
Internal station numbers	11-30	100-742
User direct inward dialing numbers	11-30	100-742
Trunk station number	700-703	from 7801 onward
Seizure codes (external codes): Trk. Grp 1 (trunk: ISDN, analog) Rte. 8 (UC Suite) Trk. Grp 12-15 (trunk: ITSP) Rte. 16 (Networking)	 0 = World / 9 = USA - not preset not preset	 0 = World / 9 = USA 851 855-858 859
Call number for remote access	not preset	not preset
Call number for voicemail UC Smart UC Suite	351 -	351 not preset

Individual Dial Plan

An individual dial plan can be imported via an XML file during 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** > **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.

5.4 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, the communication system, 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 `192.168.1." - x`:

IP address range	Clients
192.168.1.1 to **192.168.1.19**	Clients with a fixed IP address:
192.168.1.1	Internet router (gateway)
192.168.1.2	Communication system
192.168.1.3	Application Board (optional)
192.168.1.10	E-mail server
192.168.1.50 to **192.168.1.254**	Client PCs & IP phones, also the IP address range of the DHCP server; IP addresses are assigned automatically to the clients

The following IP address ranges are internally reserved and must not be used:

Connected IP address ranges	Description
10.0.0.1; 10.0.0.2	Reserved for the license server
10.186.237.65; 10.186.237.66	Reserved for remote ISDN
192.168.3.2	Internal IP address of the communication system
192.168.2.1	IP address of the LAN3 port (Admin port)

This list can also be found in the WBM under **Service Center** > **Diagnostics** > **Status** > **Overview of IP Addresses**.

Expanding the netmask when using the default network segment

Both the internal IP address of the communication system and the IP address of the LAN3 port (Admin port) must not be in the same network segment as the IP address of the communication system.

Default network segment configuration:

- 192.168.1.2: IP address of the communication system
- 255.255.255.0: Netmask
- 192.168.3.2: Internal IP address of the communication system
- 192.168.2.1: IP address of the LAN3 port (Admin port)

If the netmask when using the default network segment of 255.255.255.0 was expanded to 255.255.0.0, for example, then the above IP addresses need to be changed:

Example of a modified configuration:

- 192.168.1.2: IP address of the communication system
- 255.255.**0**.0: Netmask

- 192.**169**.3.2: Internal IP address of the communication system

  The change is made via **Expert mode** > **Telephony** > **Payload** > **HW Modules** > **Edit DSP Settings**
- 192.**170**.2.1: IP address of the LAN3 port (Admin port)

  The change is made via **Expert mode** > **Telephony** > **Network Interfaces** > **Mainboard** > **LAN 3 (Admin)**

5.5 Initial Startup

Initial startup includes starting up the communication system, connecting and configuring the admin PC and starting the OpenScape Business Assistant (WBM) administration program for the first time.

The initial startup of the communication system must be performed prior to integrating the communication system into the internal LAN. Problems can occur if the pre-configured IP address of the communication system already exists in the internal LAN and/or if a DHCP server is already in use. In such cases, the IP address of the communication system must first be reconfigured and/or the DHCP server of the communication system must be deactivated. Only then can the communication system be integrated into the internal LAN.

NOTICE: Prior to initial startup, please follow the instructions on data protection and data security.

DANGER: OpenScape Business X8 may only be powered up if all system boxes are sealed at the rear with the connection and filler panels provided.

DANGER: OpenScape Business X5 must not be powered on unless the housing front is closed. Always use dummy panels (C39165-A7027-B115) to cover slots that are not equipped with boards.

DANGER: The OpenScape Business X1 must only be switched on when the housing is closed.

Connecting the admin PC

To configure the communication system, the admin PC is directly connected to the "LAN" interface of the communication system. The communication system is then configured to obtain its IP address from the internal DHCP server of the communication system. After successful installation, the admin PC can be integrated into the internal LAN without any further configuration changes.

5.5.1 How to Restart the Communication System

Prerequisites

The hardware was correctly installed (see *OpenScape Business Installation Guide*).

The memory card (with the system software) was inserted.

The communication system has not been integrated into the customer LAN yet.

Step by Step

Connect the communication system to the power supply.

WARNING:

Risk of electric shock through contact with live wires

Make sure that the communication system (and for OpenScape Business X8, each system box) is grounded by a separate ground wire (see *OpenScape Business Installation Guide*).

The communication system is now started up, During this process, the system LEDs light up in different colors and sequences (see the *OpenScape Business Installation Guide* for details). During startup, the communication system must not be disconnected from the power supply.

After completion of the startup, the "Run" LED on the mainboard flashes green at 1Hz (0.5 sec on / 0.5 sec off).

5.5.2 How to Connect the Admin PC to the Communication System

Prerequisites

The communication system is ready for use.

Step by Step

1) Start the admin PC.

2) Check whether a dynamic IP address can be assigned to the PC. If not, you will have to reconfigure the admin PC. To do this you must have Administrator rights.

NOTICE: The IP settings described here apply to Windows 7. For more detailed information on the configuration for other

Windows operating systems, please refer to the appropriate operating system instructions.

a) Select **Start** > **Control Panel**, double-click on **Network and Internet** and then click **Network and Sharing Center**.
b) Click on **LAN connection** for the appropriate active network and then click **Properties**.
c) On the **Networking** tab, use the left mouse button to select the **Internet Protocol Version 4(TCP/IPv4)** entry and then click on **Properties**.
d) Click on the **General** and ensure that the radio button **Obtain an IP address automatically** is enabled. If it is not, then activate it.
e) Close all open windows with **OK**.

3) Connect the just configured LAN port of the admin PC to the LAN port "LAN" of the communication system using a LAN cable. The admin PC is assigned a dynamic IP address via this interface.

5.5.3 How to Start the WBM

Prerequisites

The communication system is ready for use. The "Run" LED on the mainboard flashes green at 1Hz (0.5 sec on / 0.5 sec off).

The admin PC and the communication system can communicate with one another over the LAN.

Step by Step

1) Start the web browser on the admin PC and open the login page of the OpenScape Business Assistant (WBM) at the following address:

`https://192.168.1.2`

NOTICE: If the WBM cannot be started, check the LAN connection and repeat the call. If it still cannot be started, check whether the IP address has been blocked by your PC's internal firewall. More detailed information can be found in the documentation of your firewall

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 OpenScape Business Assistant (WBM) at the following address:

      `https://192.168.1.2`
   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 OpenScape Business Assistant (WBM) at the following address:

      `https://192.168.1.2`
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.

   NOTICE: If you go to the **Password** field 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) The following steps are only required once when first logging on to the WBM:
   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` und `CapsLock` keys. The password is displayed as a string of asterisks (*).

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

c) Click **Login**.
d) Select the current date and enter the correct time.
e) Click **OK & Next**. You are automatically logged out of the WBM.
f) In the field under **Login**, enter the default user name `administrator@system` for access as an administrator.

> **NOTICE:** If you go to the **Password** field after entering `administrator`, `@system` will be added automatically.

g) In the second field under **Login**, enter your new password for access as an administrator.
h) Click **Login**. The home page of the WBM appears.

Next steps

Start the initial installation.

5.6 Integration into the Customer LAN

The WBM wizard **Initial Installation** is used for integration into the customer LAN. This wizard guides you through the basic settings for integrating the communication system into the existing LAN.

5.6.1 How to Start the Initial Installation Wizard

Prerequisites

The WBM has been started.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click on **Edit** to start the **Initial Installation** wizard.

> **NOTICE:** 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.

5.6.2 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) Edit IP addresses (if required)

By default, the communication system is assigned an IP address and a subnet mask. You may need to adjust the IP address and/or subnet mask to your own IP address range.

In addition, you can specify the IP address of your default router, e.g., the IP address of the Internet router.

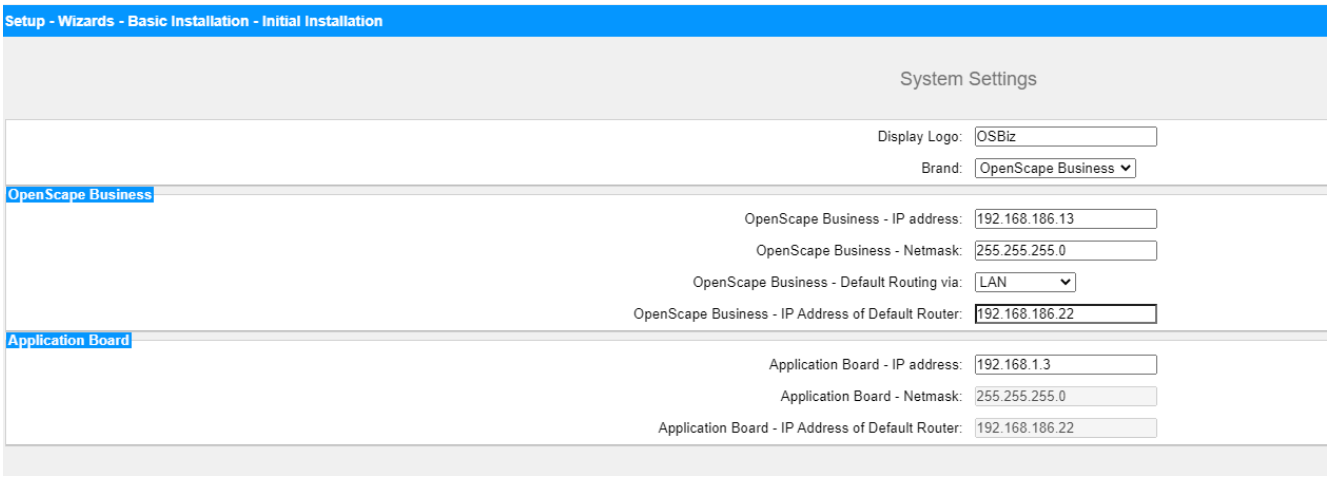
The Application Board (UC Booster Card) also requires an IP address. You can assign an IP address from your IP address range regardless of whether or not the board is installed.

If the netmask is to be expanded, e.g., from 255.255.**255**.0 to 255.255.**0**.0, both the internal IP address of the communication system and the IP address of the LAN3 port (Admin port) must be changed because they are not allowed to be in the same network segment as the IP address of the communication system (see also *IP Address Scheme*).

5.6.2.1 How to Set the Display Logo and the Product Name

Prerequisites

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



Step by Step

1) In the **Display Logo** field, enter a text of your choice (e.g., OpenScape Biz). 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

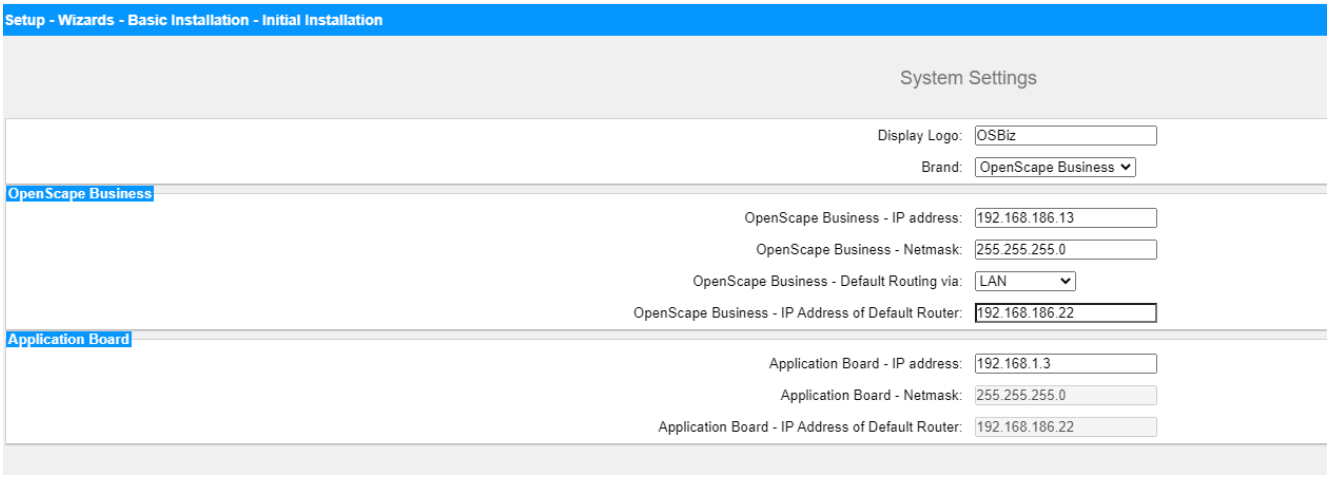
Edit IP addresses (if required) or configure DHCP.

5.6.2.2 How to Specify the IP Addresses (Optional)

Prerequisites

You know the IP address range of your internal network.

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



Step by Step

1) Specify the IP address of the communication system:
   a) In the field **OpenScape Business - IP address**, enter an IP address that lies within the IP address range of your internal network (e.g., internal network: `192.168.1.x`, OpenScape Business: `192.168.1.2`.

      NOTICE: The IP address for OpenScape Business must not be assigned to any other existing network client, since this would result in an IP address conflict.

   b) Enter the subnet mask of your internal network (e.g., `255.255.255.0`) in the **OpenScape Business - Subnet Mask** field.
2) Specify the IP address of the default router:
   a) In the **OpenScape Business - Default Routing via** field, select the entry **LAN**.
   b) Enter the IP address of your default router in the **OpenScape Business - IP Address of Default Router** field (e.g., internal network: `192.168.1.x`, Internet router as default router: `192.168.1.1`).
3) Specify the IP address of the UC Booster Card (required if installed):
4) Click on **OK & Next**.

Next steps

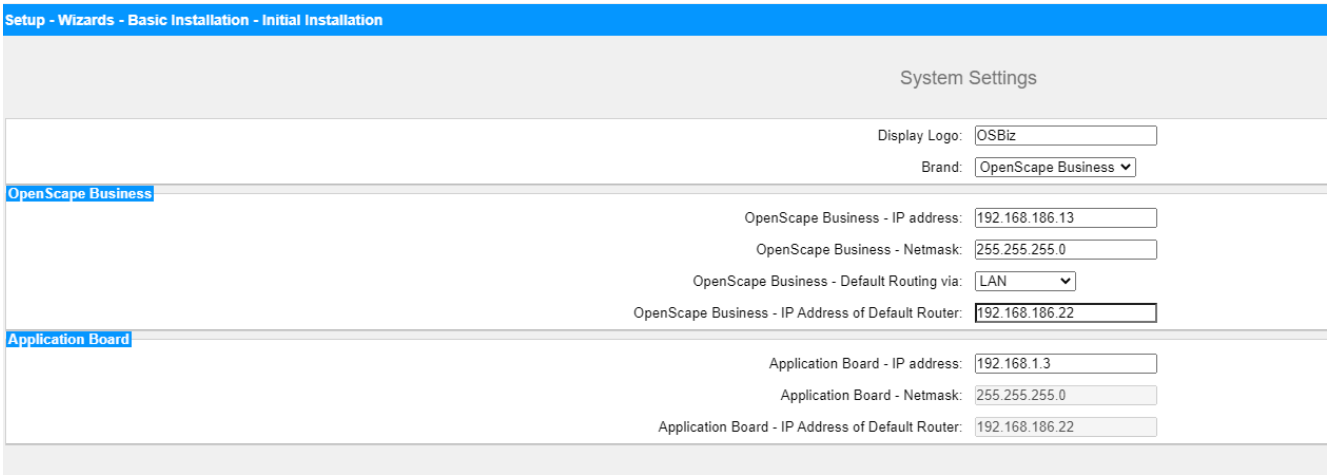
Configure DHCP.

5.6.2.3 How to Specify the Device Name

Prerequisites

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

System is in DTAG mode.



Step by Step

1) Check the **Automatic RSP.servicelink registration** checkbox:

   Device Name field is editable.
2) Specify the **Device Name**.

   By selecting the Automatic RSP.servicelink registration, system will try automatically every 10 minutes to register and connect to RSP servers using the provided Device Name.
3) Click on **OK & Next.**

Next steps

Configure DHCP.

5.6.3 DHCP Settings

In the window **DHCP global settings** enable and configure or disable the internal DHCP server of the communication system.

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

The DHCP server can be an external DHCP server (e.g., the DHCP server of the Internet router) or the internal DHCP Server of the Linux server integrated into the communication system.

Either the integrated DLI of the communication system or an external DLS server can be used for automatically updating the software of the IP system phones (*Administrator Documentation, Deployment Service (DLS and DLI)*).

The IP address of the integrated DLI or the external DLS server must be known to the DHCP server.

