A MITEL
PRODUCT
GUIDE

Mitel OpenScape Business

OpenScape Business X3/X5/X8

OpenScape Business V4

Installation Guide

06/2026

A31003-P3040-J106-01-7631

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 V4

Impacted chapters	Change description
Obsolete or end-of-life components have been removed through out the document	• myPortal to go • OpenScape Business Attendant • OpenScape Business BLF • UC Booster Server • UC Booster Card (OCAB) • X3R, X3W, X5W

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 X5/X8 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 X5/X8, Installation Guide

  This document describes the installation of the hardware and the initial installation of OpenScape Business X5/X8.

- OpenScape Business S, Installation Guide

  This documentation describes the initial installation of the OpenScape Business S softswitch.
- OpenScape Business X1, Service Documentation

  This documentation describes the hardware of OpenScape Business X1.
- OpenScape Business X5/X8, Service Documentation

  This documentation describes the hardware of OpenScape Business X5/X8.

Administration

The following documentation is intended for administrators.

- Administrator Documentation

  This documentation describes the configuration of features that are set up using the OpenScape Business Assistant (WBM). The Administrator documentation is available in the system as online help.
- Configuration for Customer Administrators, Administrator Documentation

  This documentation describes the configuration of features that can be set up using the OpenScape Business Assistant (WBM) with the **Basic** administrator profile.
- Manager E, Administrator Documentation

  This documentation describes the configuration of features that are set up using Manager E.

UC Clients / Telephone User Interfaces (TUI)

The following documentation is intended for UC users.

- myPortal for Desktop, User Guide

  This documentation describes the installation, configuration and operation of the UC client myPortal for Desktop.
- myPortal for Outlook, User Guide

  This documentation describes the installation, configuration and operation of the UC client myPortal for Outlook.
- myPortal @work, User Guide

  This documentation describes the installation, configuration and operation of the UC client myPortal @work.
- Fax Printer, User Guide

  This documentation describes the installation, configuration and operation of Fax Printer.
- myAgent, User Guide

  This documentation describes the installation, configuration and operation of the Contact Center client myAgent.
- myReports, User Guide

  This documentation describes the installation, configuration and operation of the Contact Center client myReports.
- myAttendant, User Guide

  This documentation describes the installation, configuration and operation of the attendant console myAttendant.

- UC Smart Telephone User Interface (TUI), Quick Reference Guide

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

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

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

- Use separate ground wires to provide protective grounding for the OpenScape Business X5R communication system. Before you start up the system and connect the phones and phone lines, connect the communication system with a permanent earthing conductor.
- Provide protective grounding for each system box of the OpenScape Business X8 communication system with a separate ground wire. Before you start up the system and connect the phones and phone lines, connect the communication system with a permanent earthing conductor.
- 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). Disconnect all the communication system's power plugs and make sure that the communication system is not supplied by another power source (uninterrupted power supply unit, for instance).

  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 lines from the communication system before disconnecting the prescribed ground wire from the system.

- As long as the power supply is switched on, always observe the greatest caution when performing measurements on powered components and maintenance work on PC boards and covers.

  Metallic surfaces such as mirrors are conductive. If you touch them, there is a risk of electric shocks or short circuits.

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

- Use only the approved battery packs.
- 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.
- Do not store any documents or similar flammable items in a communication system.

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.

2.2.5.1 Safety Information for Australia

The following safety precautions must always be observed when installing, starting up and operating the OpenScape Business X and OpenScape Business S communication systems in Australia:

- The OpenScape Business X and OpenScape Business S communication systems must be installed and serviced only by authorized personnel.
- OpenScape Business wall systems must be installed near the mains socket outlet that supplies power to the respective communication system. The wall

socket shall be readily accessible. The integrity of the wall socket must be assured.
- The OpenScape Business X and OpenScape Business S communication systems must be configured to allow emergency calls (for example, 000) to be made at all times.
- If no emergency backup power supply is available or if no switchover to emergency analog phones (trunk failure transfer) is possible in the event of a power failure, then no emergency calls can be made via the communication system following a power failure).
- Music on Hold and paging devices must be connected to the communication system via a Line Isolation Unit approved by the Australian Communications Authority (ACA).

2.2.5.2 Safety Information for Brazil

The following safety precautions must always be observed when installing, starting up and operating the OpenScape Business X and OpenScape Business S communication systems in Brazil:

- The use of the outlet strip with overvoltage protection with part number C39334-Z7052-C33 is absolutely mandatory. The power supply of the OpenScape Business X and OpenScape Business S communication systems must be passed through an outlet strip with overvoltage protection.
- The use of shielded Ethernet cables for the LAN/WAN interfaces/ports of the OCCL, OCCM, OCCMR, OCCMB, OCCMA, OCCMBR, OCCMRA and OCCLA mainboards is absolutely mandatory.

2.2.5.3 Safety Information for the U.S.

The following safety precautions must always be observed when installing, starting up and operating the OpenScape Business X and OpenScape Business S communication systems in the United States:

- Disruption of the Network and T1

  When communication systems are networked using T1 (1.544 Mbit/s), the telecommunications company (Federal Communications Commission (FCC)) must be notified whenever a communication system is removed from the grid.

  If any of the communication systems of Unify Software and Solutions GmbH & Co. KG described in this documentation disrupts the operation of the public telecommunications network, the telecommunications company is entitled to temporarily block access to the outside line. In general, the telecommunications company will inform you about this in advance. If this is not possible, you will receive notification at the earliest possible time. In this context, you will also be informed that you can lodge a complaint with the telecommunications company.
- Telephone Company Facility Changes

  The telecommunication company is entitled to adapt its own equipment, devices, operating procedures, and processes as necessary; Such modifications may impair the operation of your communication systems. Under normal circumstances, you should be notified in advance so you can maintain uninterrupted telephone service.

- Nonlive Voice Equipment

  Nonlive voice equipment, such as music-on-hold devices and voice recorders must be approved and released by Unify Software and Solutions GmbH & Co. KG and registered in accordance with the rules and regulations of Subpart C of the FCC Rules, Part 68.

  Unreleased devices for voice playback may only be connected through protective circuitry that is approved and released by Unify Software and Solutions GmbH & Co. KG and registered in accordance with the rules and regulations in Subpart C of the FCC Rules, Part 68.
- Ringer Equivalence Number REN

  The Ringer Equivalence Number (REN) is used to determine the number of devices that can be connected to a telephone line so that all the devices ring when that telephone number is called. In most areas, but not all, the sum of the RENs of all devices connected to a line should not exceed five. Contact the local telecommunication company to determine the maximum REN for your calling area.
- New Local Area and CO Access Codes

  Least Cost routing (LCR) must be configured to automatically recognize and take changes in local area codes and CO access codes into account. Otherwise, these codes will not be usable for calls when changes occur.
- Hearing Aid Compatibility

  Emergency phones and public phones (installed in common areas such as lobbies, hospital rooms, elevators, and hotel rooms, for example) must have handsets that are compatible with magnetically coupled hearing aids. Hearing-impaired individuals who are not in common areas must be provided with hearing-aid compatible handsets, if needed.

  All digital phones from Unify Software and Solutions GmbH & Co. KG manufactured after August 16, 1989, are hearing aid compatible and comply with FCC Rules, Part 68, Section 68.316 and 68.317.
- Programmed Dialer features

  When you program emergency numbers or make test calls to emergency numbers with programmed dialer features using products by Unify Software and Solutions GmbH & Co. KG, stay on the line and briefly explain to the dispatcher the reason for the call before hanging up. These activities should be performed during off-peak hours, such early morning or late evening.
- Connecting Off-Premises Station Facilities

  Customers who intend to connect off-premises station (OPS) facilities must inform the telecommunications company of the OPS class for which the equipment is registered and the connection desired.
- Direct Inward Dialing Answer Supervision

  Customers who operate any of the communication systems from Unify Software and Solutions GmbH & Co. KG described in this documentation

without providing proper answer supervision are in violation of Part 68 of the FCC rules.

Every communication system of Unify Software and Solutions GmbH & Co. KG described in this documentation returns proper answer supervision to the public switched telephone network (PSTN) when DID calls are:

– answered by the called station.
– answered by an attendant.
– routed to an announcement administered by the customer.

In addition, every communication system of Unify Software and Solutions GmbH & Co. KG described in this documentation also returns proper answer supervision on all DID calls forwarded to the PSTN. Permissible exceptions are when:

– A call is not answered.
– A busy tone is received.
– A congestion tone (reorder tone) is received.

- Equal Access Requirements

  Call aggregators with an increased volume of traffic (such as hotels, hospitals, airports, schools, and so on) must provide end users equal access to the providers of their choice. The current equal access codes (also known as Carrier Access Codes, CACs) are 10xxx and 101xxxx, and 800/888 and 950, where xxx or xxxx represents the provider code.

  To select the provider of choice for a call, the user dials a provider-specific access code before dialing the called party number. Equal access is also obtained by dialing the 800/888 or 950 code of the provider of choice.

  Every communication system of Unify Software and Solutions GmbH & Co. KG described in this documentation is capable of providing user access to interstate providers through the use of equal access codes.

  Modifications by aggregators to alter these capabilities are a violation of the Telephone Operator Consumer Services Improvement Act of 1990 and Part 68 of the FCC Rules.

2.2.5.4 Safety Information for Canada

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.