You have the following options:

- Enable and configure the internal DHCP server

  If the internal DHCP server of the communication system is used, an external DHCP server (e.g., the DHCP server of the Internet router) must be deactivated. The settings of the internal DHCP server may have to be adapted to the customer LAN. If the internal DHCP server and the internal DLI are used, the system phones are updated automatically. If an external DLS server is used, its IP address must be entered in the internal DHCP server using Expert mode (*Administrator Documentation, Deployment Service (DLS and DLI)*).
- Disable the internal DHCP server

  If an external DHCP server is used, the internal DHCP server of the communication system must be disabled. For IP system phones to be automatically supplied with the latest phone software, network-specific data (such as the IP address of the internal DLI or the external DLS server) must be specified on the external DHCP server.

NOTICE: Not all external DHCP servers support the entry of network-specific data! In this case, the data must be entered manually on all IP system phones.

5.6.3.1 How to Disable the Internal DHCP Server

Prerequisites

An external DHCP server (e.g., the DHCP server of the Internet router) is enabled in the internal network.

You are in the **DHCP Global Settings** window.

Step by Step

1) Clear the **Enable DHCP Server** check box.

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

Next steps

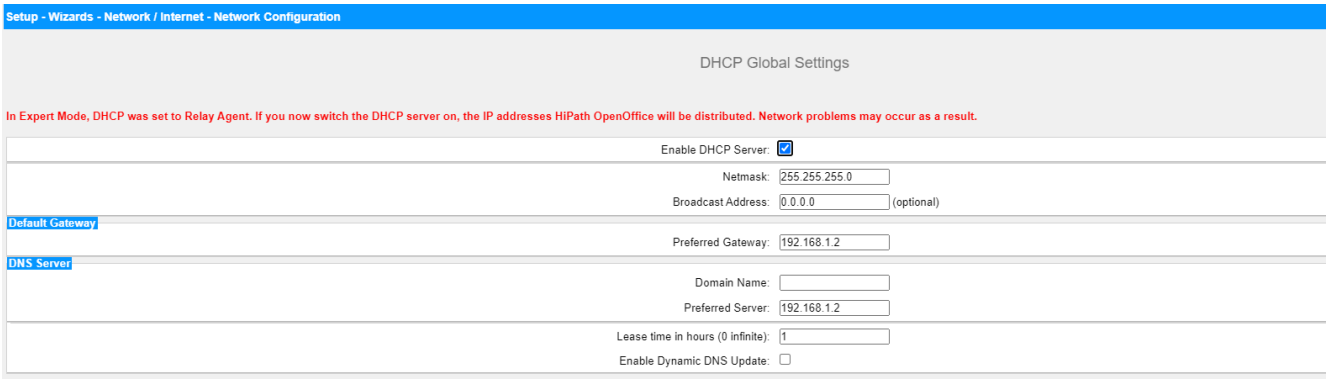
Configure country and time settings.

5.6.3.2 How to Enable and Configure the Internal DHCP Server

Prerequisites

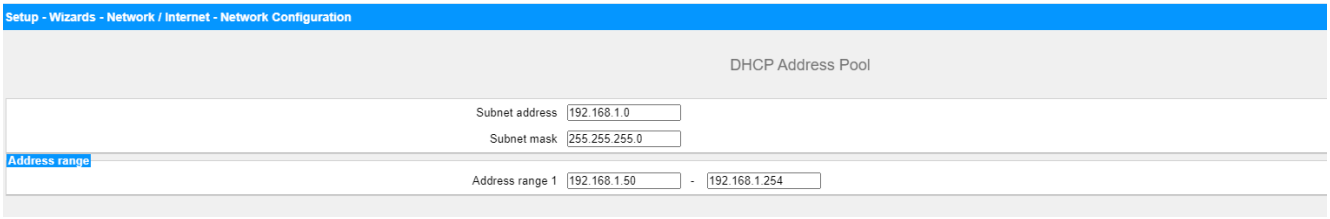
The external DHCP server (e.g., the DHCP server of the Internet router) has been disabled in the internal network.

You are in the **DHCP Global Settings** window.



Step by Step

1) Leave the **Enable DHCP Server** check box enabled.
2) Go to the **Netmask** field and adjust the subnet mask to your IP address range (for example, `255.255.255.0`).
3) In the field **Preferred Gateway**, enter the IP address of the Internet router (e.g., `192.168.1.1`).
4) In the field **Preferred Server**, enter the IP address of the DNS server (e.g., the IP address of the Internet router, `192.168.1.1`.
5) Click on **OK & Next**. The **DHCP Address Pool** window appears.



6) Specify the values for **Subnet address**, **Netmask** and **Address range 1** in order to define the IP address range to be managed by the internal DHCP server.

   If the internal network uses static IP addresses (e.g., for a printer server), the IP address range (DHCP address pool) must be selected so that the fixed IP addresses are not included within this range.

   Example:

   Internet router: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   UC Booster Card: `192.168.1.3`

   Subnet address: `192.168.1.0`

   Subnet mask: `255.255.255.0`

   Printer Server: `192.168.1.10`

   DHCP address pool: `192.168.1.50` to `192.168.1.254`
7) Click on **OK & Next**.

Next steps

Configure country and time settings.

5.6.4 Country and Time Settings

In the **Basic Configuration** window, select your country and the language for the event logs and set the date and time. If you are using the integrated Cordless solution, enter the system-wide DECT system ID here.

Proceed as follows:

1) 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.

2) Enter the DECT system identification (only for integrated Cordless solution)

If you are using the integrated Cordless solution, enter the system-wide DECT system ID here.

3) Setting Date and Time

- How to Set the Date and Time Manually

  The communication system and the stations (IP phones, TDM phones, client PCs) should have a uniform time base (date and time). If no SNTP server has been specified for time synchronization, the date and time can also be entered manually.

  NOTICE: The date and time are also updated when a connection is set up via an ISDN trunk.

- How to Obtain the Date and Time from an SNTP Server

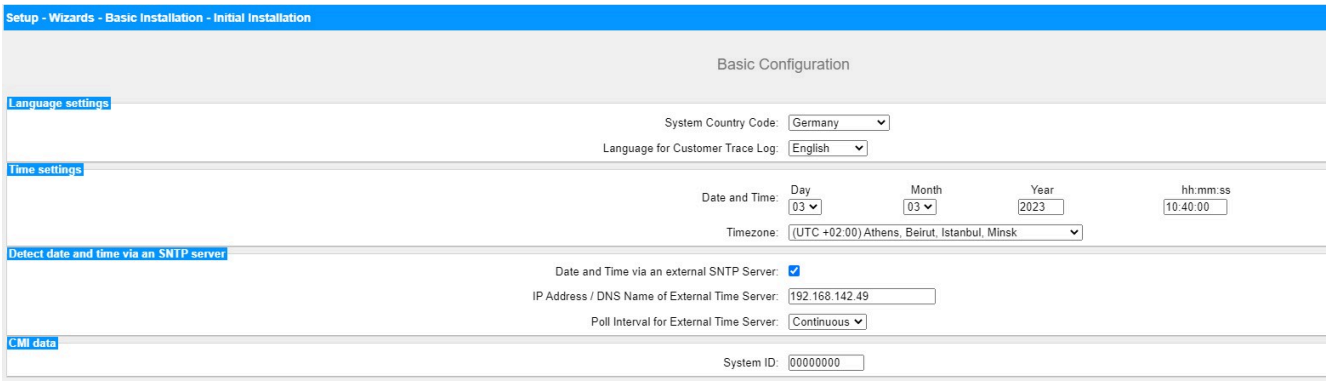
  The communication system and IP stations (IP phones, client PCs) should have a uniform time base (date and time). This time base can be provided by an SNTP server. The SNTP server can be located on the internal network or the Internet.

The IP phones receive the date and time automatically from the communication system. The client PCs on which the UC clients run must be set so that they are synchronized with the communication system (see the operating system instructions for the client PCs).

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

Prerequisites

You are in the **Basic Configuration** window.



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

Enter the DECT system identification (only for integrated Cordless solution)

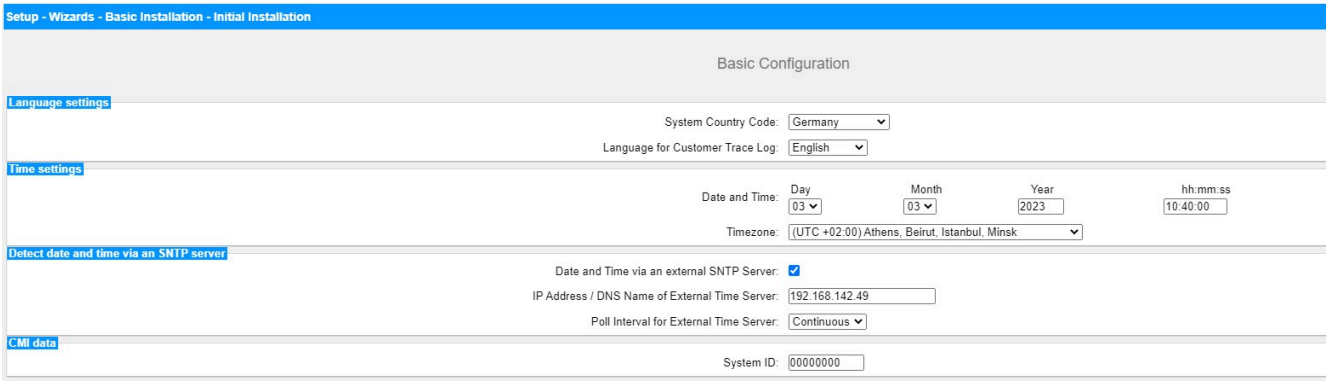
or

Set the date and time manually or obtain the date and time from an SNTP server.

5.6.4.2 How to Enter the DECT System ID

Prerequisites

You are in the **Basic Configuration** window.



Step by Step

In the **CMI data** area under **System ID**, enter the 8-digit hexadecimal DECT system ID that you received on purchasing your integrated Cordless solution.

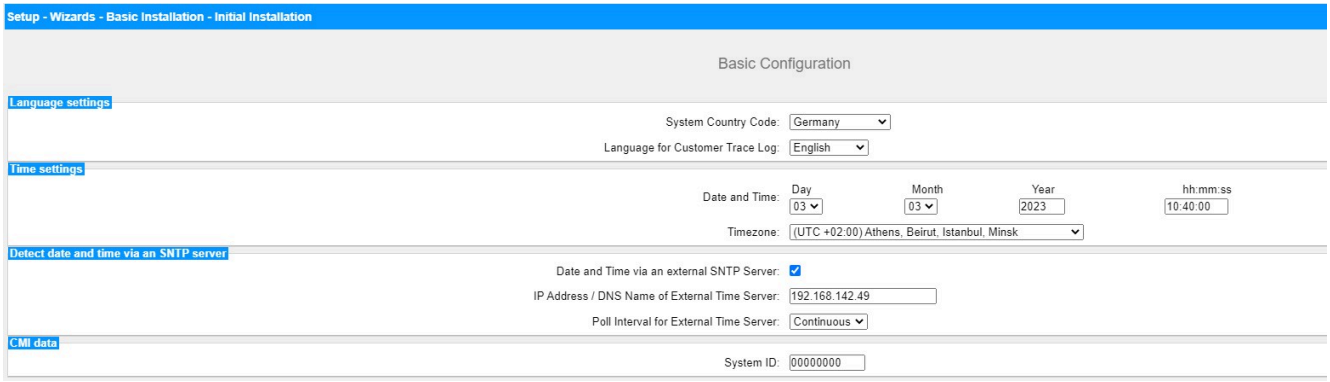
Next steps

Set the date and time manually or obtain the date and time from an SNTP server.

5.6.4.3 How to Set the Date and Time Manually

Prerequisites

You are in the **Basic Configuration** window.



Step by Step

1) Enter the current values for **Date and Time**.
2) Select the desired time zone in the **Timezone** field.
3) Click on **OK & Next**.

NOTICE: In case the Timezone setting is changed, then at the last step of Initial Wizard **the system will be restarted**.

If Timezone setting remain untouched then system will not be restarted.

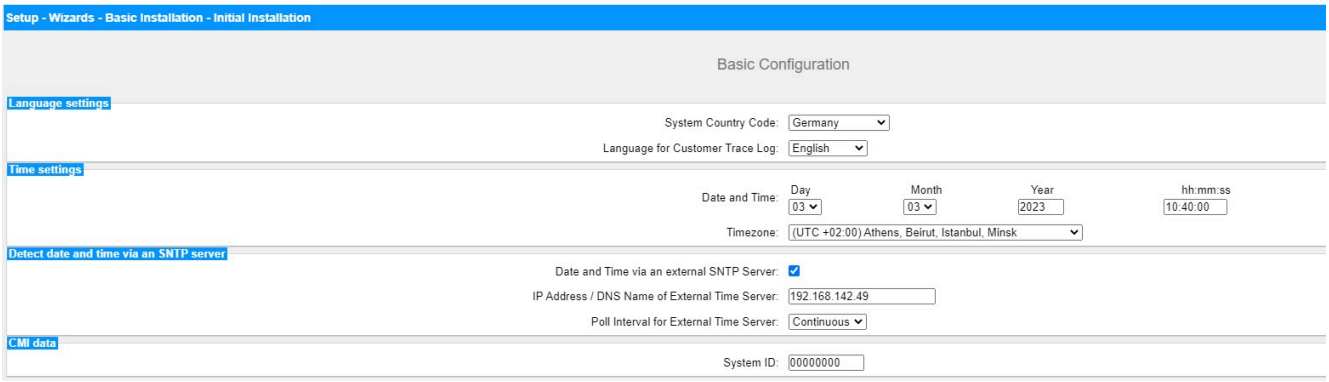
Next steps

Specify UC solution.

5.6.4.4 How to Obtain the Date and Time from an SNTP Server

Prerequisites

You are in the **Basic Configuration** window.



Step by Step

1) Select the **Date and Time via an external SNTP Server** check box.
2) Enter the IP address or the DNS name of the SNTP server (e.g., `0.de.pool.ntp.org`) in the **IP Address / DNS Name of External Time Server** field).
3) From the drop-down list **Poll Interval for External Time Server**, select after how many hours the Date and Time should be synchronized by the SNTP Server (recommended value: `4 h`).
4) Click on **OK & Next**.

Next steps

Specify UC solution.

5.6.5 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 on the OpenScape Business X mainboard.
- **Package with UC Suite**

  The UC solution UC Suite is integrated on the additional internally pluggable "UC Booster Card".
- **Package with UC Suite on OSBiz UC Booster Server**

  The UC solution UC Smart is integrated on the external Linux server "OpenScape Business UC Booster Server".
- **Package with UC Suite on OSBiz UC Booster Server**

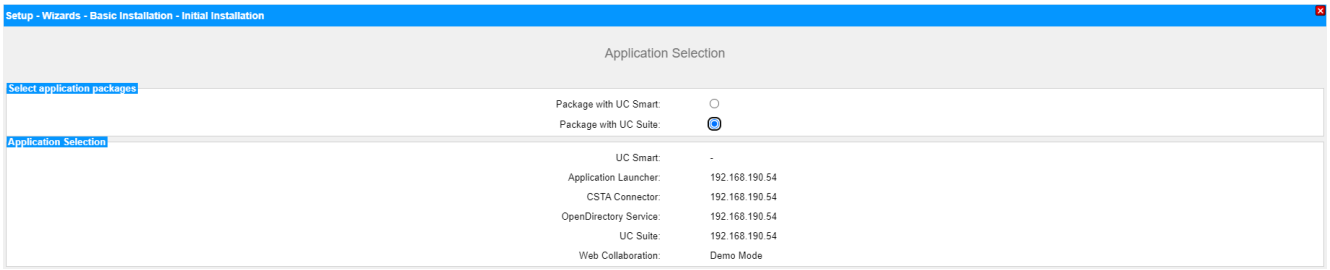
  The UC solution UC Suite is integrated on the external Linux server "OpenScape Business UC Booster Server".

5.6.5.1 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.



Step by Step

1) If you are using the UC solution UC Smart without a UC Booster Server, click **Package with UC Smart**.
2) If you are using the UC solution UC Smart with the UC Booster Server, click on **Package with UC Smart on OSBiz UC Booster Server**. In addition, enter the IP address of the external Linux server "OpenScape Business UC Booster Server" in the **IP address of OSBiz UC Booster Server** field.
3) If you want to use the UC solution UC Suite with the UC Booster Card, click on **Package with UC Suite**.
4) If you are using the UC solution UC Suite with the UC Booster Server, click on **Package with UC Suite on OSBiz UC Booster Server**. In addition, enter the IP address of the external Linux server "OpenScape Business UC Booster Server" in the **IP address of OSBiz UC Booster Server** field.
5) Click on **OK & Next**.
6) The **Initial installation** wizard is closed. Click **Finish**.
7) Exit the WBM by right-clicking the **Logout** link on the top right of the screen and then close the window.

NOTICE: If IP addresses or DHCP server settings have been changed, the communication system performs a restart. This can take a few minutes.

Next steps

Connect the communication system to the customer LAN.