The following safety precautions must always be observed when installing, starting up and operating the OpenScape Business X and OpenScape Business S communication systems in Canada:

- Ringer Equivalence Number REN

  The Ringer Equivalence Number (REN) defines how many devices can be connected to a telephone line at the same time. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

- Restrictions for connecting devices

  The Innovation, Science and Economic Development Canada (ISED) label identifies certified equipment. This certification means that the equipment meets certain requirements with regard to the protection, operation and security of telecommunication networks. The requirements are documented in the Terminal Equipment Technical Requirements. Innovation, Science and Economic Development Canada (ISED) provides no assurances that certified devices will always operate to the satisfaction of the customer.

  Before installing the equipment and components described in this documentation, it must be ensured that connections to the facilities of the local telecommunications company are permitted. The communication systems and servers must also be installed using an acceptable method of connection. The customer should be aware that compliance with these conditions may not prevent degradation of performance in some situations.

  Repairs to certified equipment should be coordinated by a service technician designated by the manufacturer or supplier. Any repairs or alterations made by the user to any of the equipment or components described in this documentation, or any equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

  To ensure their own safety, users must verify that the electrical ground connections of the power supply, telephone lines and the metallic water pipe system, if present, are interconnected. This precaution may be particularly important in rural areas.

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.

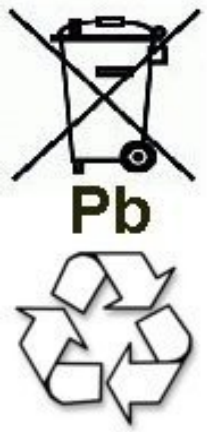
The prerequisites for the proper use of the communication systems and servers include proper transportation, storage, installation, startup, operation and maintenance of the system.

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 Connecting OpenScape Business S to the Power Supply Circuit

For information regarding the connection of OpenScape Business S to the power supply circuit, please refer to the manufacturer's documentation for the server PC and the other components.

Only qualified electricians should perform any work that may be required on the low-voltage network. These installation activities to connect OpenScape Business S must be performed in compliance with IEC 60364-1 and IEC 60364-4-41 or any corresponding legal norms or national regulations (for example in the U.S. and in Canada).

2.3.4.3 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.[***)]

---

*) 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).

2.3.4.4 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.

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.

2.3.4.5 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*.

NOTICE: 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).

2.3.4.6 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 US and Canadian Standards

	Standards reference
Safety USA and Canada	CSA/UL 62368-1

	Standards reference
EMC Emission Canada	ICES-003 Issue 6 Class B
EMC Emission USA	FCC 47 CFR Part 15 Subpart B Class B

FCC Registration Number and Power Consumption

A label on the rear of the housing of the communication systems identifies the FCC registration number, the ringer equivalence number (REN), and other information. Upon request, this information may be disclosed to the telecommunication company.

2.3.7.3 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 the OpenScape Business X and OpenScape Business S communication systems.

2.3.8.1 Operating Conditions for OpenScape Business X

The environmental and mechanical conditions for operating the OpenScape Business X communication systems are specified.

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 systems 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.

2.3.8.2 Operating Conditions for OpenScape Business S

For details on the environmental and mechanical conditions for operating OpenScape Business S, please also refer to the manufacturer documentation of the server PCs and the other components.

3 Preparing for the Installation of OpenScape BusinessX5/X8

Before one of the OpenScape Business X5/X8 communication systems can be set up and put into operation for the first time, a suitable installation site must be found, that complies with the operating conditions (see Operating Conditions for OpenScape Business X), 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 the OpenScape Business X5/X8 communication systems. Certain requirements must be observed when selecting the installation site. Note that there are also some specific requirements regarding the power supply when using the communication systems in the United States and Canada.

OpenScape Business X5R is a communication system in 19-inch rack mount cases that can be mounted in 19-inch rack mount cabinets, as standalone unit (desktop operation).

OpenScape Business X8 is a modular communication system that can be used as a one-box system (base box) or a two-box system (base box + expansion box). OpenScape Business X8 can be installed as a standalone unit or mounted in a 19-inch rack.

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

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
- Meter stick
- Hex or open-end wrench, 8 mm, open-end wrench, 13 mm (only for X8)
- Board wrench (only for X8)
- Drill, hammer, spirit level (only for wall mounting)
- Wiring tool for splitting and jumper strips in main distribution frames
- Digital multimeter for testing ground connections and partial voltages

General Prerequisites for Selecting the Installation Site

Make sure that the installation site meets the following requirements:

- Do not expose the communication system (and the 19" rack) to direct sources of heat (for example, direct sunlight, radiators, etc).
- The communication system (and the 19 " rack) must not be exposed to excessive dust.
- Avoid any contact between the communication system (and the 19 " rack) and abrasive chemicals.

- Avoid all condensation of humidity on or in the communication system during operation.

  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 (see Operating Conditions for OpenScape Business X).
- The power cable connector must be readily accessible for quick disconnection from the power source at any time.
- Allow sufficient space for a main distribution frame or other additional equipment.
- For U.S. and Canada only: The distance between equipment from Unify Software and Solutions GmbH & Co. KG and other electrical equipment must be no less than 40 in. (101.6 cm). The National Electrical Code (NEC) requires 36 in. (91.4 cm) of clearance in front of electrical equipment and 40 in. (101.6 cm) of clearance from other electrical service equipment.

Special Prerequisites for Selecting the X5R Installation Site

Make sure that the installation site meets the following requirements:

- Make sure that a clearance distance of 10 cm to the housing is maintained to guarantee sufficient ventilation for the communication system.

Special Prerequisites for Selecting the X8 Installation Site for a Standalone Installation

Make sure that the installation site meets the following requirements for standalone installation:

- Between the base of a system box and the ground or between stacked system boxes, a minimum clearance of 50 mm must be maintained to guarantee sufficient ventilation for the system boxes.
- When system boxes are stacked, the base box must always be at the bottom of the stack.
- Allow a minimum clearance of 10 cm at the rear and the front of the system boxes for board installation and change.

Special Prerequisites for Selecting the X8 Installation Site for 19-Inch Rack Mounting

Make sure that the installation site meets the following requirements for 19’’ rack-mount installation:

- The 19-inch rack(s) provided for installing the OpenScape Business X8 communication system must have the following characteristics:
  - Components installed in the 19-inch rack must be accessible from both the front and the rear.
  - It should be possible to install components both at the front and at the rear of the 19-inch rack (no less than four vertical bars).
  - It is recommended that the width of the cabinet measure 70 to 80 cm; the depth at least 60 cm. Deeper cabinets (80 to 90 cm) make installation,

cable servicing, and the installation of additional components in the rear of the cabinet much easier.
  - The support brackets required for installing the system boxes must have a minimum ultimate load of 40 kg. The support brackets must be obtained from vendor of the 19-inch rack.
  - The system boxes must be fixed to the cabinet bars using the angle brackets included in the delivery.
- One height unit (one height unit is approx. 1.7” = 43 mm) must be kept clear above the system box to accommodate the gray plastic cover attached to the top of a system box. Never remove this plastic cover.
- To guarantee sufficient heat dissipation, the base box must be mounted at the lowest position in a 19-inch rack. In a 19-inch rack with active (heat-emitting) components already installed, the lowest position must be cleared for installation of the base box. If inactive components (e.g., patch panels) are involved, the base box can also be installed above them.

- The following minimum clearance must be observed in order to ensure adequate ventilation of the system boxes in the 19-inch rack:
  - three height units between two stacked system boxes.
  - one height unit above one system box if a patch panel is being installed, for example.

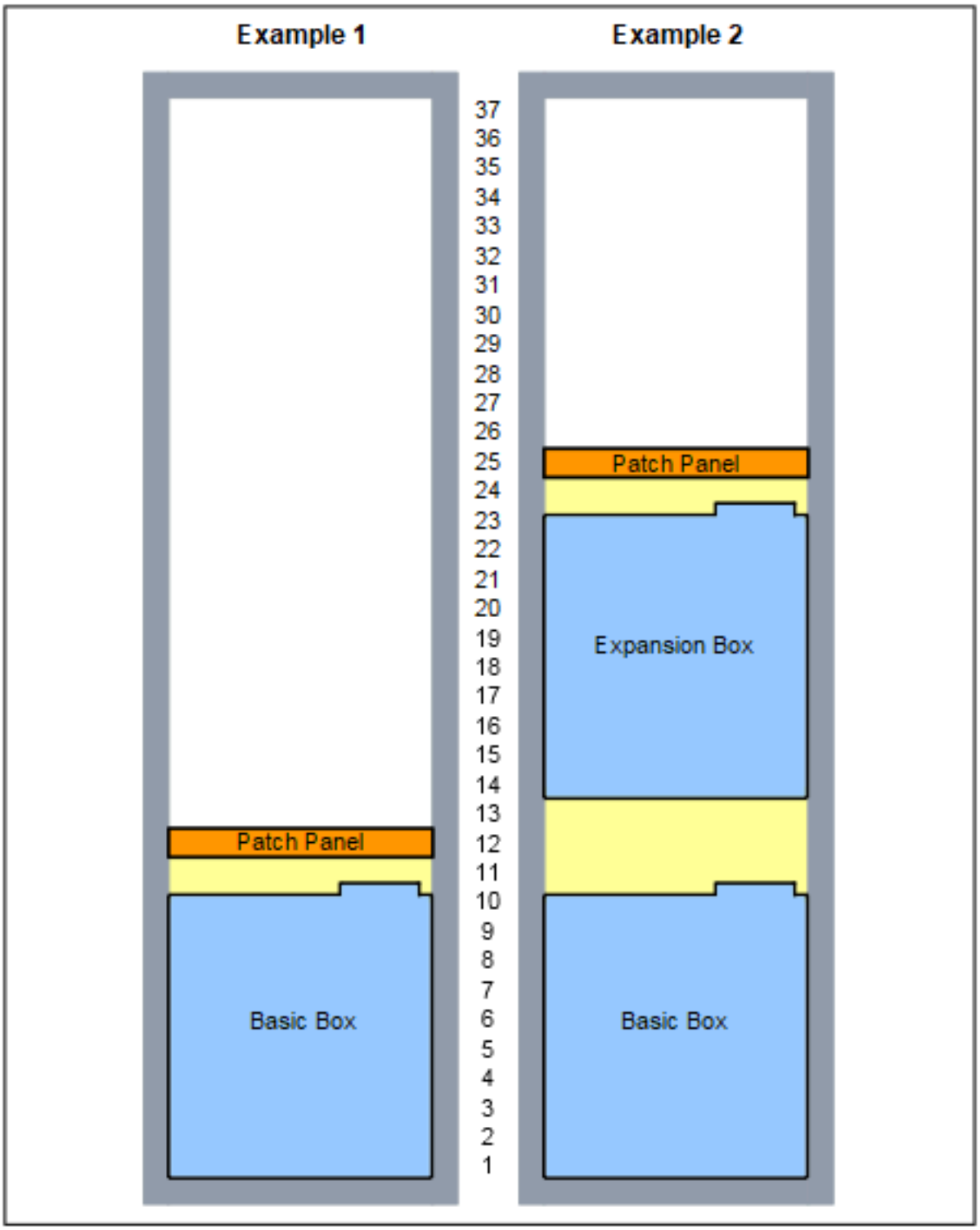


Figure 1: OpenScape Business X8 – Examples for a 19-inch rack height of 1.92 m (37 height units)

For U.S. and Canada only: Prerequisites for Connecting the Power Supply

The power supply for the communication systems must meet the following requirements:

- Electrical Connection Specifications:

Nominal voltage	Nominal voltage range		Nominal frequency range		Wall Outlet Configurations
	from	to	from	to	
120 V AC/60 Hz	110 V AC	130 V AC	47 Hz	63 Hz	NEMA 5-15, 2-pin, 3-wire, grounded

- For X8 only: A UL-listed or CSA-certified overvoltage protector must be inserted between the socket and the communication system. Two system boxes can be connected to each overvoltage protector.

  NOTICE: The OpenScape Business X8 communication system must not be connected directly to a socket!

- For X5 only: An overvoltage protector must be inserted between the socket and the communication system.
- For X8 only: The power source must not be more than 2.4 m (8 ft.) away from the communication system and must provide 120 V AC (single-phase, fused) power at 50-60 Hz and 20 A.
- For X5 only: The power source must not be more than 2 m (6 ft.) away from the communication system and must provide 120 V AC (single-phase, fused) power at 50-60 Hz.
- An independent electric circuit with an isolated ground conductor should be used for each communication system.
- A warning should be attached to the circuit breaker of the power supply to prevent accidental removal of power from the communication system.

3.2 Preparatory Steps

Unpack and check the supplied components before starting the installation.

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.

---

4 Installing the Hardware for OpenScape Business X5R

This section covers the standard installation procedure for the OpenScape Business X5R communication system.

OpenScape Business X5R is a communication systems in 19-inch rack mount cases that can be mounted in 19-inch rack mount cabinets, as standalone unit (desktop operation) or as wall-mounted units.

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 Installation Methods

The OpenScape Business X5R communication system can be mounted in a 19" rack, on a wall or as a standalone unit (desktop operation).

4.1.1 How to Mount OpenScape Business X5R in a 19-inch Rack

Prerequisites

The prerequisites for selecting the installation site were taken into account (see Prerequisites for the Installation on page 28).

The cabinet-specific screws required for attaching the support and angle brackets to the 19-inch rack are available (These must be provided by the 19-inch rack supplier).

Step by Step

1) Attach the two supplied angle brackets to the sides of the communication system using the two screws provided for each bracket.

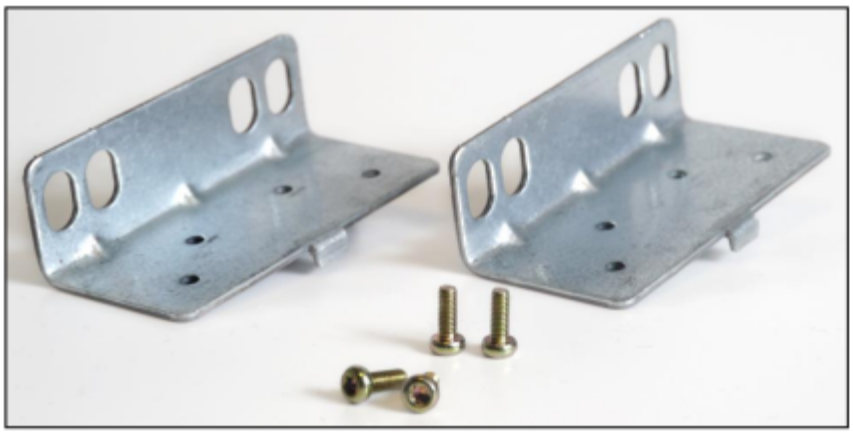


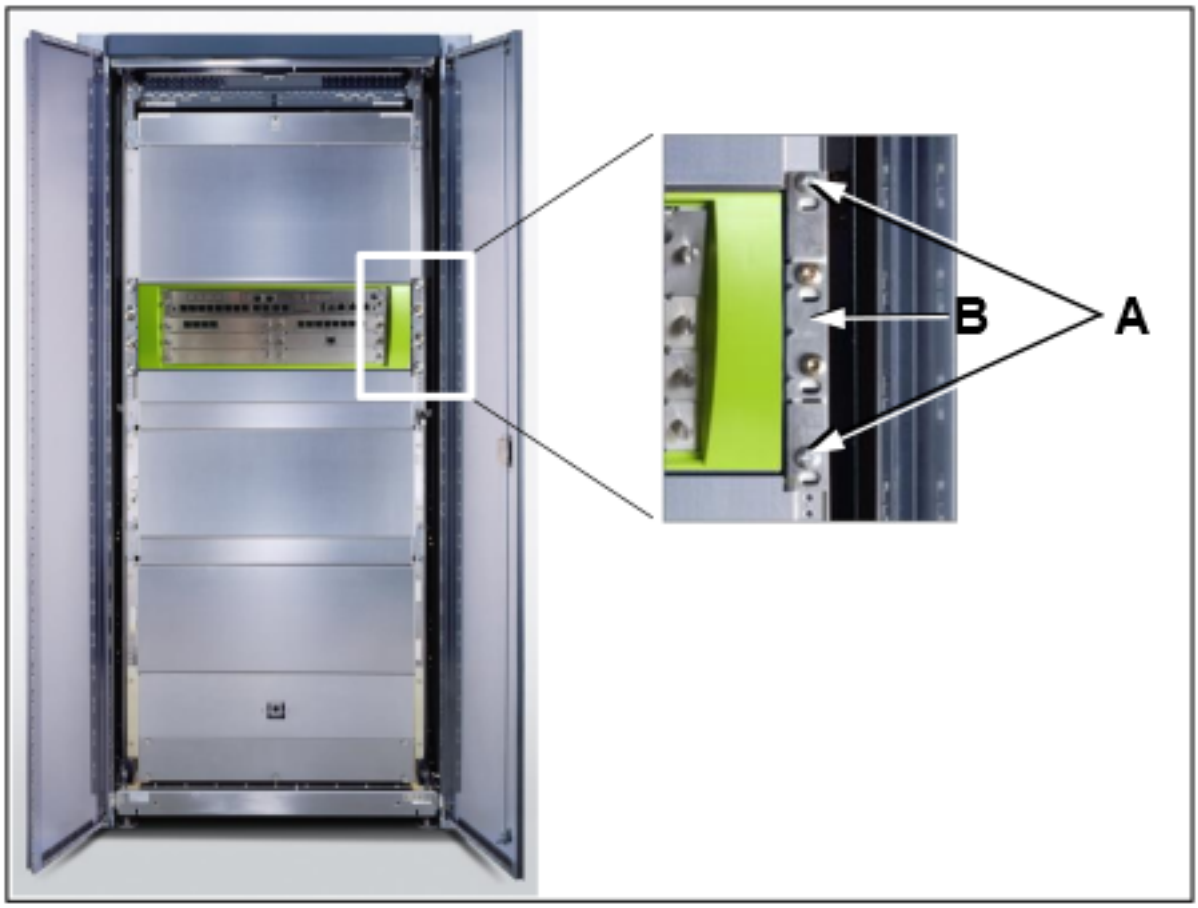
Figure 2: OpenScape Business X5R – Angle Brackets

2) Mount a right and a left support bracket (included with the 19 inch rack mounting kit (C39165-A7027-D1)) to the 19-inch rack with the screws provided for this purpose.

Figure 3: OpenScape Business X5R – Support Brackets

3) Lift the communication system into the 19-inch rack and place it on the two support brackets [A]. Slide the communication system into the 19-inch rack until the two brackets are flush with the front of the 19-inch frame.