5.6.6 Connecting the Communication System to the Customer LAN

After a successful initial installation, the communication system is connected to the existing customer LAN.

5.6.6.1 How to Connect the Communication System to the Customer LAN

Prerequisites

The communication system is ready for use.

Step by Step

1) Remove the LAN cable of the admin PC from the central LAN port "LAN" and integrate the admin PC in the customer's LAN by connecting it to a switch, for example.
2) Connect a LAN cable to the middle "LAN" port of the communication system.
3) Integrate the communication system via this LAN cable in the customer LAN by connecting it to a switch, for example.
4) If a UC Booster Card (Application Board) is plugged in, connect another LAN cable to the "LAN2" port of the UC Booster Card (right/lower of the two LAN interfaces) and integrate the UC Booster Card via this LAN cable in the customer LAN by connecting it to a switch, for example.

Next steps

Start the basic configuration.

5.7 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.

5.7.1 How to Start the Basic Installation Wizard

Prerequisites

The **Initial installation** has been completed.

The communication system is integrated in the customer LAN

The communication system is ready for use. The "Run" LED on the mainboard flashes green at 1Hz (0.5 sec on / 0.5 sec off).

Step by Step

1) Open the WBM login page on the admin PC by entering the following address in your web browser:
   `https://<IP address of OpenScape Business>`
   The default IP address for OpenScape Business is `192.168.1.2`, i.e., `https://192.168.1.2`, for example.
2) In the **User Name** field, enter the default user name `administrator@system` for access as an administrator.
3) Enter the password you defined at initial startup in the **Password** field.
4) Click on **Login**.

5) In the navigation bar, click on **Setup**.
6) 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.

5.7.2 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

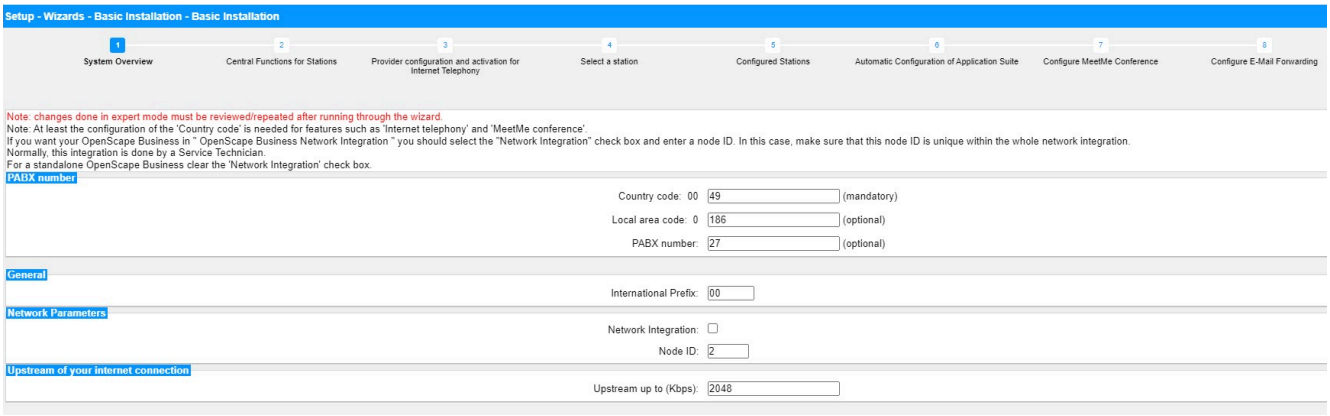
   If OpenScape Business is to be networked with other OpenScape Business systems, networking must be enabled, and OpenScape Business must be assigned a node ID. Every OpenScape Business must have a unique node ID in the network.

5.7.2.1 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.



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

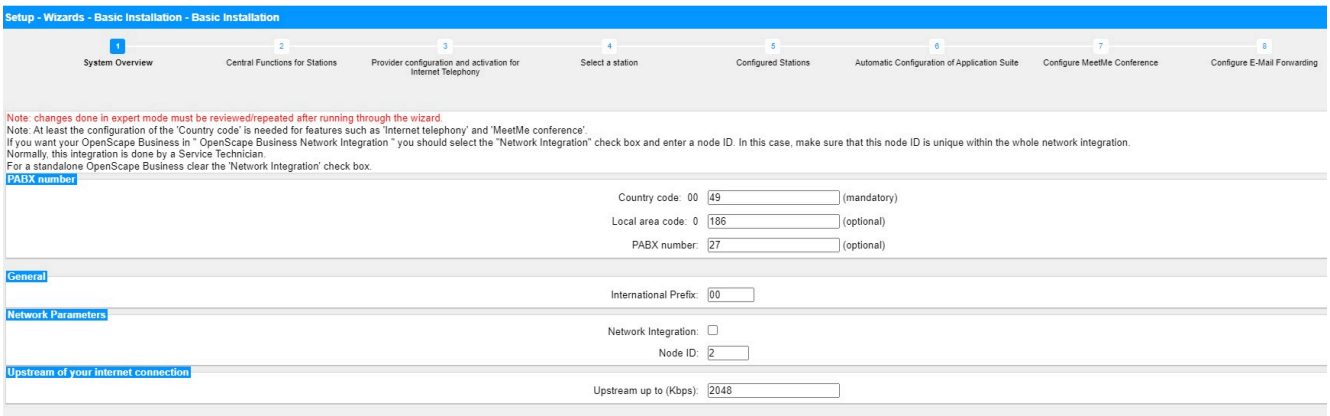
Activate or deactivate networking

5.7.2.2 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.



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.

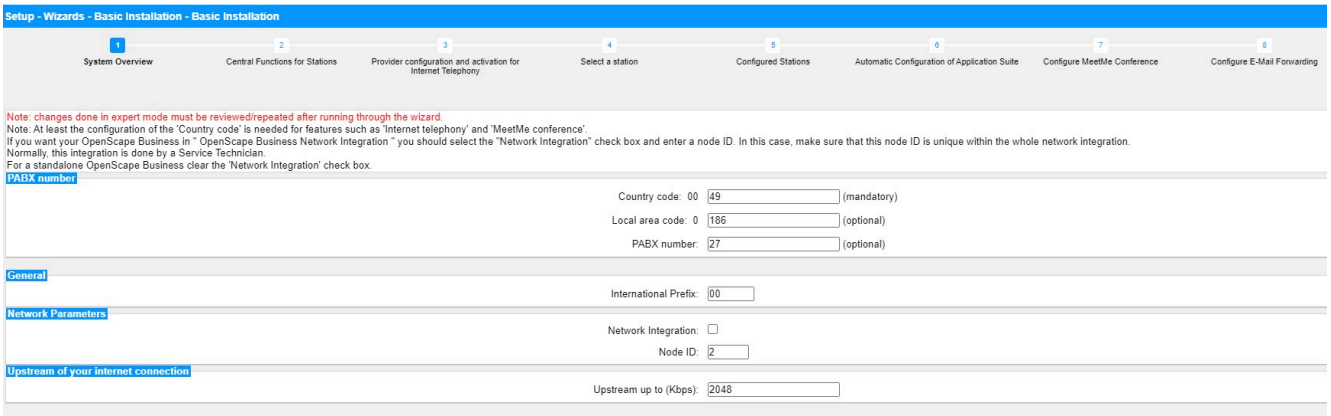
Next steps

Activate or deactivate networking

5.7.2.3 How to Activate or Deactivate Networking

Prerequisites

You are in the **Summary** window.



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.

Next steps

Configure the upstream of your Internet connection.

5.7.3 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.

NOTICE: 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:

  1) Display the station data

  You can have all preconfigured station numbers and station data displayed.

  2) Delete all station numbers (optional)

  If you use an individual dial plan, you must delete all preconfigured station numbers.

  3) 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.

  NOTICE: If the user passes through the **Change preconfigured functional call numbers,** any existing custom configuration done in UC Suite must be reviewed or repeated (e.g., pilot queues)

  ---

  4) 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:

  1) 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.

2) 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.

5.7.3.1 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**.

5.7.3.2 How to Delete all Call Numbers

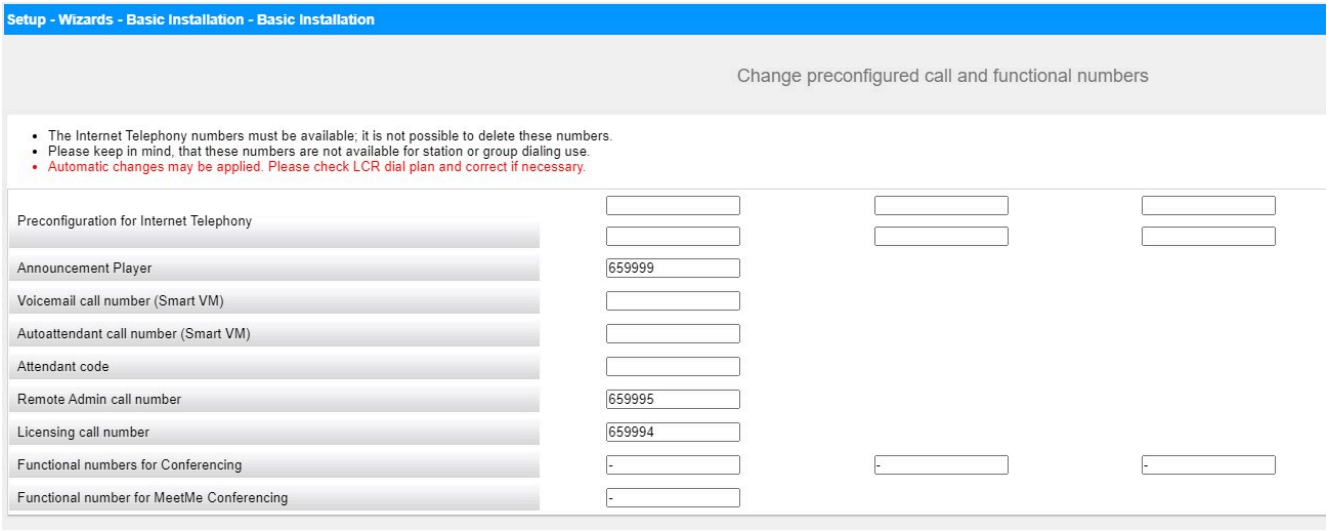
Prerequisites

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.



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**.

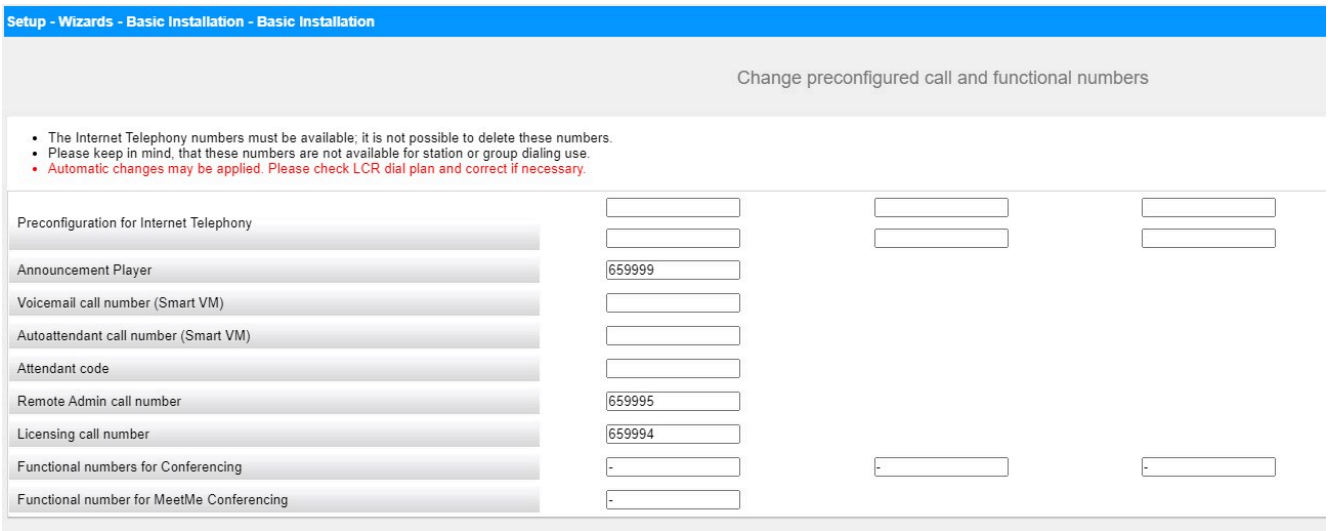
5.7.3.3 How to Adapt Preconfigured Station Numbers for the Individual Dial Plan

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.



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**.

5.7.3.4 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**.

5.7.3.5 How to display Mass data

Prerequisites

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

Step by Step

1) Enable the **Mass Data wizard** button.
2) Click on **Execute function**.
3) In the **Mass Data Wizard** window you can validate the entries of the system, by clicking on **Validate**. There are two types of validation, the Front End Consistency Check and the Back End Consistency Check.
   The green color in validation field indicates only the actions that have been recently validated. The validation of data is not saved, so if the values are changed the user has to validate again the data.
4) During Back End Consistency Check and after the successful validation of data no editing in **Mass Data Wizard** window is possible. After the successful validation **OK&Next** becomes available with Edit restrict mode. If the user clicks on **Back**, Edit mode becomes available but **OK&Next** disappears. When the validation is unsuccessful Edit mode remains intact and **OK&Next** stays hidden.

NOTICE: The user can click on **Back** to re-edit the data and the window returns to Edit mode again.The Edit restrict mode ensures that the user cannot click on OK&Next and submit changes that are not validated.

---

5) When **Mass Data Wizard** is configured successfully click on **Finish**. In the finish page is displayed a sum up with all the changes.

   Fields that are not editable are already filled in with the relevant values obtained by the Database. As a result Copy/paste function will have no effect in data.

   Type field is a selectable drop down menu with editing functionality. However the only options accepted are No Port, System Client, SIP Client, Deskshare User and potentially a predefined value based on the Baugruppe it belongs. If the user tries to enter something else then this will not be accepted and drop down menu will not be disappear persisting in providing a proper entry.

   Another restriction is that some ports are not changeable (for instance ports belonging in an Analog card, type is not changeable and should remain Analog Station).All restrictions apply when the user tries to perform copy paste on top of Type column. If the user tries to paste irrelevant data not compromising with the rules above paste will not be performed at all.

   Copy and paste can be applied on the whole table as well as on specific parts.

   NOTICE: When selecting two following cells, with a numeric value, and you pull down the fields the following columns are not filled in with ascending numbers but they are filled in with a copy of the selected cells.

5.7.4 ISDN Configuration

In the **ISDN Configuration** window, you specify whether ISDN stations are to be connected and whether ISDN is to be used for the trunk connection. The ISDN trunk connection can be set up as an ISDN point-to-point connection and/or an ISDN-point-to-multipoint connection. Depending on the communication system and board used, different S_0 ports are available for this purpose.

You have the following options:

- Enable ISDN configuration:
  1) Configure an ISDN point-to-point connection

     You can set up an ISDN trunk connection as a point-to-point connection with DID numbers.
  2) Configure an ISDN point-to-multipoint connection

     You can set up an ISDN trunk connection as a point-to-multipoint connection with MSN.
  3) Set up a connection for ISDN subscribers (optional)

     One or more S_0 interfaces can be configured as internal S_0 connections in order to connect ISDN stations (ISDN phones or ISDN fax devices). A station license is required for each ISDN station.
- Disable ISDN configuration

  If you do not have an ISDN trunk connection, you must disable the ISDN configuration. All S_0 interfaces automatically configured as internal S_0ports.

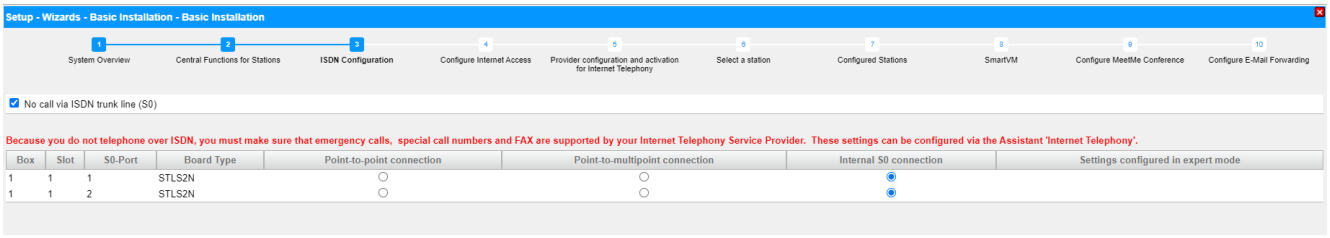
Other options for trunk connections

Instead of setting up an ISDN trunk connection, you can also set up an analog trunk connection or a trunk connection through an Internet Telephony Service Provider (ITSP, SIP provider). Basic installation must be complete before the analog trunk connection can be configured.