4) Use the two angle brackets [B] and the screws provided to attach the communication system to the 19-inch rack.



4.1.2 How to Mount the Communication System to a Wall

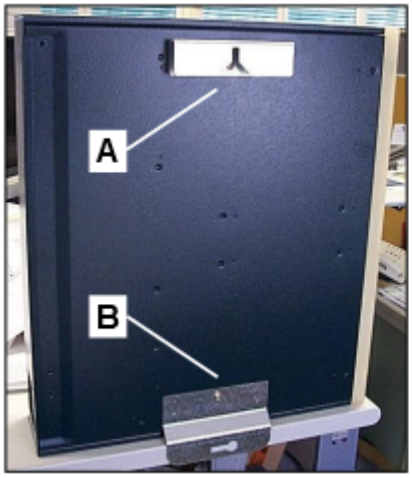
Prerequisites

The prerequisites for selecting the installation site were taken into account (see Prerequisites for the Installation on page 28).

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

Step by Step

1) Attach the two angle brackets [A] and [B] of the wall mount kit C39165-A7027-D2 to the underside of the communication system housing using the supplied screws.



2) Drill a hole for the top angle bracket [A].
3) Insert a wall anchor into the drilled hole and screw in a screw, leaving approx. 2 mm projecting.
4) Hang the communication system with the upper angle bracket [A].
5) Drill a hole for the bottom angle bracket [B].
6) Insert a wall anchor into the drilled hole and secure the bottom angle bracket [B] with a screw.

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.

WARNING:

Risk of electric shock through contact with live wires

- Use separate ground wires to provide protective grounding for the OpenScape Business X5R communication system. Before you start up the system and connect the phones and phone lines, connect the communication system with a permanent earthing conductor.
- Make sure that the ground wire laid is protected and strain-relieved.

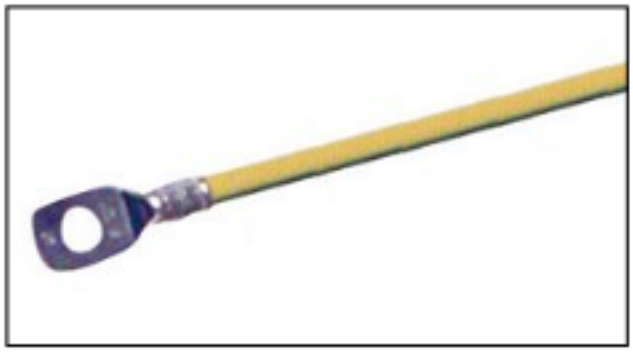
4.2.1 Protective Grounding for 19” Rack-mount Installations

The equipotential bonding strip of the 19’’ rack is used to provide protective grounding for the communication system.

4.2.1.1 How to Provide Protective Grounding for the Communication System

Prerequisites

A protective ground wire with a minimum cross section of 12 AWG/2.5 mm^2 and a ring terminal exists (see figure below). 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.



A low-impedance ground connection is available.

The 19-inch rack is grounded by a separate ground conductor (green/yellow). The 19-inch rack is equipped with an equipotential bonding strip at which the communication system can be separately grounded.

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

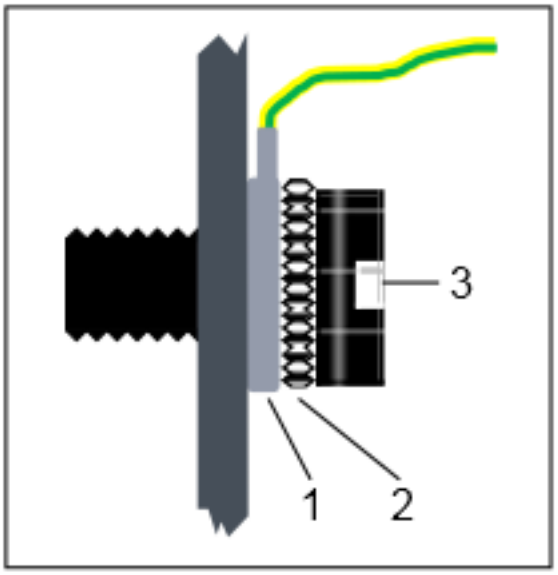
- Use separate ground wires to provide protective grounding for the OpenScape Business X5R communication system. Before you start up the system and connect the phones and phone lines, connect the communication system with a permanent earthing conductor.
- Make sure that the ground wire laid is protected and strain-relieved.

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:

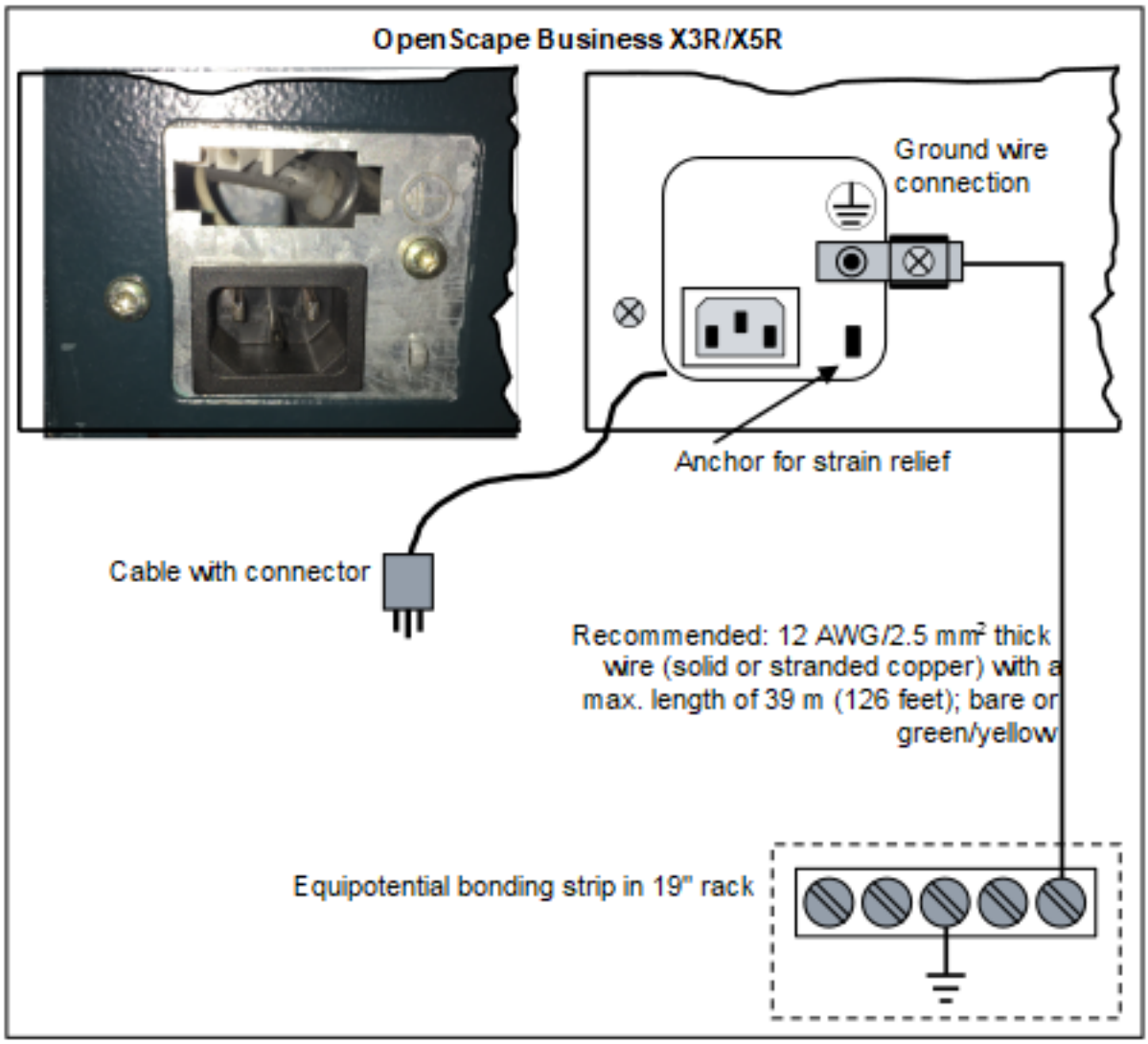
Step by Step

1) Attach the ring terminal [1] of the separate ground wire as shown in the figure using a tooth lock washer [2] and an M4 screw [3] to the protective conductor of the communication system.



2) Secure the ground wire with a cable tie to the appropriate fastening eyelet for strain relief.

3) Connect the ground wire with the equipotential bonding strip in the 19-inch rack as shown in the conceptual diagram in the figure below.



Make sure that the ground wire is protected and strain-relieved (minimum conductor cross section = 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.

4.2.1.2 How to Check the Grounding

Prerequisites

The communication system and all other devices in the 19-inch rack are not connected to the low-voltage network via power cables.

The communication system has been properly grounded using a separate ground wire.

The 19-inch rack is grounded by a separate ground conductor (green/yellow).

Run the following test before startup to make sure that the communication system's protective grounding is working properly.

Step by Step

Check the ohmic resistance on the ground connection to the communication system:

a) The first measurement is taken between the ground contact of a grounded power outlet of the home installation and the equipotential bonding strip in the 19-inch rack.
b) The second measurement is taken between the equipotential bonding strip in the 19-inch rack and the housing of the communication system.

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

If you obtain some other measurement 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.