5.7.4.1 How to Configure the Connection of ISDN Stations

Prerequisites

You are in the **ISDN Configuration** window.



Step by Step

1) Clear the check box **No call via ISDN trunk line (S0)**.
2) Activate the **Internal S0 connection** radio button for the desired S_0 port.

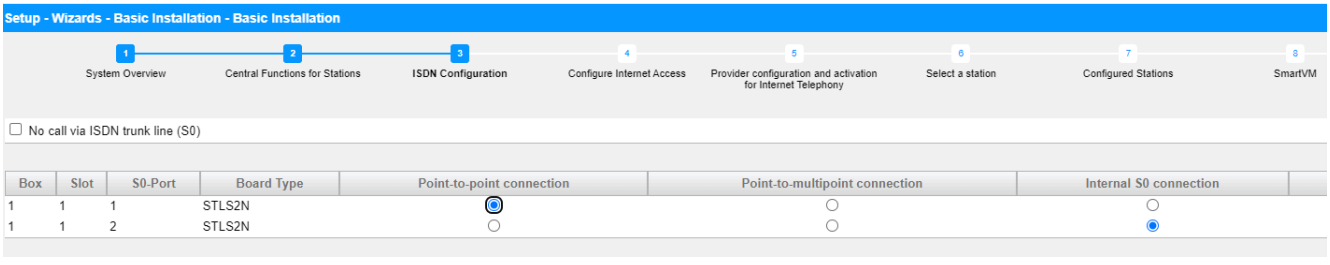
Next steps

Configure ISDN point-to-point connection and/or configure ISDN point-to-multipoint connection.

5.7.4.2 How to Configure the ISDN Point-to-Point Connection

Prerequisites

You are in the **ISDN Configuration** window.



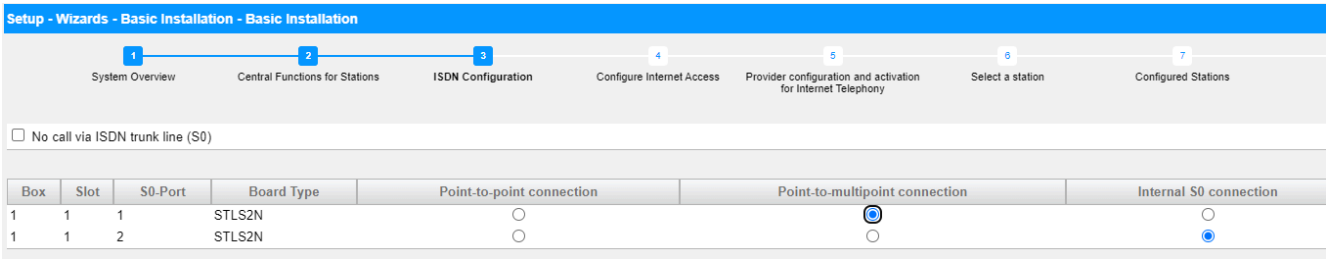
Step by Step

1) To configure the ISDN trunk connection, clear the check box **No call via ISDN trunk line (S0)**.
2) Enable the radio button **Point-to-point connection** for the desired S_0 port.
3) Click on **OK & Next**.

5.7.4.3 How to Configure the ISDN Point-to-Multipoint Connection

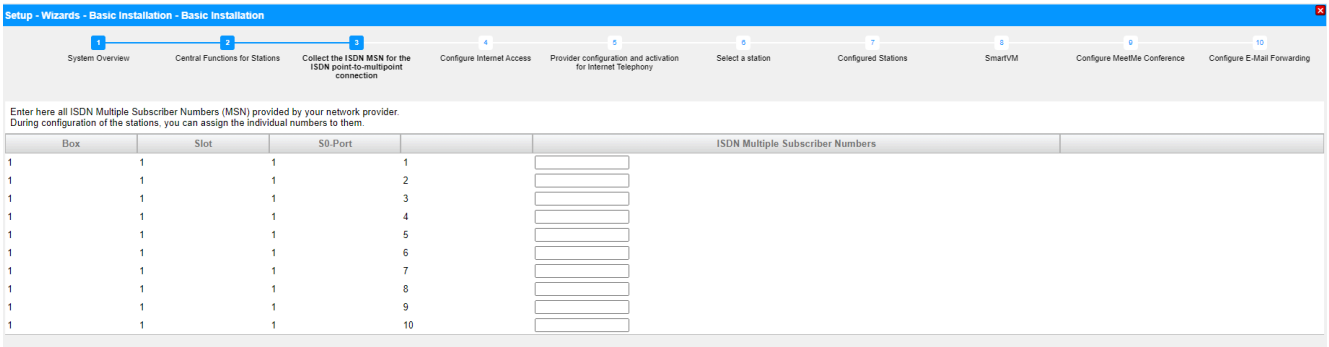
Prerequisites

You are in the **ISDN Configuration** window.



Step by Step

1) To configure the ISDN trunk connection, clear the check box **No call via ISDN trunk line (S0)**.
2) Enable the radio button Point-to-multipoint connection for the desired S**0** port.
3) Click on **OK & Next**.



4) Enter all phone numbers (MSNs) supplied by your provider in the **ISDN multiple subscriber numbers** column. You can enter up to 10 MSNs for each S_0 port. The number of the S_0 connections depends on the communication system and possibly the board being used.
5) Click on **OK & Next**.

5.7.4.4 How to Deactivate the ISDN Configuration

Prerequisites

You are in the **ISDN Configuration** window.

Step by Step

1) Select the **No call via ISDN trunk line (S0)** check box.

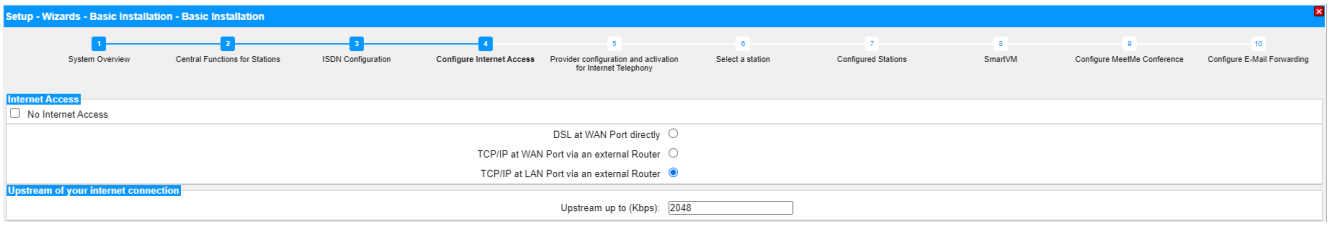
NOTICE: Calls can also be conducted via an Internet Telephony Service Provider; see .

---

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

5.7.5 Internet Access

The **Configure Internet Access** window can be used to configure Internet access.



The configuration of Internet access in the WBM depends on whether the Internet connection has already been set up in an external router or whether it occurs via an Internet modem and thus needs to be set up in the WBM.

Only one of the options listed here may be selected.

- Internet access through an Internet modem (**DSL at WAN port directly**)

  You want to operate the communication system directly at an Internet modem (DSL, cable, UMTS ...). OpenScape Business has the Internet router integrated. Enter the access data of the Internet Service Provider (ISP) directly in the communication system and use the WAN port of the communication system.

You have the following options:

– **Internet access via a preconfigured ISP**
– **Internet access via the standard ISP PPPoE**
– **Internet access via the standard ISP PPTP**

If your ISP is not listed under the preconfigured ISPs, use the default ISP PPPoE or PPTP.

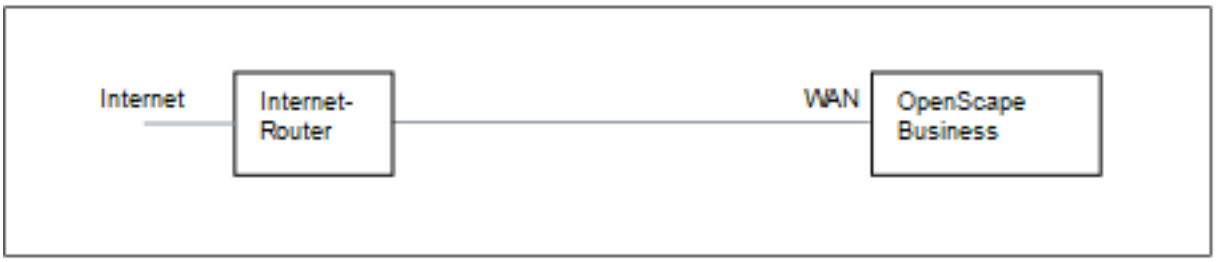
- Internet access via an external Internet router

  You want to operate the communication system at an external Internet router. The Internet Service Provider is already configured in the Internet router.

  You have the following options:

  – **Internet access via an external Internet router at the WAN port**

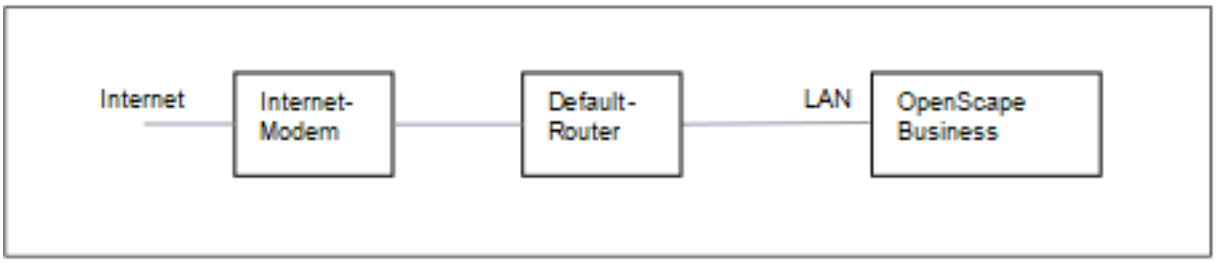
    (**TCP/IP at WAN port via an external router**)



    To do this, you use the WAN port of the communication system. OpenScape Business either knows the Internet router or works as a DHCP client. This option can be used if the Internet router is located in another network segment and has its own DHCP server.

  – **Internet access via an external Internet router at the LAN port**

    (**TCP/IP at LAN port via an external router**)



    To do this, you use the LAN port of the communication system. OpenScape Business knows only the default router and not the underlying infrastructure. To activate the connection to the Internet router, the IP address of the default router and that of the DNS server must be made known to the communication system.

- Deactivate Internet access (default setting)

  You do not want to use the Internet.

5.7.5.1 How to Configure Internet Access via an External Internet Router over the LAN Port

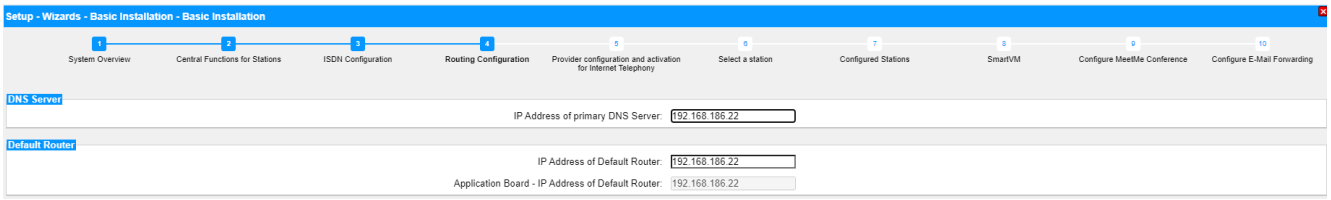
Prerequisites

The communication system must be connected to the customer LAN via the "LAN" interface. The connection must not use the WAN port, since the WAN port will be disabled.

You are in the **Configure Internet Access** window.

Step by Step

1) Disable the **No Internet Access** check box.
2) Activate the radio button **TCP/IP at LAN Port via an external router**, enter the upload speed of your Internet connection in the **Upstream up to (Kbps)** field and click **OK & Next**.



3) Enter the IP address of the local DNS server (e.g., the Internet router) or the Internet DNS server (for Internet telephony, for example) in the **IP address of the preferred DNS server** field.
4) Enter the IP address of the external Internet router in the **IP Address of Default Router** field.
5) Click on **OK & Next**.

5.7.5.2 How to Configure Internet Access via an External Internet Router over the WAN Port

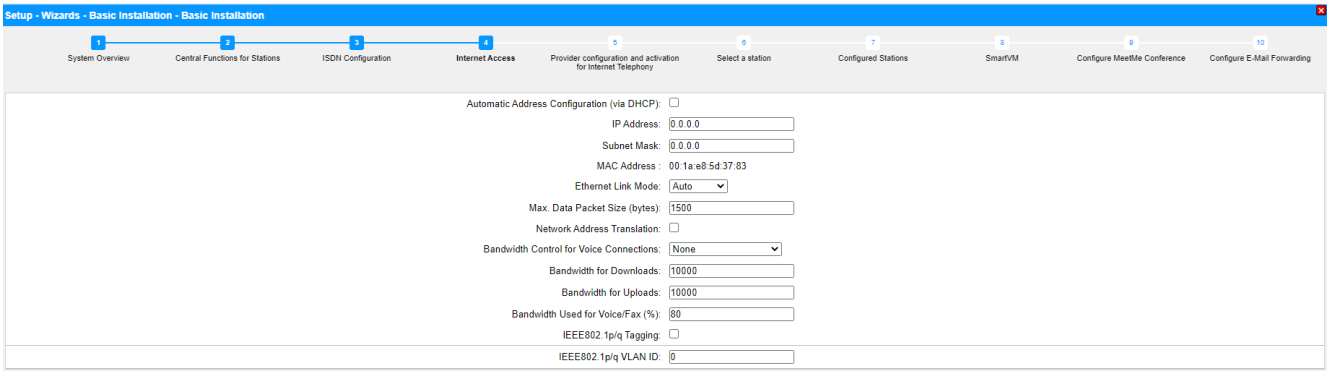
Prerequisites

The communication system must be connected to the LAN segment of the customer LAN in which the Internet router is located via the LAN interface "WAN".

You are in the **Configure Internet Access** window.

Step by Step

1) Disable the **No Internet Access** check box.
2) Activate the radio button **TCP/IP at WAN Port via an external router** and click **OK & Next**.



3) If the network-specific data for the WAN interface are to be obtained from an already active DHCP server:
   a) Select the check box **Automatic Address Configuration (with DHCP)**.
   b) Select the **Accept IP Address of the Default Router** check box if you want this IP address to be used.
   c) Select the check box **Accept IP Address of the DNS Server** if required.
   d) Select the check box **Accept IP Address of the SNTP Server** if required.
4) If a fixed IP address is to be assigned to the WAN interface:
   a) Clear the check box **Automatic Address Configuration (with DHCP)**.
   b) Enter the desired **IP address** and **Netmask** of the WAN interface.
5) Enable the **NAT** check box.
6) If you also want to use Internet Telephony, select the item **Upload only** or **Upload and Download** as needed from the **Bandwidth Control for Voice Connections** drop-down list. If the download bandwidth is high and the upload bandwidth is low, bandwidth control should only be activated for the upload direction to ensure that the download bandwidth reserved for voice transmission is not unnecessarily high.
7) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your Internet Service Provider.
8) Click on **OK & Next**.

5.7.5.3 How to Configure Internet Access via a Preconfigured ISP

Prerequisites

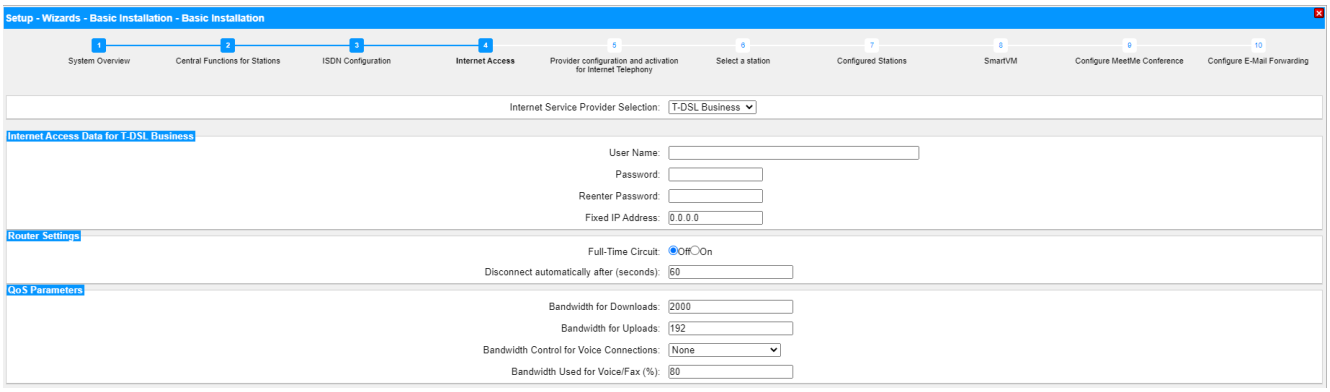
You are in the **Configure Internet Access** window.

Your ISP's Internet access data is available (for example, user account, password, bandwidth for upload and download, etc.).

Optional: The data for a DynDNS account is available to you (name, password, host name, domain name of the DynDNS provider)

Step by Step

1) Disable the **No Internet Access** check box.
2) Activate the radio button **DSL directly at Mainboard WAN Port** and click **OK & Next**.



3) Select your ISP from the **Internet Service Provider Selection** drop-down list.

4) Enter the access data that you received from your ISP in the **Internet Access Data for...** area. The fields in this area ate provider-specific. When entering your data, bear in mind that the input is case-sensitive!

5) Depending on your tariff model, select one of the following two options under **Full-Time Circuit** in the **Router Settings** area:

   - If you have a flat rate tariff model, enable the radio button **On**. In the **Forced Disconnect at (hour:min)** field, enter the time at which the Internet connection is to be interrupted (e.g., 01:30). Make sure that no data is exchanged with the Internet (e.g., software downloads or Internet telephony) during this time.
   - If you have a time-based tariff model, enable the radio button **Off**. In the **Disconnect automatically after (seconds)** field, enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds).

6) Set the following values in the **QoS Parameters** area:

   a) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your ISP.

   b) If you want to use Internet Telephony as well, open the drop-down list **Bandwidth Control for Voice Connections** and select the item **Upload only** or **Upload and Download**, as required. In the field **Bandwidth Used for Voice/Fax (%)**, enter how much bandwidth is to be reserved for voice and fax connections as a percentage value (default value: 80%).

7) Click **OK & Next**. You are taken to the **Configure DynDNS-Account** window.

8) If you want to use a VPN or remote access and do not have a public static IP address, you will need to have already applied for and set up a DynDNS account (at dyndns.org, for example).

   a) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).

   b) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.

      `http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`

   c) Enter the **User name** and the **Password** of your DynDNS account.

   d) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.

   e) Test the DynDNS account with **Connection test**.

   f) After the test succeeds, click **OK**.

   g) Click **OK & Next**.

9) If you have a public static IP address or do not want to use a VPN or remote access, click **No DynDNS**.

10) Click **OK & Next**.

5.7.5.4 How to Configure Internet Access via the Standard ISP PPPoE

Prerequisites

You are in the **Configure Internet Access** window.

The following ISP-specific Internet access data is available to you:

Field	Description	Value from ISP
IP Parameters (only for a fixed IP address)		
Remote IP Address of the PPP Connection	IP address of your ISP's server.	
Local IP Address of the PPP Connection	IP address that was assigned to you by your ISP for Internet access.	
Authentication (via PAP or CHAP). PAP is seldom used, since the authentication is unencrypted.		
PPP User Name	User name that was assigned to you by your ISP for the PPP connection.	
PAP Authentication Mode	Authentication mode for the PPP connection over PAP: **PAP Client**, **PAP Host** or **Not used**.	
PAP Password	Password assigned to you by the ISP for PAP authentication	
CHAP Authentication Mode	Authentication mode for PPP connection via CHAP: **CHAP Client**, **CHAP Host**, **CHAP Client and Host** or **Not used**.	
CHAP Password	Password assigned to you by the ISP for CHAP authentication	
QoS Parameters of Interface		
Bandwidth for Downloads	Value of the full download bandwidth in Kbps provided by the ISP.	
Bandwidth for Uploads	Value of the full upload bandwidth in Kbps provided by the ISP.	

Optional: The data for a DynDNS account is available to you (name, password, host name, domain name of the DynDNS provider)

Step by Step

1) Disable the **No Internet Access** check box.
2) Activate the radio button **DSL at WAN Port directly** and click **OK & Next**.
3) From the **Internet Service Provider Selection** drop-down list, select the standard ISP Type **Provider PPPoE**.
4) The **IP parameters** check box in the **IP Parameters** area should only be enabled if the ISP requires an adjustment of these parameters. In this case, enter the values that you have received from your ISP in the **Remote IP Address of the PPP Connection**, **Local IP Address of the PPP Connection** and **Max. Data Packet Size (bytes)** fields. From the **IP Address Negotiation** drop-down list, select the item **Use configured IP address**.

5) Depending on your tariff model, select one of the following two options under **Full-Time Circuit** in the **Router Settings** area:

- If you have a flat rate tariff model, enable the radio button **On**. In the **Forced Disconnect at (hour:min)** field, enter the time at which the Internet connection is to be interrupted (e.g., 01:30). Make sure that no data is exchanged with the Internet (e.g., software downloads or Internet telephony) during this time.
- If you have a time-based tariff model, enable the radio button **Off**. In the **Disconnect automatically after (seconds)** field, enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds).

6) The settings in the **Authentication** area depend on whether or not the ISP requires authentication via PPP.

- Authentication required by ISP: Make sure that the check box **PPP Authentication** is enabled. Enter the Internet access name of the ISP as the PPP user name. The customary standard is the **CHAP Client** authentication mode.
- Authentication not required by ISP: Make sure that the check box PPP Authentication is disabled.

7) If you want to use NAT, enable the **NAT** check box (enabled by default) in the **Address Translation** area.

8) Set the following values in the **QoS Parameters of Interface** area:

a) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your ISP.

b) If you want to use Internet Telephony as well, open the drop-down list **Bandwidth Control for Voice Connections** and select the item **Upload only** or **Upload and Download**, as required. In the field **Bandwidth Used for Voice/Fax (%)**, enter how much bandwidth is to be reserved for voice and fax connections as a percentage value (default value: 80%).

9) Click **OK & Next**. You are taken to the **Configure DynDNS-Account** window.

10) If you want to use a VPN or remote access and do not have a public static IP address, you will need to have already applied for and set up a DynDNS account (at dyndns.org, for example).

a) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).

b) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.

`http://www.anydns.info/update.php?`
`user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Enter the **User name** and the **Password** of your DynDNS account.

d) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.

e) Test the DynDNS account with **Connection test**.

f) After the test succeeds, click **OK**.
g) Click **OK & Next**.

11) If you have a public static IP address or do not want to use a VPN or remote access, click **No DynDNS**.

12) Click **OK & Next**.

5.7.5.5 How to Configure Internet Access via a Standard ISP PPTP

Prerequisites

You are in the **Configure Internet Access** window.

The following ISP-specific Internet access data is available to you:

Field	Description	Value from ISP
IP Parameters (only for a fixed IP address)		
Remote IP Address of the PPP Connection	IP address of your ISP's server.	
Local IP Address of the PPP Connection	IP address that was assigned to you by your ISP for Internet access.	
PPTP Parameter		
Local IP Address of the Control Connection	IP address that was assigned to you by your ISP for the PPTP connection. The default value is 10.0.0.140.	
Remote IP Address of the Control Connection	IP address of your ISP's server for the PPTP connection. The default value is 10.0.0.138.	
Remote Netmask for the Control Connection	Subnet mask that was assigned to you by your ISP for the PPTP connection. The default value is 255.255.255.248.	
Authentication (via PAP or CHAP). PAP is seldom used, since the authentication is unencrypted.		
PPP User Name	User name that was assigned to you by your ISP for the PPP connection.	
PAP Authentication Mode	Authentication mode for the PPP connection over PAP: **PAP Client**, **PAP Host** or **Not used**.	
PAP Password	Password assigned to you by the ISP for PAP authentication	
CHAP Authentication Mode	Authentication mode for PPP connection via CHAP: **CHAP Client**, **CHAP Host**, **CHAP Client and Host** or **Not used**.	
CHAP Password	Password assigned to you by the ISP for CHAP authentication	
QoS Parameters of Interface		

Field	Description	Value from ISP
Bandwidth for Downloads	Value of the full download bandwidth in Kbps provided by the ISP.	
Bandwidth for Uploads	Value of the full upload bandwidth in Kbps provided by the ISP.	

Optional: The data for a DynDNS account is available to you (name, password, host name, domain name of the DynDNS provider)

Step by Step

1) Disable the **No Internet Access** check box.

2) Activate the radio button **DSL at WAN Port directly** and click **OK & Next**.

3) From the **Internet Service Provider Selection** drop-down list, select the standard ISP Type **Provider PPTP**.

4) The **IP parameters** check box in the **IP Parameters** area should only be enabled if the ISP requires an adjustment of these parameters. In this case, enter the values that you have received from your ISP in the **Remote IP Address of the PPP Connection**, **Local IP Address of the PPP Connection** and **Max. Data Packet Size (bytes)** fields. From the **IP Address Negotiation** drop-down list, select the item **Use configured IP address**.

5) Enter the values that you received from your ISP in the **PPTP Parameter** area.

6) If you have a time-based tariff model, select the **Short Hold** check box. In the **Short Hold Time (sec)** field, enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds).

7) The settings in the **Authentication** area depend on whether or not the ISP requires authentication via PPP.

- Authentication required by ISP: Make sure that the check box **PPP Authentication** is enabled. Enter the Internet access name of the ISP as the PPP user name. Make the PAP and CHAP settings, as assigned to you by your ISP.
- Authentication not required by ISP: Make sure that the check box PPP Authentication is disabled.

8) If you want to use NAT, enable the **NAT** check box (enabled by default) in the **Address Translation** area.

9) Set the following values in the **QoS Parameters of Interface** area:

a) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your ISP.

b) If you want to use Internet Telephony as well, open the drop-down list **Bandwidth Control for Voice Connections** and select the item **Upload only** or **Upload and Download**, as required. In the field **Bandwidth Used for Voice/Fax (%)**, enter how much bandwidth is to be reserved for voice and fax connections as a percentage value (default value: 80%).

10) Click **OK & Next**. You are taken to the **Configure DynDNS-Account** window.

11) If you want to use a VPN or remote access and do not have a public static IP address, you will need to have already applied for and set up a DynDNS account (at dyndns.org, for example).
    a) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).
    b) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.

       `http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
    c) Enter the **User name** and the **Password** of your DynDNS account.
    d) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.
    e) Test the DynDNS account with **Connection test**.
    f) After the test succeeds, click **OK**.
    g) Click **OK & Next**.
12) If you have a public static IP address or do not want to use a VPN or remote access, click **No DynDNS**.
13) Click **OK & Next**.

5.7.5.6 How to Disable Internet Access

Prerequisites

You are in the **Configure Internet Access** window.

Step by Step

1) Leave the **No Internet Access** check box enabled.
2) Click on **OK & Next**.

5.7.6 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, Configuring an ITSP*.
- **Disable Internet telephony**

  You can disable Internet telephony.

NOTICE: 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).

5.7.6.1 How to Configure a Predefined ITSP

Prerequisites

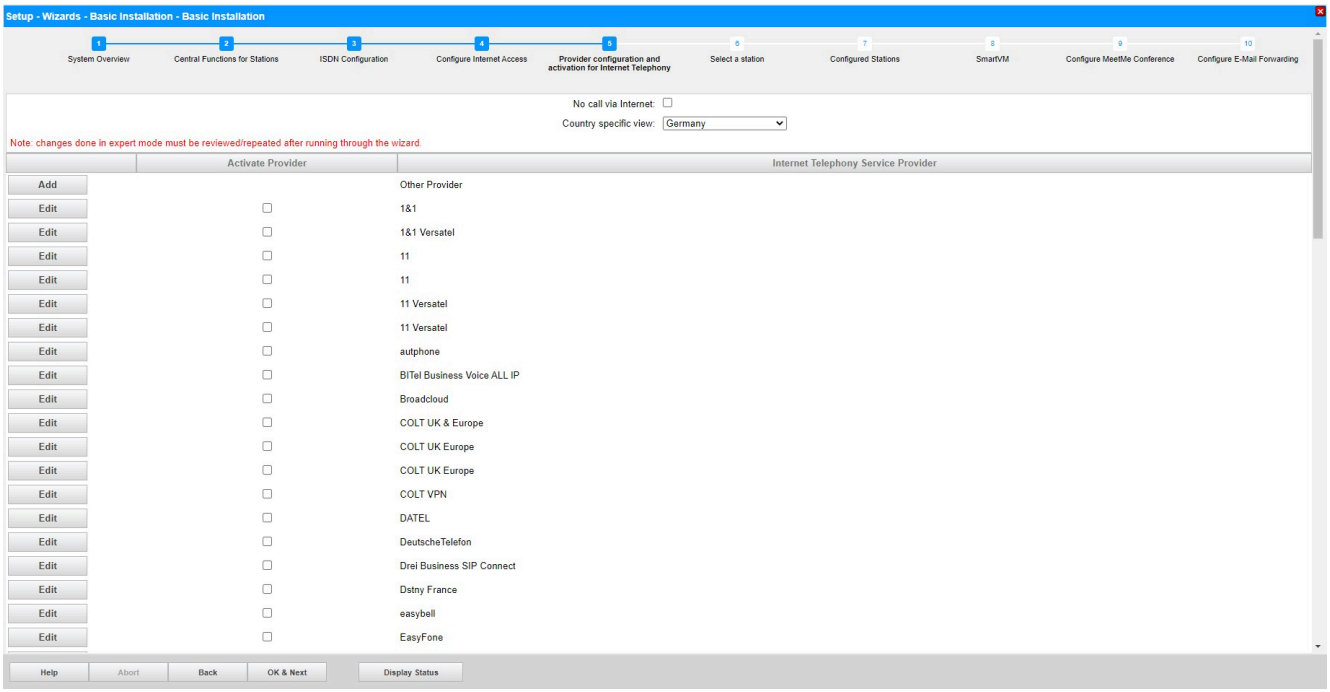
You are in the **Provider configuration and activation for Internet Telephony** window.

The Internet connection is operational.

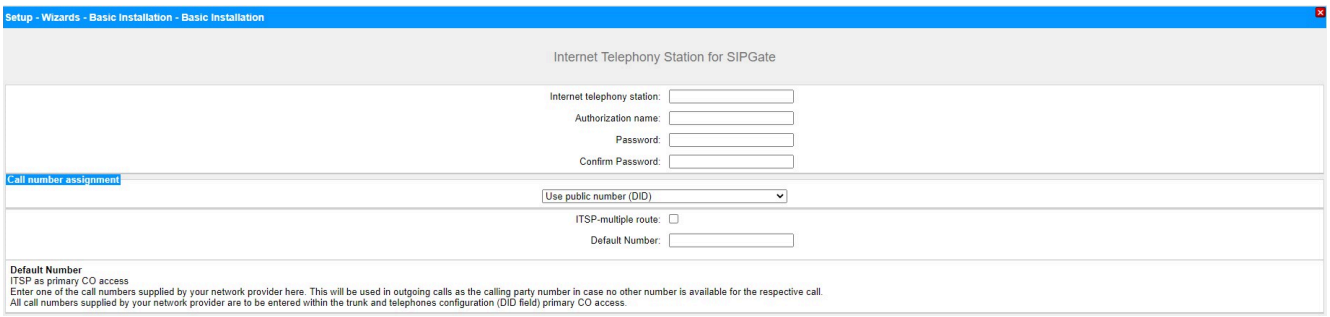
Your ITSP's Internet telephony access data is available (for example, user account, password and Internet telephony numbers).

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.



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.



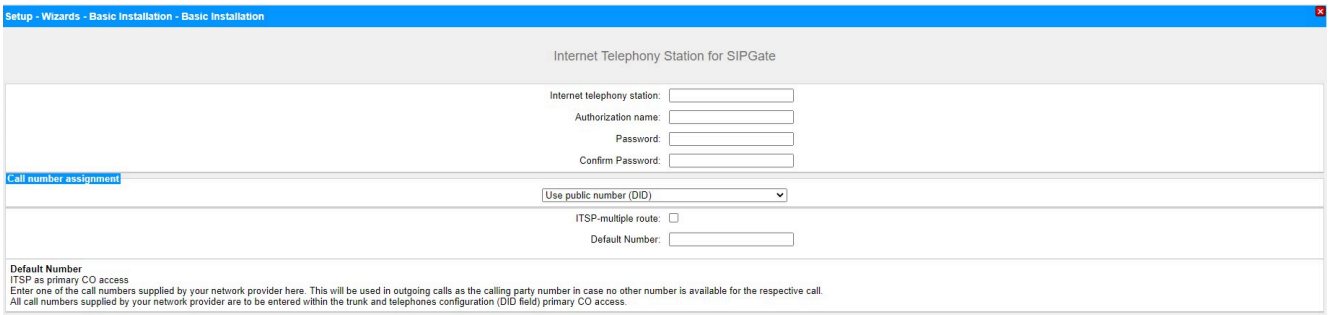
8) Enter the credentials for your account in the **Internet Telephony Station** field. You received this data from your ITSP. Depending on the ITSP, different designations are used for this, for example: SIP User, SIP ID, etc.

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).