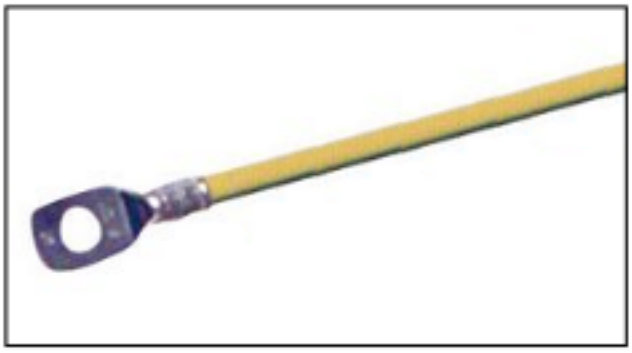
4.2.2 Protective Grounding for Wall-Mount and Standalone Installations

The protective grounding of the communication system occurs via the equipotential bonding strip of the building, an additional outlet to the low-voltage network, a main ground busbar or a ground field, for example.

4.2.2.1 How to Provide Protective Grounding for the Communication System

Prerequisites

A protective ground wire with a minimum cross section of 12 AWG/2.5 mm^2 and a ring terminal exists (see figure below). 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. When using an additional junction box of the low-voltage network, the minimum conductor cross-section may also be 16 AWG/1.5 mm^2.



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

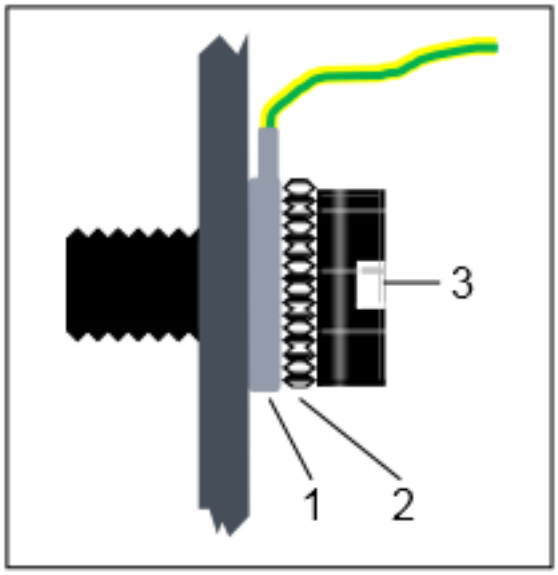
- Use separate ground wires to provide protective grounding for the OpenScape Business X5R communication system. Before you start up the system and connect the phones and phone lines, connect the communication system with a permanent earthing conductor.
- Make sure that the ground wire laid is protected and strain-relieved.

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 the ring terminal [1] of the separate ground wire as shown in the figure using a tooth lock washer [2] and an M4 screw [3] to the protective conductor of the communication system.

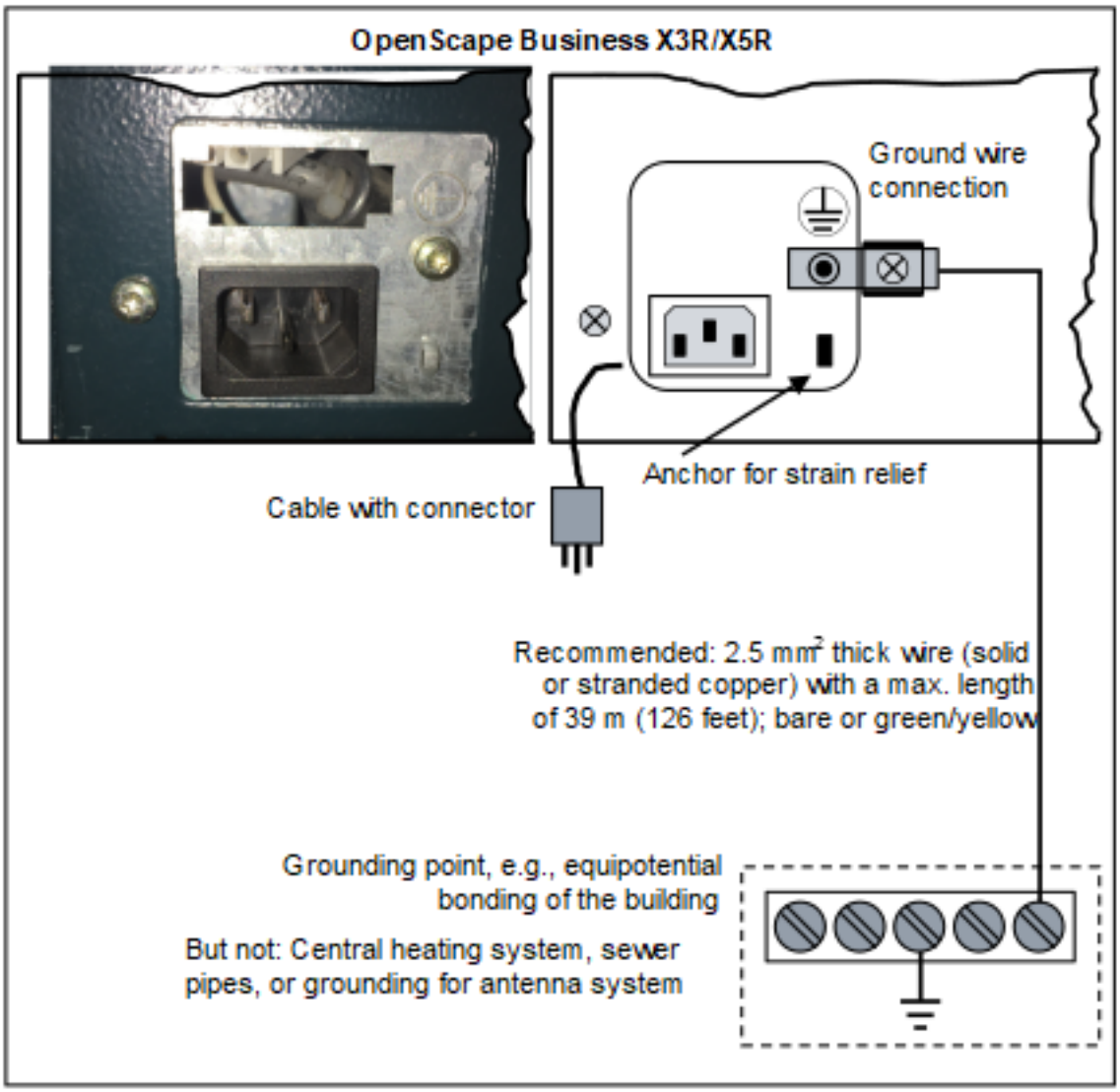


2) Secure the ground wire with a cable tie to the appropriate fastening eyelet for strain relief.

3) Select one of the following options:

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

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

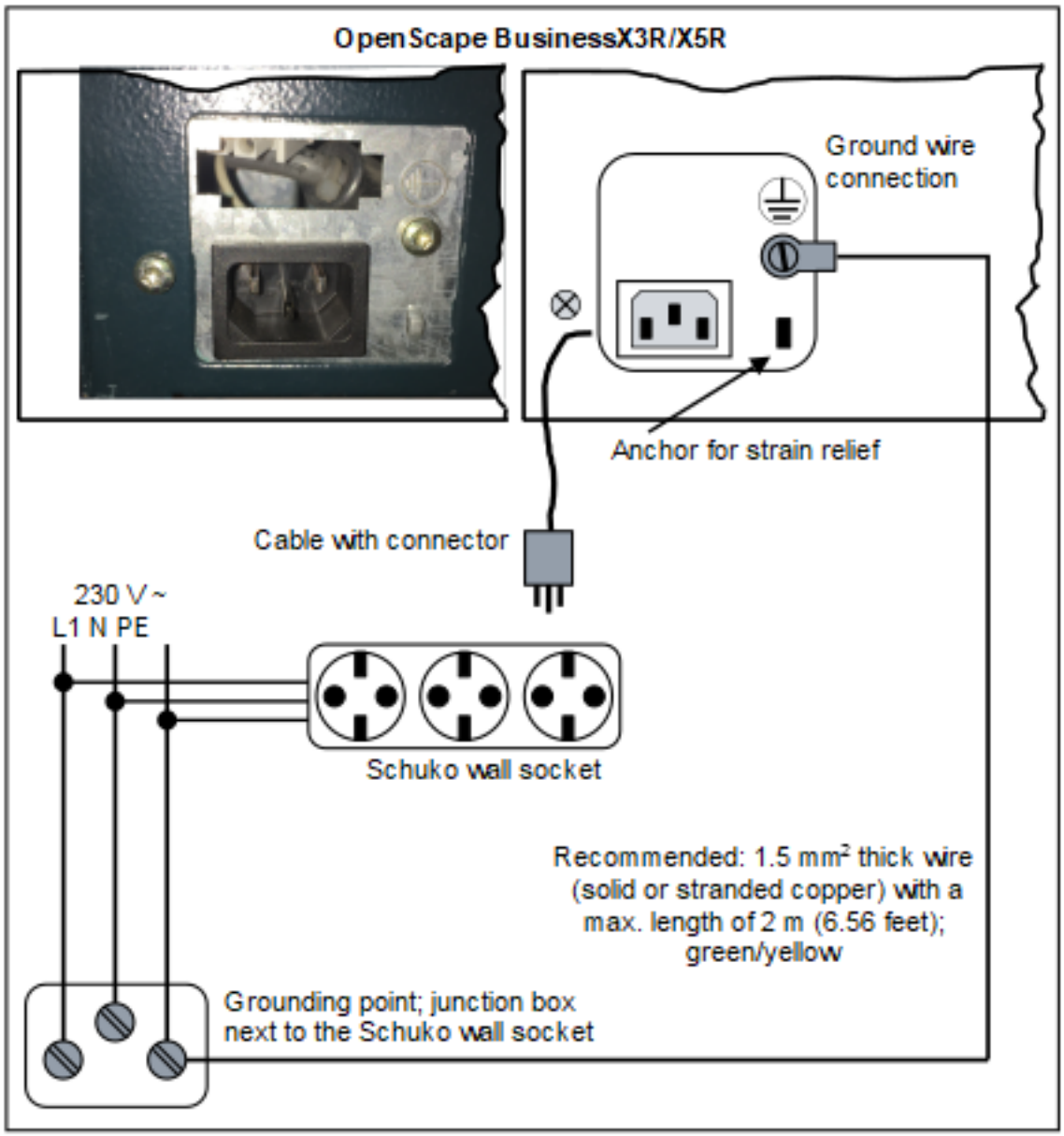


  Make sure that the ground wire is protected and strain-relieved. The minimum conductor cross section equals 12 AWG/2.5 mm^2). A minimum conductor cross section of 10 AWG/4 mm^2 is needed to block the effects of external factors if the ground wire cannot be protected.

- **Not for U.S. and Canada - Outlet to 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.

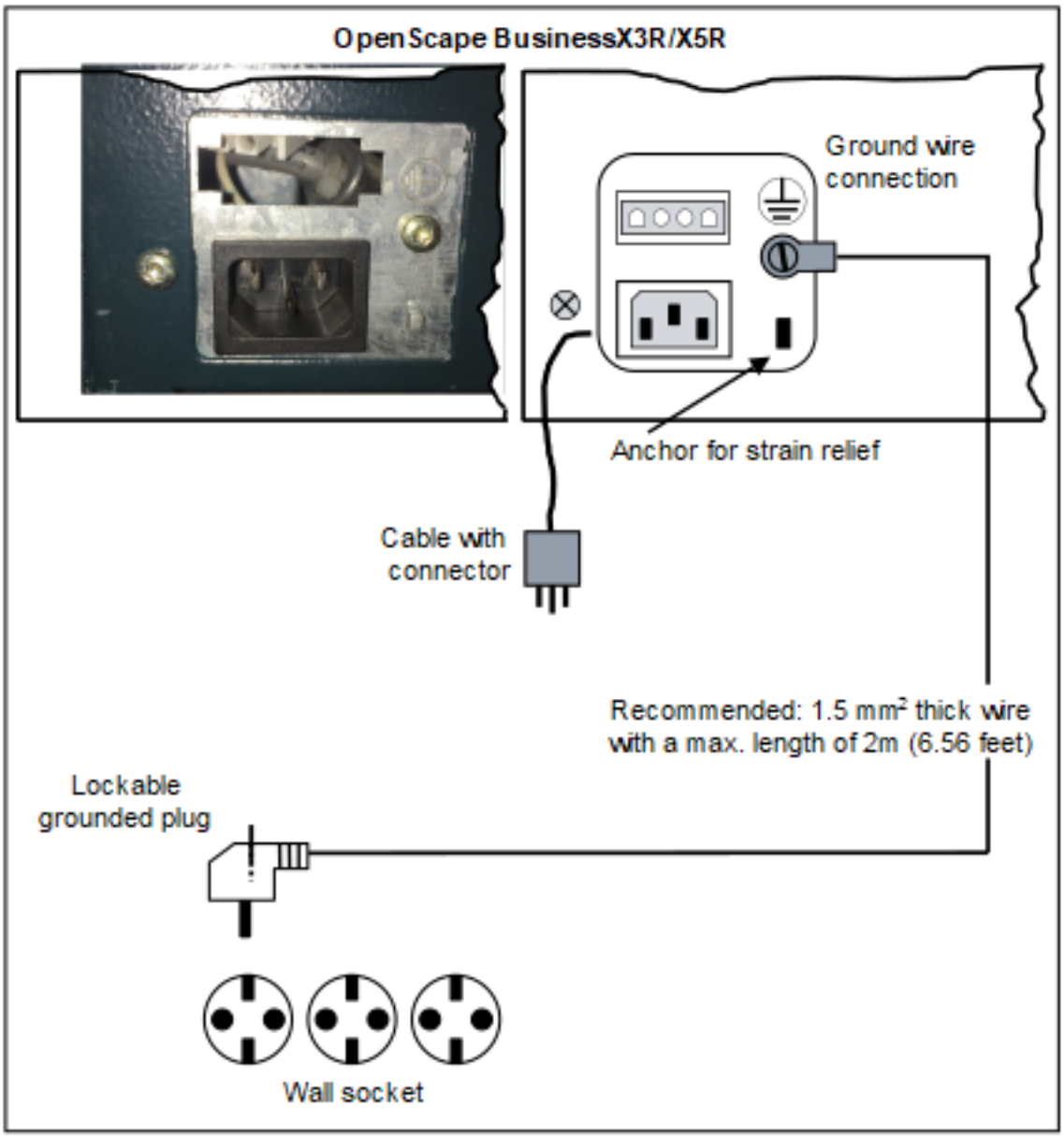


Make sure that the ground wire is protected and strain-relieved. The minimum conductor cross section is 16 AWG/1.5 mm^2.

- **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

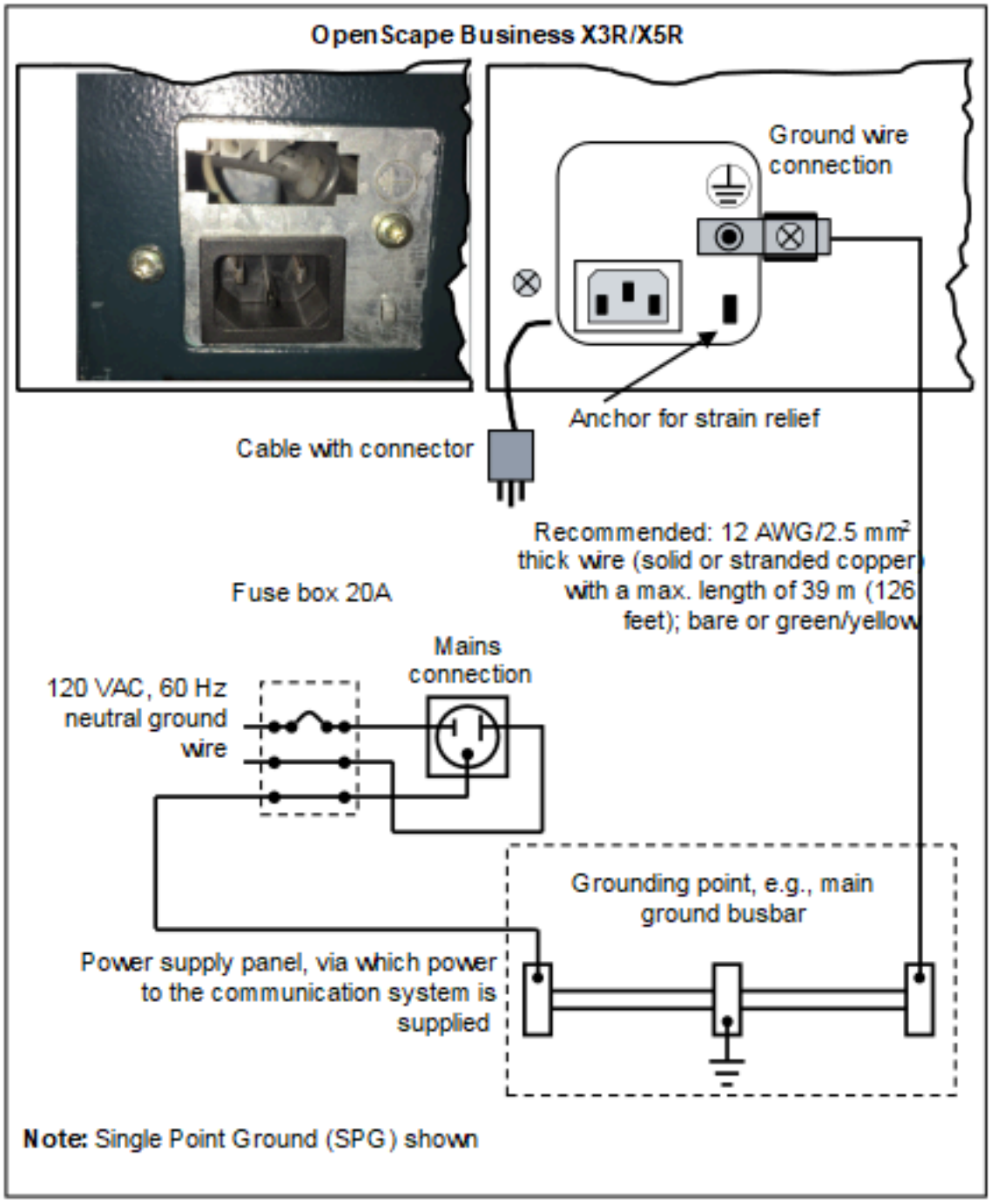
diagram. Use a second lockable grounded plug for a possibly existing MDFU.