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

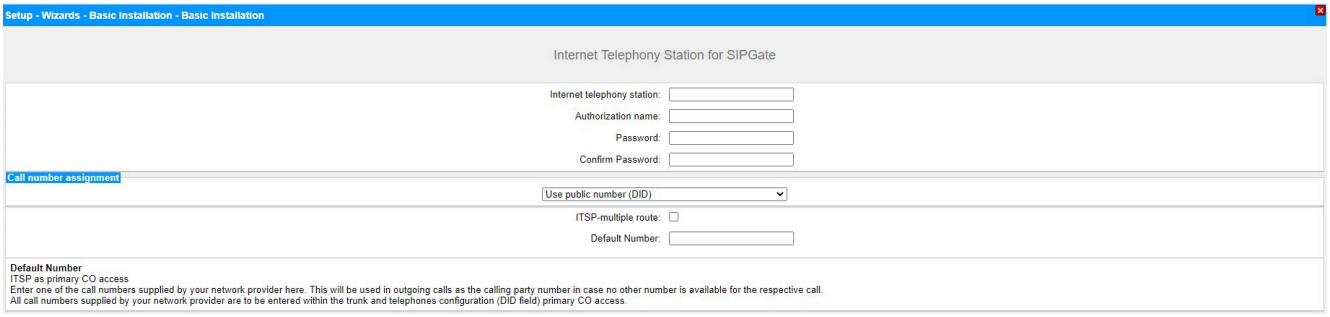
b) Under **Default Number**, enter the phone number to be used for outgoing calls to subscribers who do not have their own phone number.

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.



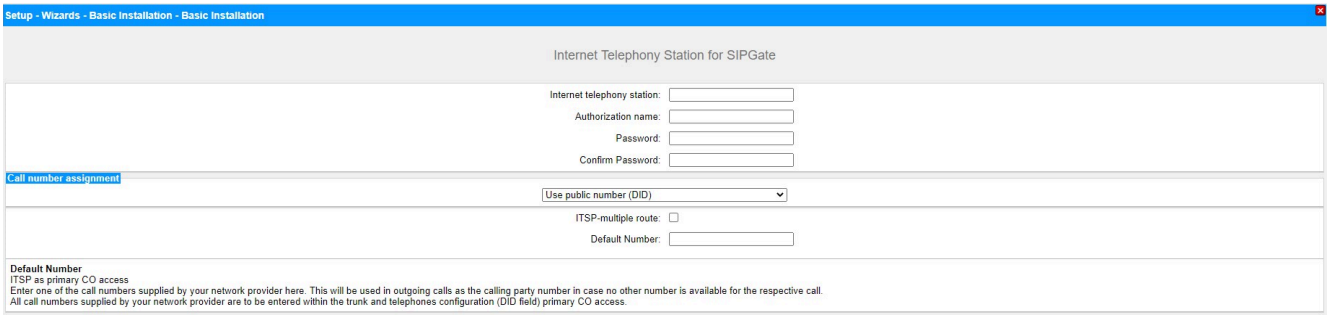
a) Select the option field **Use internal number (CalIno) / Single entries** in the **Call number assignment** area.

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 (CalIno) / 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.



a) Select the option field **Use internal number (CalIno) / 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**.

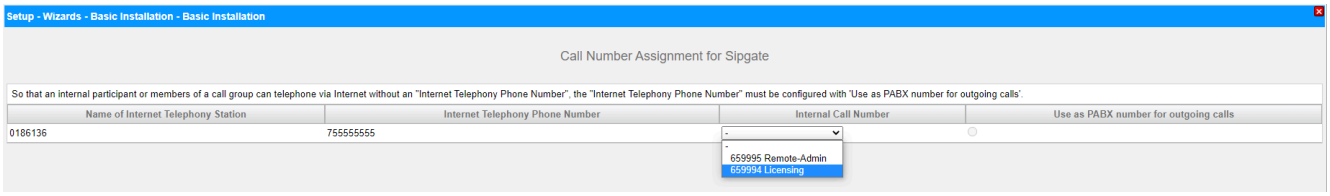
15) If you want to configure additional accounts and their associated Internet telephony numbers, repeat steps 7 through 14.

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.



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!

NOTICE: 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**.

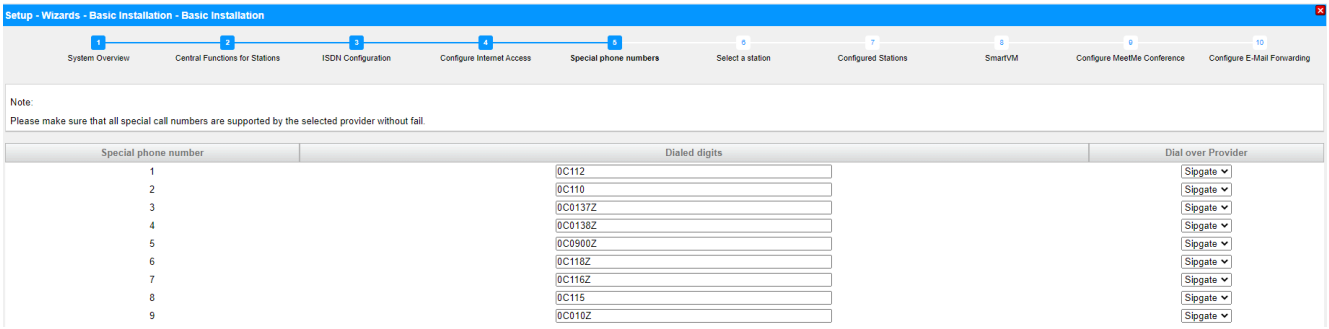
22) If you did not activate the full-time circuit when setting up your Internet access, you can now do this here. Without a permanent connection (full-time circuit), you cannot receive calls over the Internet. If the full-time circuit has already been set up, the fields described under a) to c) will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



The following station number entries are valid:

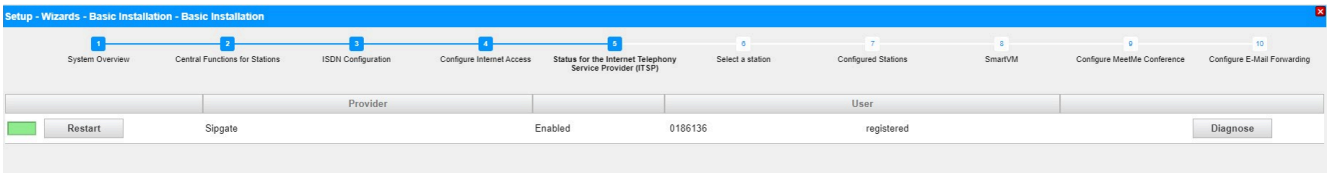
- 0 to 9: allowed digits
- -: Field separator
- X: Any digit from 0 to 9
- N: Any digit from 2 to 9
- Z: One or more digits to follow up to the end of dialing
- C: Simulated dial tone (can be entered up to three times)

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.

NOTICE: 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.



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**.

5.7.6.2 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.

5.7.7 Stations

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

Proceed as follows:

1) Configure ISDN stations

ISDN stations include ISDN phones or ISDN fax devices, for example. ISDN stations can only be configured if an S_0 interface has been set up as the internal S_0 port.

2) Configure analog stations

Analog stations include analog phones or analog fax devices, for example.

3) Configure UP0 stations

UP0 stations include system phones such as OpenStage 60 T.

4) Configure DECT stations

DECT stations are Cordless/DECT phones. DECT stations can only be configured if one or more Cordless base stations are connected and if the DECT phones have been registered at the base stations. Manager E is used to perform the configuration. For more detailed information on the Cordless configuration, see *Administrator Documentation, Configuring the Integrated Cordless Solution*

5) Configure the IP and SIP stations

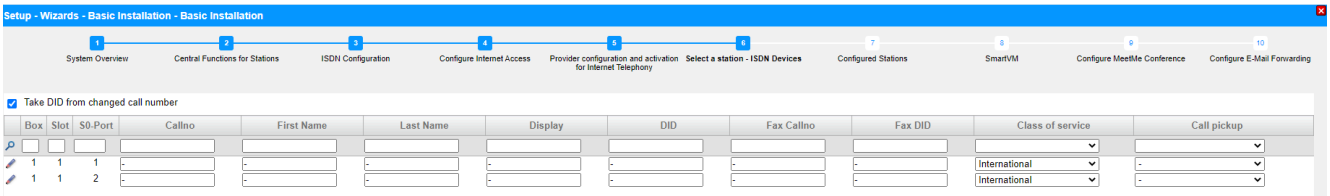
IP and SIP stations include LAN phones or WLAN phones, for example.

5.7.7.1 How to Configure ISDN Stations

Prerequisites

You are in the **Select a station - ISDN Devices** window of the **Basic Installation** wizard.

The S_0 ports to which the ISDN phones are to be connected must be configured as internal S_0ports.



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:

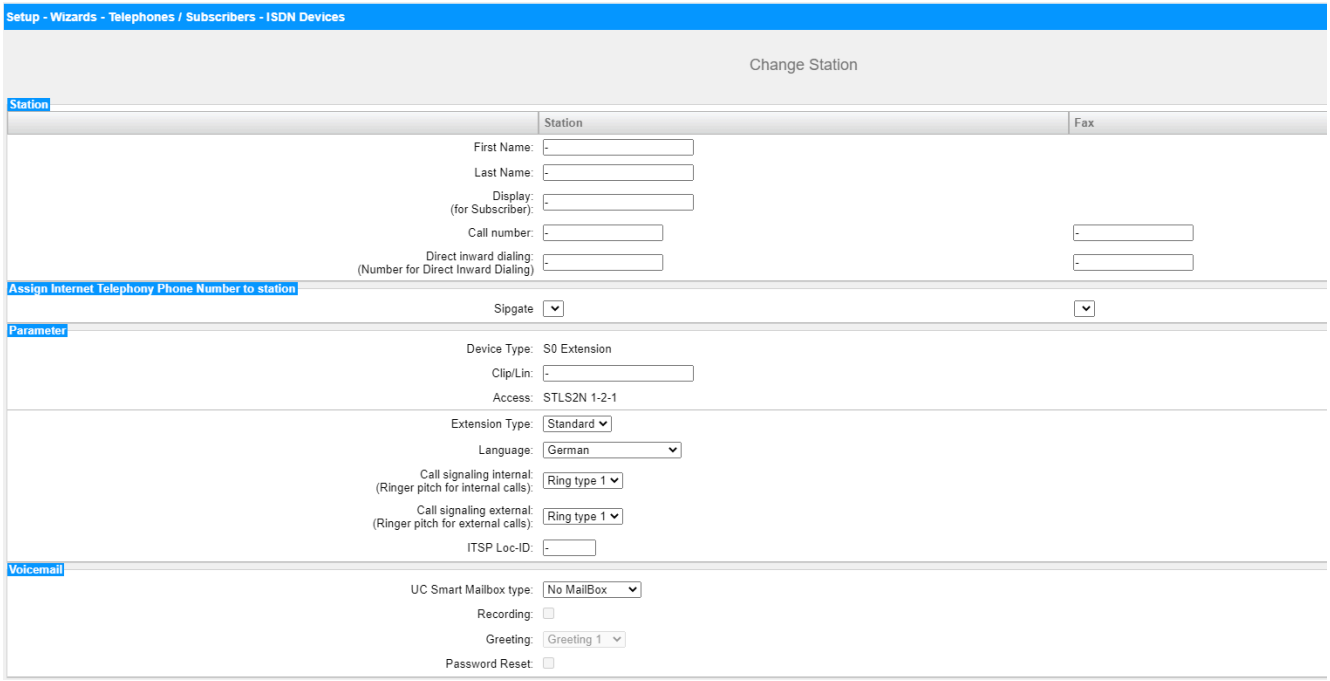
     Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
   - For point-to-point and point-to-multipoint connections:

     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` or `First Name Last Name`.

   NOTICE: The name can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.
4) 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.
5) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.
6) 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.

7) Make the settings described under this step only if needed:

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



b) 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.

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

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

c) Select the type of ISDN terminal from the **Extension Type** drop-down list.

d) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

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) Click on **OK & Next**.

h) Change the station flags as needed. For a description of the station flags, see *Administrator Documentation,* ***Station*** > ***Station*** > ***Station Parameters***.

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

8) If you want to configure additional ISDN stations, click on **Store data** and repeat steps 1 through 7.

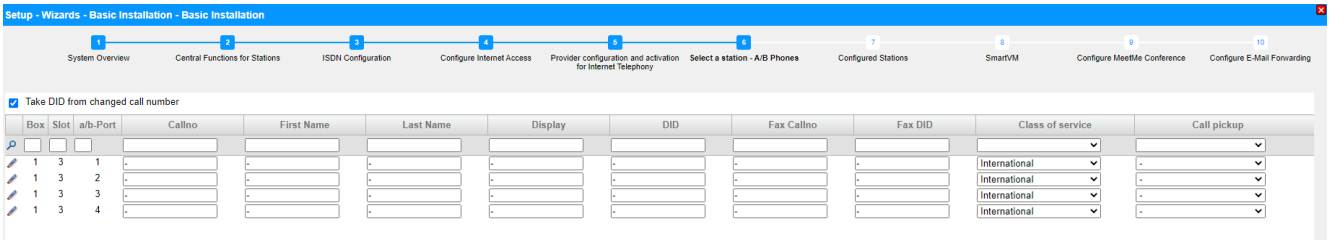
9) Click on **OK & Next**.

5.7.7.2 How to Configure Analog Stations

Prerequisites

You are in the **Select a station - A/B Phones** window of the **Basic Installation** wizard.

A mainboard or a board with analog interfaces is available.



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:

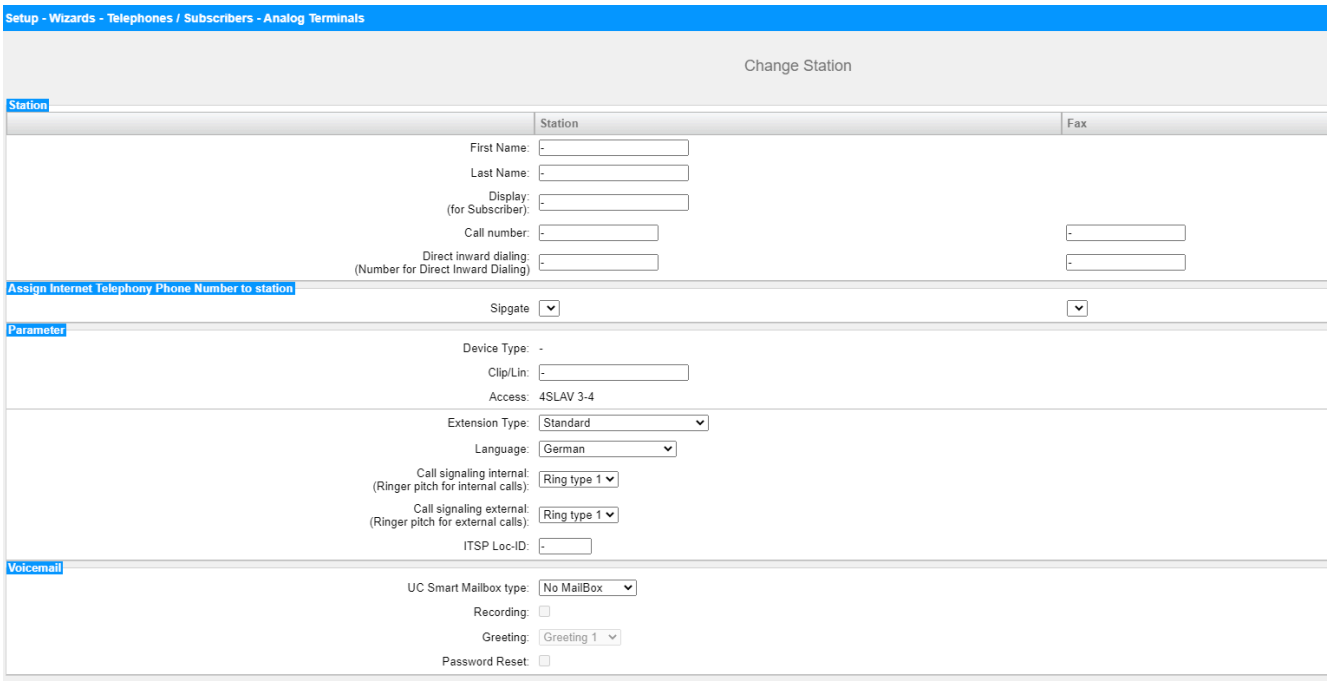
  Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

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` or `First Name Last Name`.

NOTICE: The name can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.

4) 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 DID** field in the row of the desired subscriber.
5) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.
6) 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.
7) Make the settings described under this step only if needed:
   a) Click in the row of the desired analog station on the pencil icon **Edit**.



   b) 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.