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 ground wire 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.

4.2.2.2 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 has been properly grounded using a separate ground wire.

Run the following test before startup to make sure that the communication system's protective grounding is working properly.

Step by Step

Check the ohmic resistance on the 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.

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 Configuration Notes

The configuration notes include information about the board slots of the OpenScape Business X5R communication system.

4.3.1 Board Slots in OpenScape Business X5R

OpenScape Business X5R has five slot levels for the installation of boards and options.

- Slot levels 1 through 3: each slot level provides slots for two peripheral boards
- Slot level 4: slot for the OCCMR mainboard
- Slot level 5: slots for three options

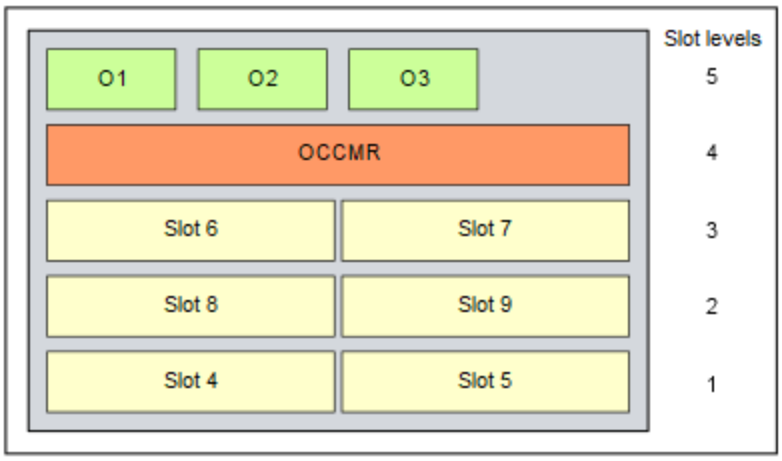


Figure 4: OpenScape Business X5R Board Slots

4.3.2 Board Installation

4.3.2.1 How to Insert a Board

Prerequisites

A free board slot is available.

NOTICE: Always wear an antistatic wristband when handling boards.

The ESD measures for protecting electrostatically sensitive devices must be observed and followed (see Warnings: Note on page 15)

Step by Step

1) Loosen the two locking screws for the shielding panel of the desired board slot.
2) Remove the shielding cover.
3) Using its guide rails slide the board into the board slot until it stops.
4) Attach the board to the housing using the two locking screws.

4.3.2.2 How to Remove a Board

Prerequisites

NOTICE: Always wear an antistatic wristband when handling boards.

The ESD measures for protecting electrostatically sensitive devices must be observed and followed (see Warnings: Note on page 15)

Step by Step

1) Loosen the two locking screws in the front panel of the board to be removed.
2) Pull out the board from the board slot.

4.3.2.3 How to Install a Shielding Cover

To ensure sufficient shielding, all empty board slots must be provided with a shielding panel.

Step by Step

1) Place the shielding cover on the empty board slot.
2) Attach the shielding cover to the housing using the two locking screws.

4.4 Trunk Connection

The OpenScape Business X5R communication system offer different options for trunk connections and thus for access to the public communication network.

You can select the trunk connection or connections required for your communication system from the following options:

- ISDN point-to-point connection and ISDN point-to-multipoint connection via S_0 interface (not for U.S. and Canada)
- Only for OpenScape Business X5R: ISDN Primary Rate Interface via S_{5M} interface (not for U.S. and Canada)
- Only for OpenScape Business X5R: ISDN Primary Rate Interface via T1 interface (for U.S. and Canada only)
- Only for OpenScape Business X5R: Trunk connection with CAS protocol via CAS interface (for selected countries only)
- Analog trunk connections

4.4.1 Not for U.S. and Canada: How to Set up an ISDN Point-to-Point or ISDN Point-to-Multipoint Connection via the S_0 Port

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for your communication system 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.

At least one free S_0 port is available (mainboard OCCMR, OCCMRA, OCCMRB or peripheral board STLSX4R, STLS4R).

During startup, the S_0 interface must be configured as an ISDN point-to-point or ISDN point-to-multipoint connection.

An ISDN point-to-point or point-to-multipoint connection is available.

Step by Step

Connect the desired S_0 port with NTBA of the ISDN point-to-point or ISDN multipoint connection.

4.4.2 Not for U.S. and Canada: How to Set up an ISDN Primary Rate Interface via the S_{2M} Port

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for your communication system 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.

OpenScape Business X5R is equipped with one TS2RN board.

One ISDN Primary Rate Interface is available.

Step by Step

Connect the S_{2M} port with the NTPM the ISDN Primary Rate Interface.

4.4.3 For U.S. and Canada Only: How to Set up the ISDN Primary Rate Interface via the T1 Interface

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for your communication system 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.

OpenScape Business X5R is equipped with one TST1R board.

One Channel Service Unit (CSU) that is approved as per FCC Part 68 and that satisfies the ANSI directive T1.403 is available. The T1 interface must not be directly connected to the PSTN (Public Switched Telephone Network). It is essential that one CSU be installed between the communication system and the digital trunk connection. The CSU provides the following features for OpenScape Business X5R: Isolation and overvoltage protection of the communication system, diagnostic options in the event of a malfunction (such as signal loopback, application of test signals and test patterns), line-up of the output signal in compliance with the line lengths specified by the network provider. A CSU is not a delivery component of the OpenScape Business X5R communication system.

One ISDN Primary Rate Interface is available.

Step by Step

Connect the T1 interface with the Channel Service Unit (CSU).

4.4.4 For Selected Countries Only: How to Set up a Trunk Connection via the E1-CAS Interface

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for your communication system 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.

OpenScape Business X5R is equipped with one TCASR-2 board.

A trunk connection with the CAS protocol is available.

Step by Step

Connect the required CAS interface of the TCASR-2 board with the NT of the trunk connection.

4.4.5 How to Set up an Analog Trunk Connection

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for your communication system 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 TLANI4R board 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 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.

The communication system is equipped with at least one TLANI4R board.

For the U.S. and Canada only: A protector as per UL 497A or CSA C22.2 No. 226 is available. The installation regulations require analog trunks to be connected using approved protectors as per UL 497A or CSA C22.2 No. 226.

An analog trunk connection with MSI (main station interface) signaling procedures (ground-start and loop-start signaling) is available.

Step by Step

Connect the desired a/b port of the desired board with the TAE socket of the analog trunk connection.

4.5 Connection of phones and devices

The OpenScape Business X5R communication system offer different options for connecting phones and devices.

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

- Direct connection of ISDN phones (not for U.S. and Canada)
- Connection of ISDN phones via the S_0 bus (not for U.S. and Canada)
- Connection of $U_{P0/E}$ phones
- Connection of analog phones and devices

NOTICE: Only one analog device can be connected to an a/b interface.

4.5.1 Not for U.S. and Canada: How to Connect ISDN Phones Directly

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for your communication system 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

Only for the station connection interfaces: In the case of line lengths exceeding 500 m and where the lines exit the building, the OCCMR, STLSX4R and STLS4R boards 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 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.

At least one free S_0 port is available (mainboard OCCMR or peripheral board STLSX4R, STLS4R).

The S_0 ports used must be configured at startup as an internal S_0 connection.

The ISDN phones to be connected must have a separate power source, e.g., via a power adapter. It is not possible to obtain power via the S_0 ports of the OCCMR, OCCMRA, OCCMRB, STLSX4R and STLS4R boards.

Step by Step

1) Connect the desired S_0 port with the ISDN telephone.

INFO:

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

2) If present, connect any further ISDN phones to the communication system by the same method.

4.5.2 Not for U.S. and Canada: How to Connect ISDN Phones via the S_0 Bus

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for your communication system 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

Only for the station connection interfaces: In the case of line lengths exceeding 500 m and where the lines exit the building, the OCCMR, OCCMRA, OCCMRB, STLSX4R and STLS4R boards 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 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.

At least one free S_0 port is available (mainboard OCCMR, OCCMRA, OCCMRB or peripheral board STLSX4R, STLS4R).

The S_0 ports used must be configured at startup as an internal S_0 connection.

The ISDN phones to be connected must have a separate power source, e.g., via a power adapter. It is not possible to obtain power via the S_0 ports of the OCCMR, OCCMRA, OCCMRB, STLSX4R and STLS4R boards.

Every individual ISDN phone (ISDN stations) must be assigned a unique Multiple Subscriber Number (MSN). This assignment must be made in the configuration menu of the ISDN station.