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

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP

number and the internal call number is formatted and sent as the Calling Party Number for the external call.

c) Select the analog terminal type (Fax, for instance) from the **Extension Type** drop-down list.

d) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

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) Click on **OK & Next**.

h) Change the station flags as needed. For a description of the station flags, see *Administrator Documentation,* ***Station*** > ***Station*** > ***Station Parameters***.

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

8) If you want to configure another analog station, click on **Store data** and repeat steps 1 through 7.

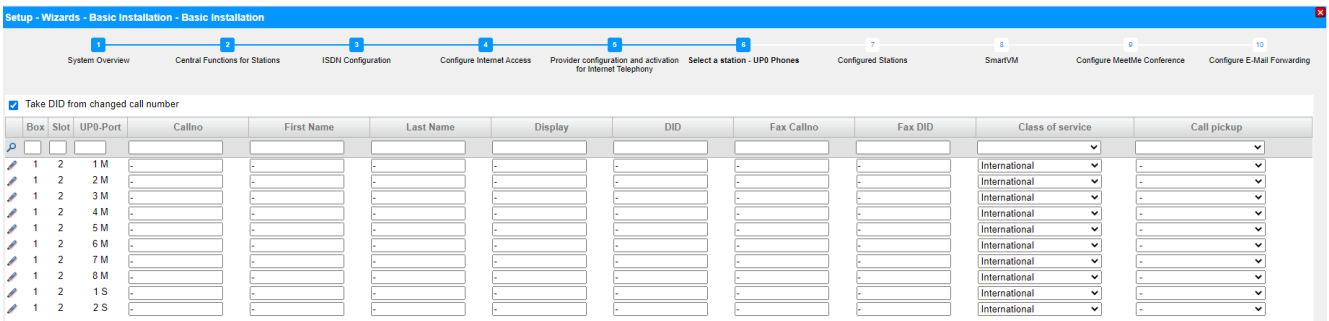
9) Click on **OK & Next**.

5.7.7.3 How to Configure UP0 Stations

Prerequisites

You are in the **Select a station - UP0 Stations** window of the **Basic Installation** wizard.

A mainboard or a board with UP0interfaces is available.



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` or `First Name Last Name`.

NOTICE: The name can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.

---

4) 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.

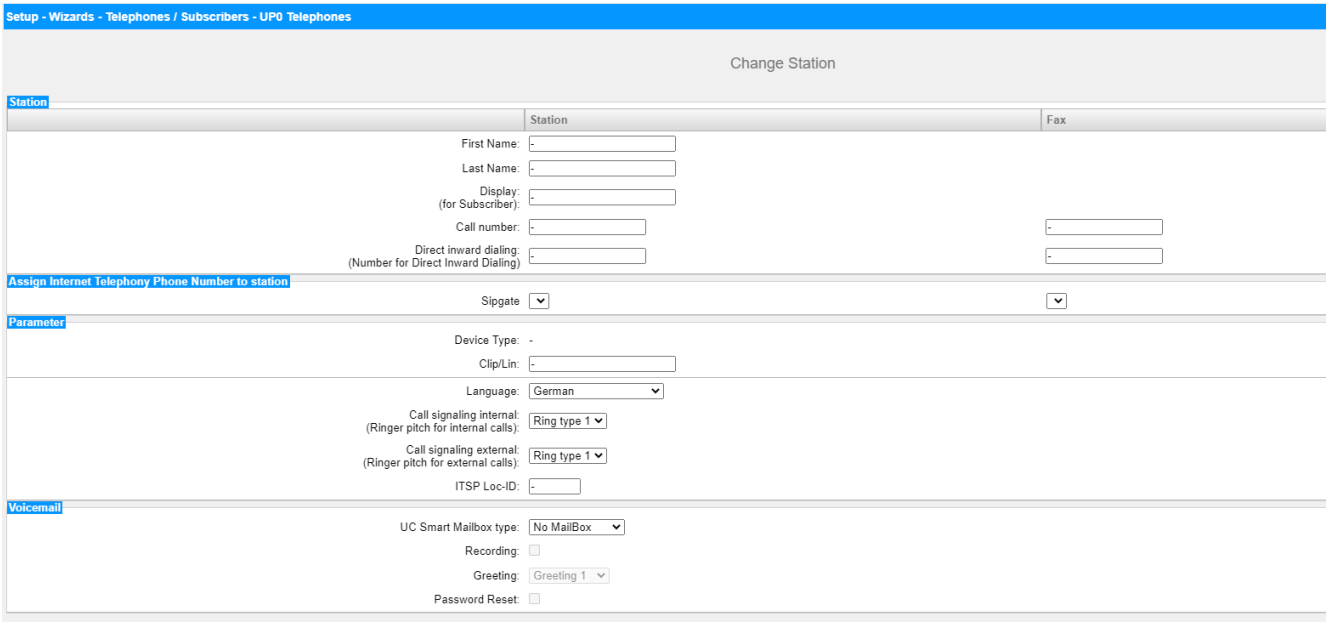
b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.

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

6) 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.

7) Make the settings described under this step only if needed:

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



b) 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.

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

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

c) Select the type of TDM terminal from the **Extension Type** drop-down list.

d) Do not change the default selection in the **Language** drop-down list. This setting has no relevance for TDM terminals.

e) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

f) 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).

g) 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).

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

i) Change the station flags as needed. For a description of the station flags, see *Administrator Documentation,* ***Station*** > ***Station*** > ***Station Parameters***.

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

8) If you want to configure another UP0 station, click on **Store data** and repeat steps 1 through 7.

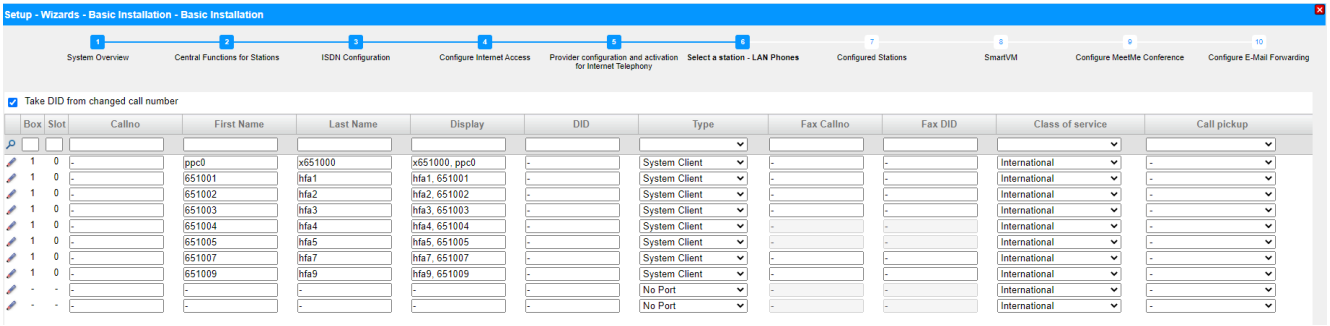
9) Click on **OK & Next**.

5.7.7.4 How to Configure DECT Stations

Prerequisites

You are in the **Select a station - DECT Stations** window of the **Basic Installation** wizard.

To configure DECT stations, a base station must be connected, and the DECT phones must be logged in there. If this is not the case, skip this window. You can also configure the DECT stations later (see *Administrator Documentation, Configuring Stations*).



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) 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.

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

NOTICE: The name can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.

---

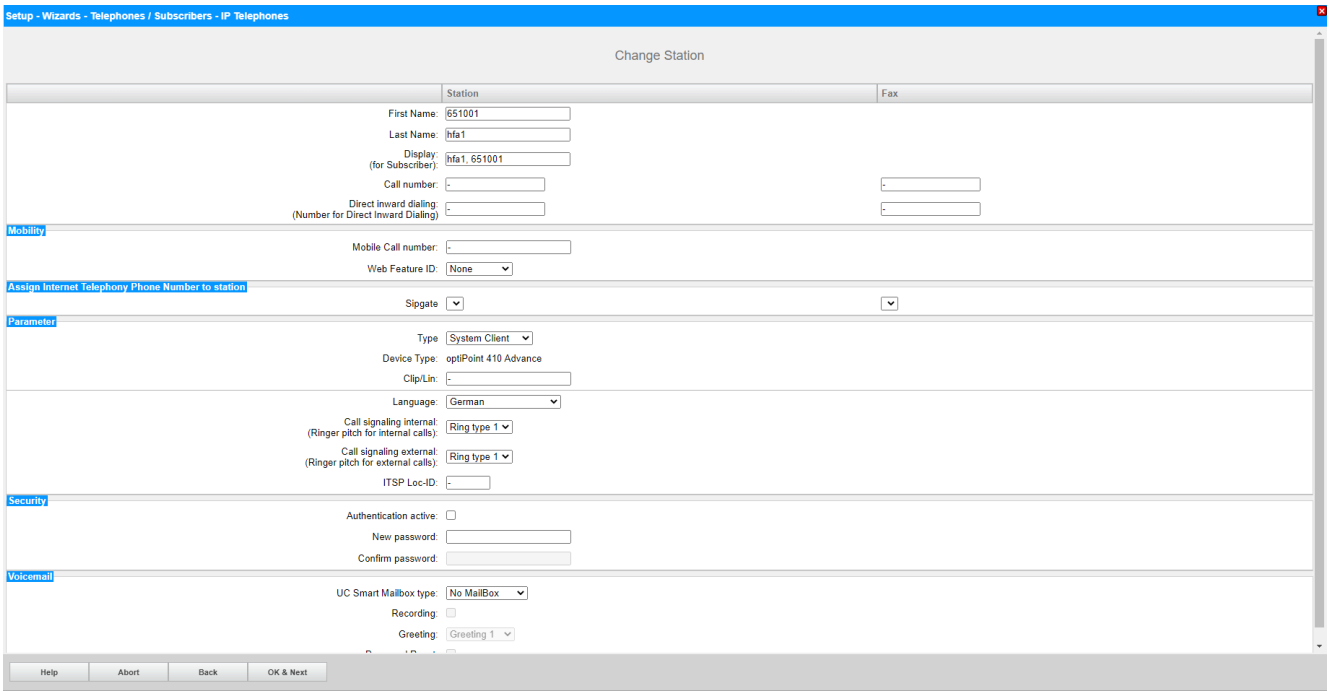
5) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

6) 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.

7) If you want to change the DECT phone code (PIN), enter the new code in the row of the desired subscriber under **Mobile code**. The DECT subscribers must log on at the base station again with this code.

8) Make the settings described under this step only if needed:

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



b) 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.

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

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

c) Select the type of cordless device from the **Extension Type** drop-down list.

d) Do not change the default selection in the **Language** drop-down list. This setting has no relevance for cordless devices.

e) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

f) 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).

g) 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).

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

i) Change the station flags as needed. For a description of the station flags, see *Administrator Documentation,* ***Station*** > ***Station*** > ***Station Parameters***.

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

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

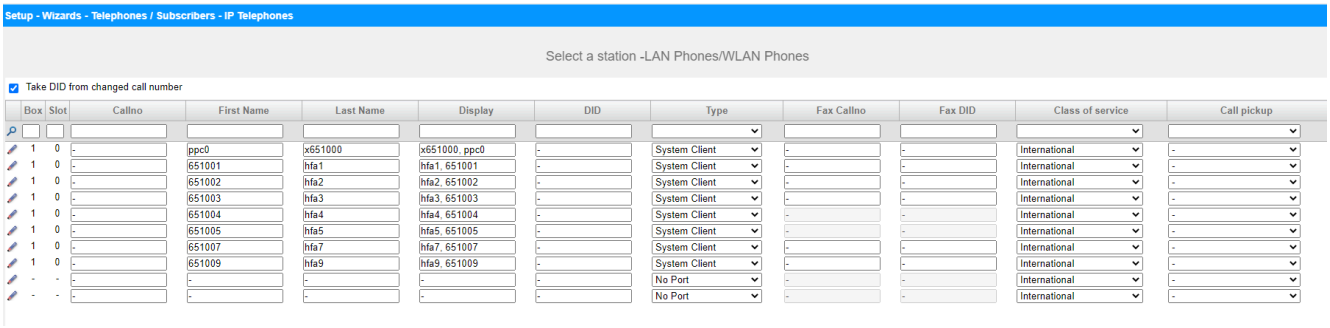
10) Click on **OK & Next**.

5.7.7.5 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.



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`.

> **NOTICE:** 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.

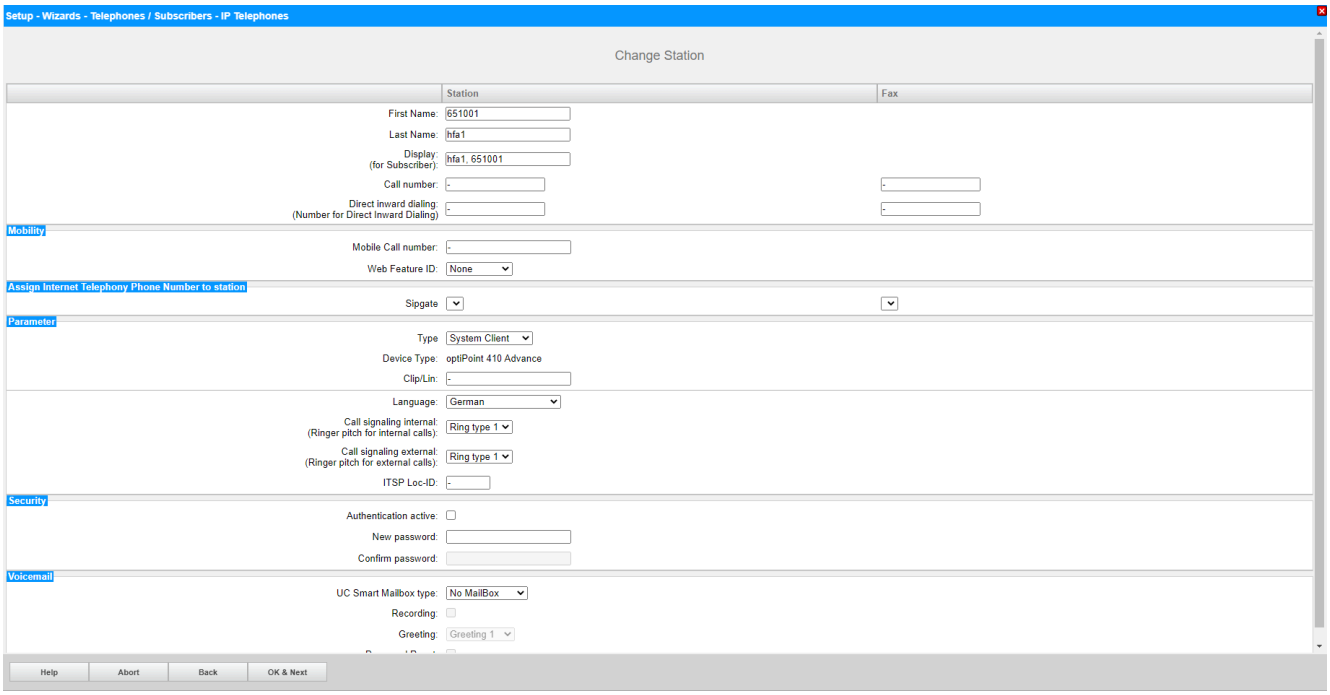
   b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.

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**.



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, Dual-Mode Telephony*).

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.

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

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

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 *Administrator Documentation,* ***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**.

5.7.8 Configuring UC Suite

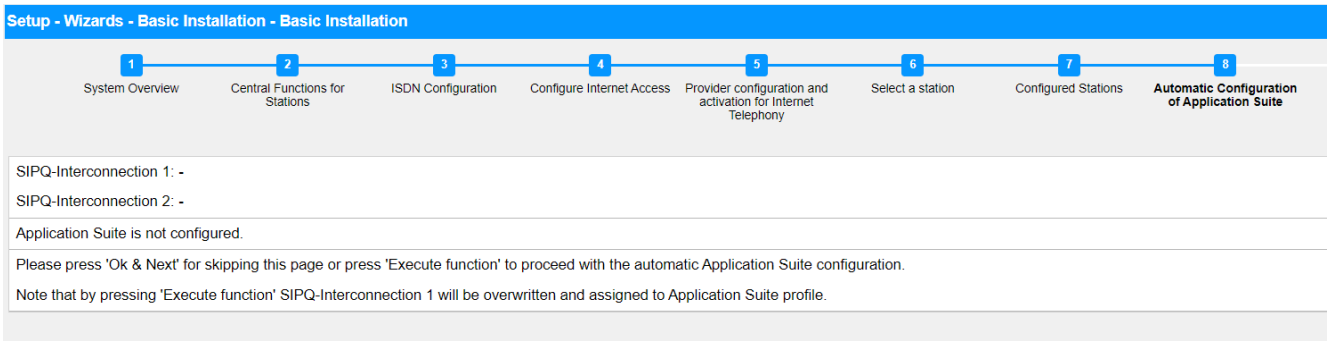
You can perform the automatic configuration of the UC solution UC Suite in the **Automatic Configuration of the Application Suite** window.

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

5.7.8.1 How to Configure the UC Suite

Prerequisites

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



Step by Step

1) If no UC Booster Card is integrated into the communication system, click on **OK & Next**. The configuration will be skipped.

2) If the UC Booster Card is integrated into the communication system, click on **Execute function**. The UC Suite is configured automatically. Once the progress bar shows 100%, click on **OK & Next**.

5.7.9 Configuring UC Smart Mailboxes

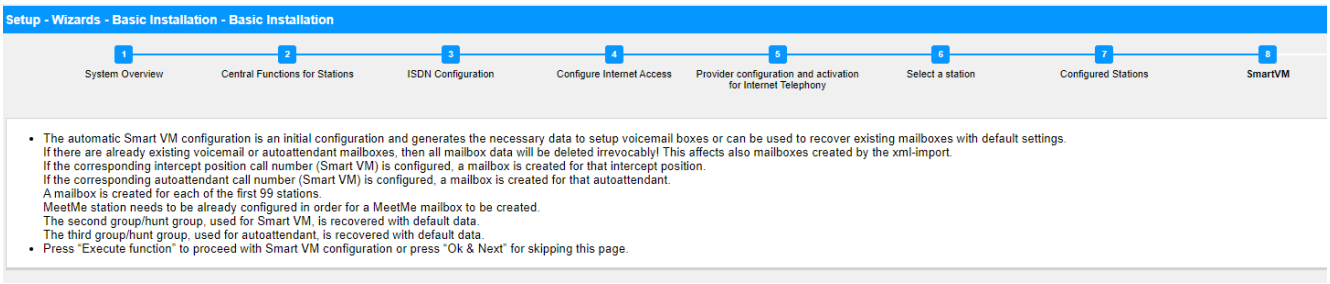
If you are using the UC solution UC Smart, you can perform the automatic configuration of the UC Smart voicemail boxes (Smart VM, Smart VoiceMail) in the **Automatic Configuration of Smart VM** window.

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

5.7.9.1 How to Configure UC Smart Voicemail Boxes

Prerequisites

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



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**.

NOTICE: Existing UC Smart or UC Smart AutoAttendant voicemail boxes are irrevocably deleted in the process.

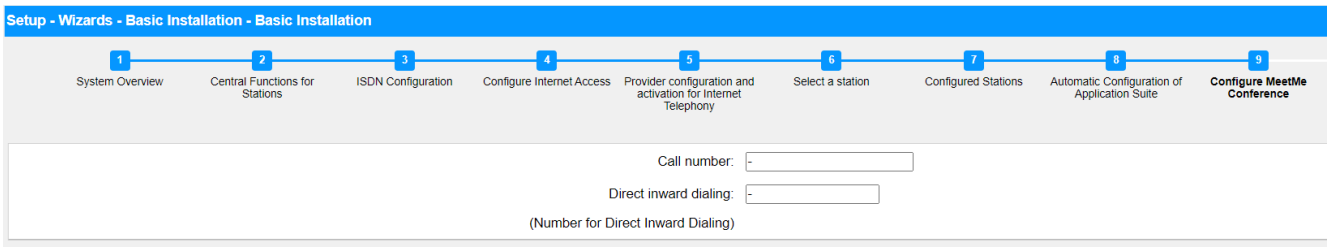
5.7.10 Conference Server Settings

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

5.7.10.1 How to Edit the Conference Server Settings

Prerequisites

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



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**.

5.7.11 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.

  NOTICE: 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.

5.7.11.1 How to Configure the Sending of E-mails

Prerequisites

If the external E-mail server has been configured to use basic authentication, make sure an e-mail account with a password exists with an e-mail provider, and you know the access data for this account.

If the external E-mail server has been configured to use modern authentication (Microsoft OAuth 2.0 token-based authorization), as in the case of Exchange Online, make sure that:

- An application with the required permissions has been registered in Microsoft Azure Active Directory (Azure AD) for your OpenScape Business system to send emails.
- You know the Application (client) ID and the Directory (tenant) ID of the registered application.

  Ask your Azure AD administrator to provide these values, if required.
- The email address that will appear as the sender of the emails belongs to the same Azure AD or tenant as the registered application.

You are in the **Configure E-Mail Forwarding** window of the **Basic Installation** wizard.

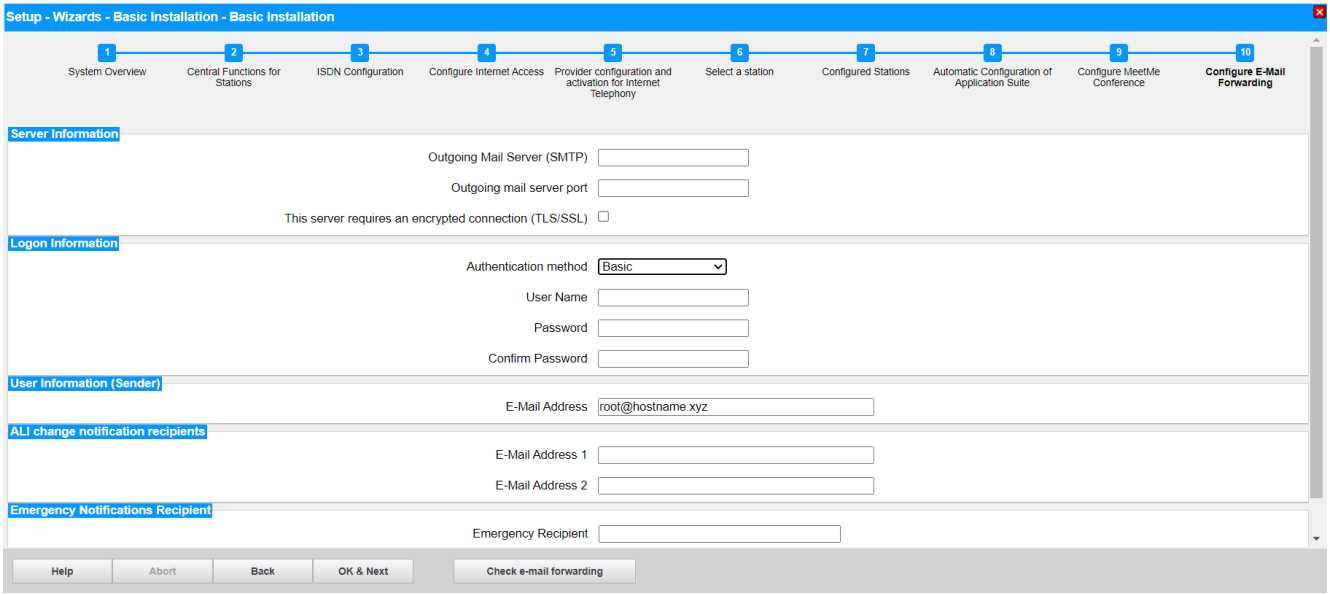


Figure 4: E-mail forwarding options when basic authentication method is selected

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.

> **NOTICE:** 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) Enter the **Outgoing mail server port** for the server port to be used for sending e-mails. Ask your e-mail provider for the outgoing mail server if required.

3) If a secure connection is required, enable the **This server requires an encrypted connection (TLS/SSL)** check box. If required, check with your e-mail provider whether this option needs to be enabled.

4) If the external E-mail server has been configured to use basic authentication, proceed as follows:
   a) From the **Authentication method** drop-down list, select **Basic**.
   b) Enter the **User Name** of the e-mail account, e.g.,: `john.doe`.
   c) Enter the **Password** for the e-mail account and repeat it in the **Confirm Password** field.
5) If the external E-mail server has been configured to use modern authentication, proceed as follows:
   a) From the **Authentication method** drop-down list, select **Microsoft OAuth 2.0**.
   b) Enter the Application (client) ID obtained from the Microsoft Azure portal in the **Application ID** field.
   c) Enter the Directory (tenant) ID obtained from the Microsoft Azure portal in the **Tenant** field.
6) Enter the **E-mail Address** that will appear as the sender of the emails, for example: `john.doe@web.de`.
7) Enter the **E-mail Address 1** to get a notification email when ALI tolerance has been used. You may also enter a second email address in the **E-mail Address 2** field.
8) In the **Emergency Recipient** field, enter the e-mail address of an on-site security officer to which an e-mail is sent when an emergency number is dialed.

   The subject of the e-mail will be "New emergency call". The call number and the name of the caller, if configured, are included in the e-mail which are retrieved from the database of the system.
9) If you have selected **Microsoft OAuth 2.0** as authentication method, proceed as follows:
   a) Click on **OK & Next**.
   b) Wait for an authorization link and user code to appear.

      The authorization code expires after some minutes.
   c) Open the authorization link and enter the user code on the pop-up.
   d) Sign in with the email address you have entered in step 6 on page 107 (**E-mail Address**).

      The email address must be in the same Azure AD or tenant as the registered application.
   e) After successful authentication, the pop-up displays a message as below:

      `You have signed in to the <application-name> on your device. You may now close this window..`
   f) Close the pop-up and return to WBM. If the authentication was successful, you will see the message `The authentication was successful!.`

10) If you want to check the entered e-mail settings, proceed as follows:

a) Click on **Check e-mail forwarding**.

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, click **Back** and proceed to the next step.

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

11) 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.

5.8 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. In a standalone system, system-wide features are enabled automatically upon activation.

2) Provision the UC Smart client for installation (only for UC Smart)

3) How to Provision the UC Suite Clients for Installation (for UC Suite only)

The UC Suite clients are part of 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 *Administrator Documentation, Silent Installation/Uninstallation for UC Suite PC Clients*.

4) Go through the product-specific security checklist with the customer and document any deviations.

5) Perform a data backup

All previous changes to OpenScape Business must be backed up. The backup can be stored as a backup set on a USB storage device or in the internal network.

5.8.1 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.

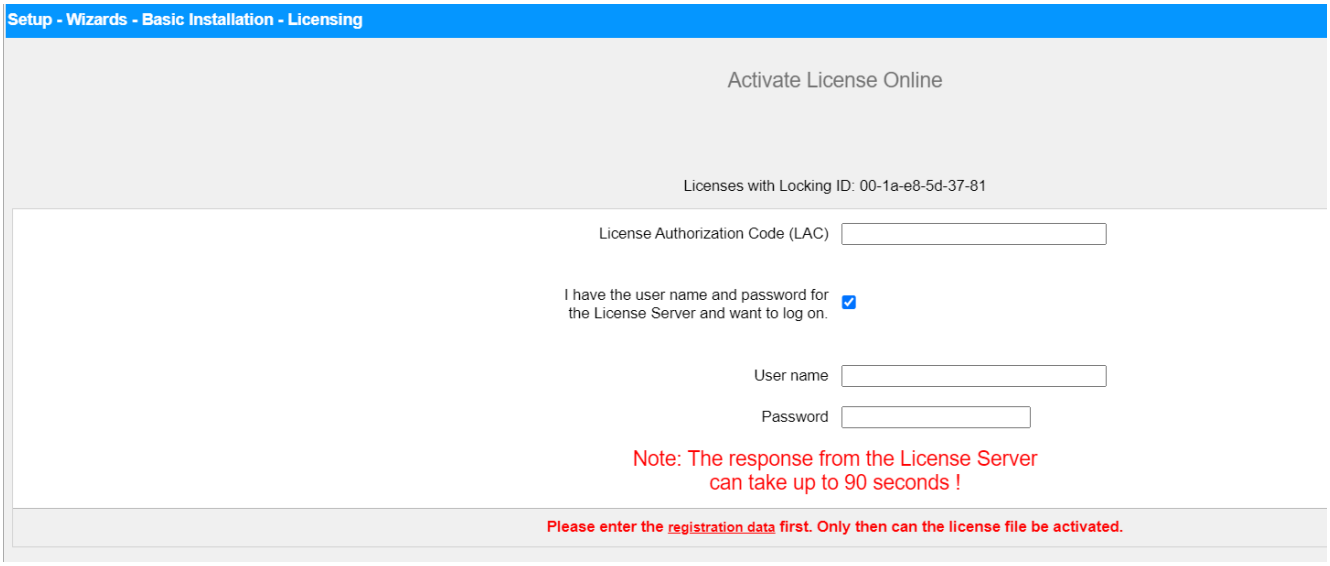
Step by Step

1) Activate license online:

a) In the navigation bar, click on **Setup**.

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

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



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.

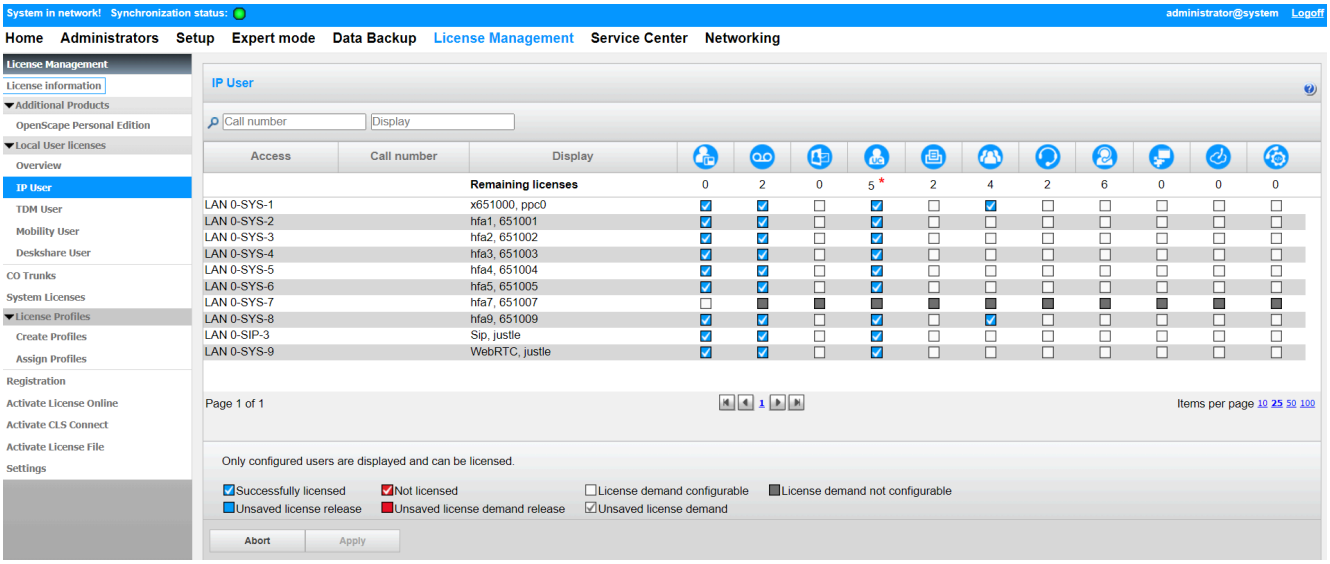
g) Click on **OK & Next**. The connection to the license server is established, and the licenses are released.

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).



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

NOTICE: 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) For S_{2M} trunks: In the **S2M** area, in the row of the desired slot, select the number of desired B-channels in the drop-down list of the **Demands** column.
   d) For T1 trunks (only for the U.S.): In the **T1** area, in the row of the desired slot, select the number of desired B-channels in the drop-down list of the **Demands** column.
   e) Click on **OK & Next**.

NOTICE: The number of licensed SIP trunks and S_{2M}/T1 trunks must not exceed the number of trunk licenses purchased.

5.8.2 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 @work are available.

NOTICE: Licenses are required to use the UC Smart client myPortal @work.

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 @work** and save the installation file on a shared network drive.
4) Send the two installation files to the users of myPortal @work.
5) Alternatively, you can also send the users of myPortal @work the link with which they can access the installation file:

```
https://<IP address of the communication system>/
management/downloads/myPortalAtWorkSetup.exe
```

5.8.3 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.

NOTICE: 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.

NOTICE: 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
```

5.8.4 How to Perform a Data Backup

Prerequisites

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

For a backup to a USB storage device (USB stick or USB hard disk), the USB device must be connected to the USB server port.

NOTICE: For more information on backing up data, see *Administrator Documentation, Immediate Backup*.

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 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) If you are using a USB stick as the backup medium, wait until the LED of the USB stick stops blinking. This ensures that the backup has been successfully saved on the USB stick. You can then safely remove the USB stick.
8) 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.

NOTICE: If a new software version for the communication system is available, you will be notified about this on the home page of the WBM, provided the Internet connection was set up correctly. If a new software version is available, perform an update (see *Administrator Documentation, Updating the Communication System*).

5.9 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.

NOTICE: 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.

5.9.1 How to Configure an IP Phone

Prerequisites

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

NOTICE: 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.

5.9.2 How to Configure a SIP Phone

Prerequisites

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

NOTICE: 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.

Index