Step by Step

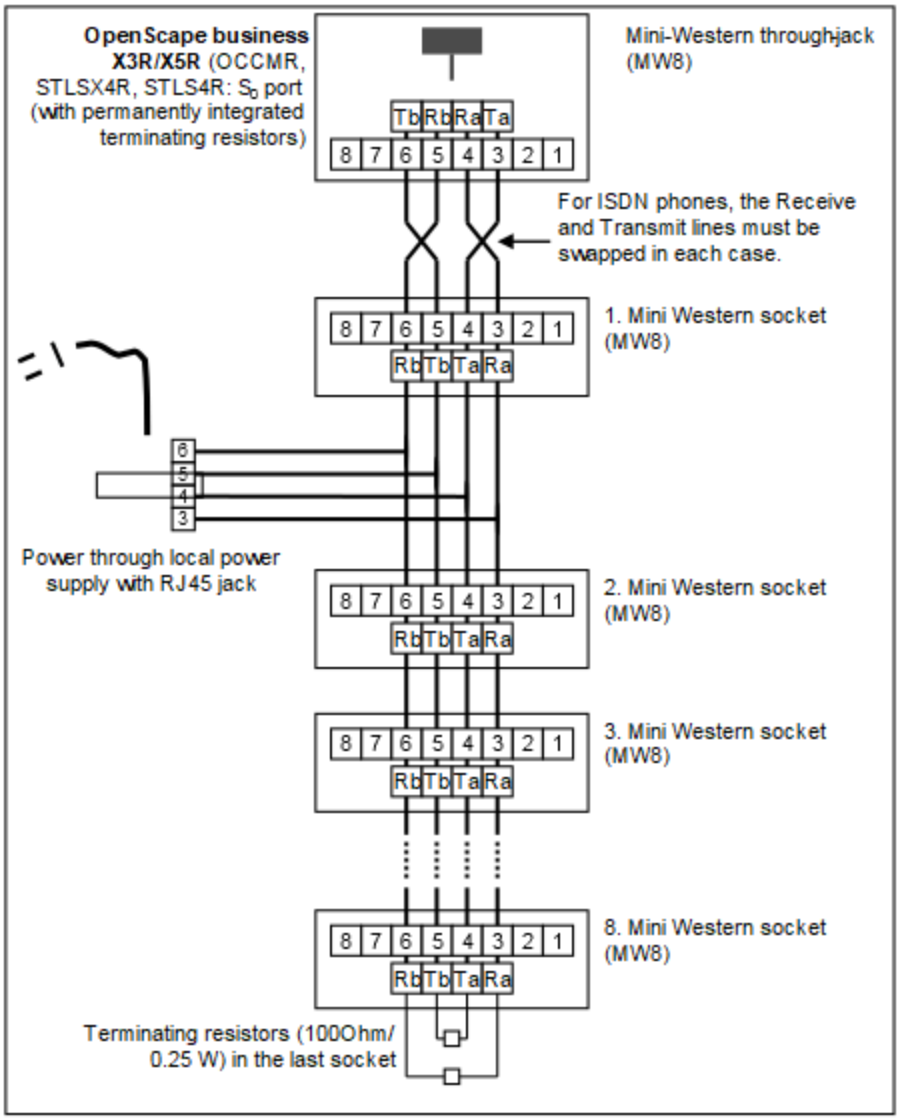
1) Connect the desired S_0 port with the Mini Western socket of the S_0 bus.

INFO:

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

---

2) Complete the wiring as shown in the following diagram.



3) Install terminating resistors (100 Ohm/0.25 W) in the last socket of the S_0 bus.

4) Make sure that terminating resistors are only connected to the two ends of the S_0 bus. No terminating resistors are required for the other sockets of the S_0 bus.

INFO:

Since terminating resistors are already integrated into OpenScape Business X5R, the communication system forms one end of an S_0 bus.

INFO:

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

4.5.3 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 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 OCCMR, OCCMRA, OCCMRB and SLU8NR boards 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 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.

At least one free $U_{P0/E}$ port is available (mainboard OCCMR, OCCMRA, OCCMRB or peripheral board SLU8NR).

Step by Step

1) Connect the desired $U_{P0/E}$ port with the $U_{P0/E}$ phone.

INFO:

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

2) If present, connect any further $U_{P0/E}$ phones to the communication system by the same method.

4.5.4 How to Connect Analog Telephones and Devices

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for your communication system 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 OCCMR, OCCMRA, OCCMRB, SLAV8R and SLAv16R boards 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 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.

At least one free a/b port is available (mainboard OCCMR, OCCMRA and OCCMRB or peripheral board SLAV8R, SLAV16R).

Step by Step

1) Connect the desired a/b port to be connected to the analog telephone or analog device (fax, modem, TFE-S, etc.).

INFO:

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

2) If present, connect any further analog phones or devices to the communication system by the same method.

4.6 Closing Activities

To complete the installation, the M.2 SSD or SDHC card must be inserted, a visual inspection must be performed, 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

---

4.6.1 How to Insert the M.2 SSD or the SDHC Card (system with OCCM)

The M.2 SSD or the SDHC card contains the OpenScape Business communication software and must be mounted/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.

4.6.2 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

Disconnect all power supply circuits of the communication system before starting to perform a visual inspection:

- Disconnect the line cords of any connected battery pack or any connected batteries.
- Disconnect the power plug of the communication system.

NOTICE: Always wear an antistatic wristband when handling boards.

The ESD measures for protecting electrostatically sensitive devices must be observed and followed (see Warnings: Note on page 15).

Step by Step

1) Disconnect all power supply circuits of the communication system.
2) Make sure that the communication system is de-energized.
3) Verify that the M.2 SSD or SDHC card is properly seated. The write protection of the SDHC card must be disabled (switch directed toward metal contacts).
4) Verify that all boards are secure.

   If requires, verify that the boards involved have been inserted properly (see How to Insert a Board).
5) Verify the presence of shielding covers at the empty board slots.

   If required, install the missing shielding covers (see How to Install a Shielding Cover).
6) 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.
7) Check whether a separate ground wire is connected to the communication system's ground terminal.

   If necessary, ground the communication system using a separate ground wire (see Protective Grounding for 19'' Rack-mount Installations and Protective Grounding for Wall-Mount and Standalone Installations).
8) Check whether the nominal voltage of the mains power supply corresponds to the nominal voltage of the communication system (type plate).

4.6.3 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 Installing the Hardware for OpenScape Business X8

This section covers the standard installation procedure for the OpenScape Business X8 communication system.

OpenScape Business X8 is a modular communication system that can be used as a one-box system (base box) or a two-box system (base box + expansion box). OpenScape Business X8 can be installed as a standalone unit or mounted in a 19-inch rack.

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.

5.1 Installation Methods

OpenScape Business X8 can be installed as a standalone unit or mounted in a 19-inch rack.

5.1.1 Standalone Installation

OpenScape Business X8 is a modular communication system that can be used as a one-box system (base box) or a two-box system (base box + expansion box). In a two-box system, the system boxes can either be stacked or set up side by side.

5.1.1.1 How to Set Up a One-Box System

Prerequisites

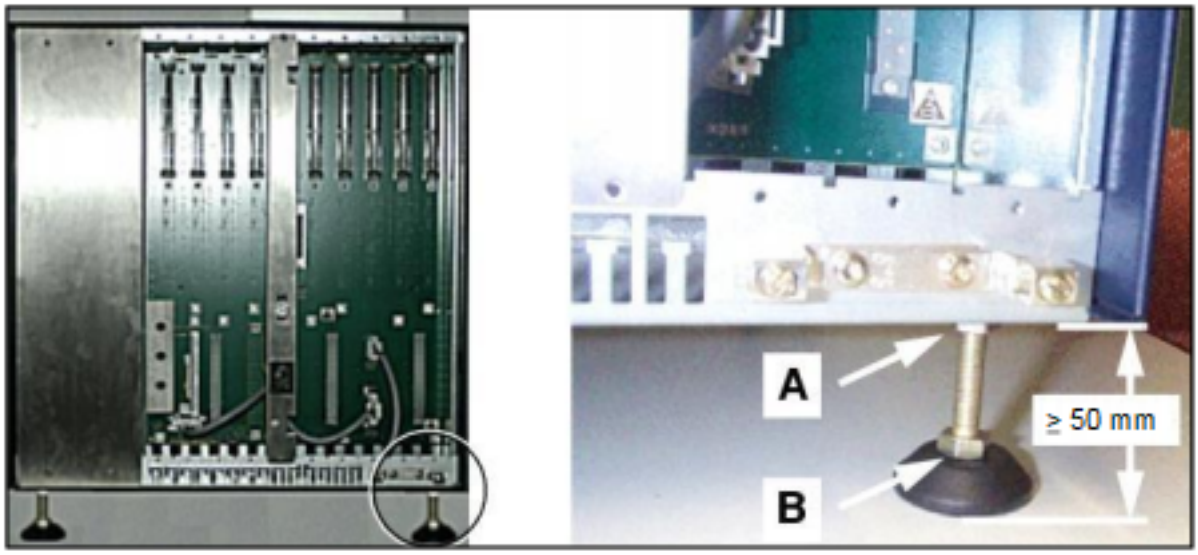
The prerequisites for selecting the installation site for a standalone installation were taken into account (see Prerequisites for the Installation on page 28).

The front and rear plastic covers are not attached to the system box.

Step by Step

1) Place the system box in the installation site and make sure that it is level and stable.
2) Check that the space between the base of the system box and the ground is at least 50 mm.

3) If necessary, set up the system box in the following way:
   a) Unscrew lock nut [A] on one of the feet using an open-end wrench (wrench size = 13 mm).
   b) Adjust the height of the foot by turning the screw nut [B] so that the system box is steady and the minimum clearance is observed.
   c) Fix the foot in position by tightening the lock nut [A].
   d) If necessary, repeat steps a through c for more feet until the system box is level and the minimum clearance is maintained.



5.1.1.2 Two-box System: How to Stack System Boxes

Prerequisites

The prerequisites for selecting the installation site for a standalone installation were taken into account (see Prerequisites for the Installation on page 28).

The front and rear plastic covers are not attached to the system boxes.

Step by Step

1) Place the base box at the installation site and make sure that it is level and stable.
2) Check that the space between the base of the base box and the ground is at least 50 mm.

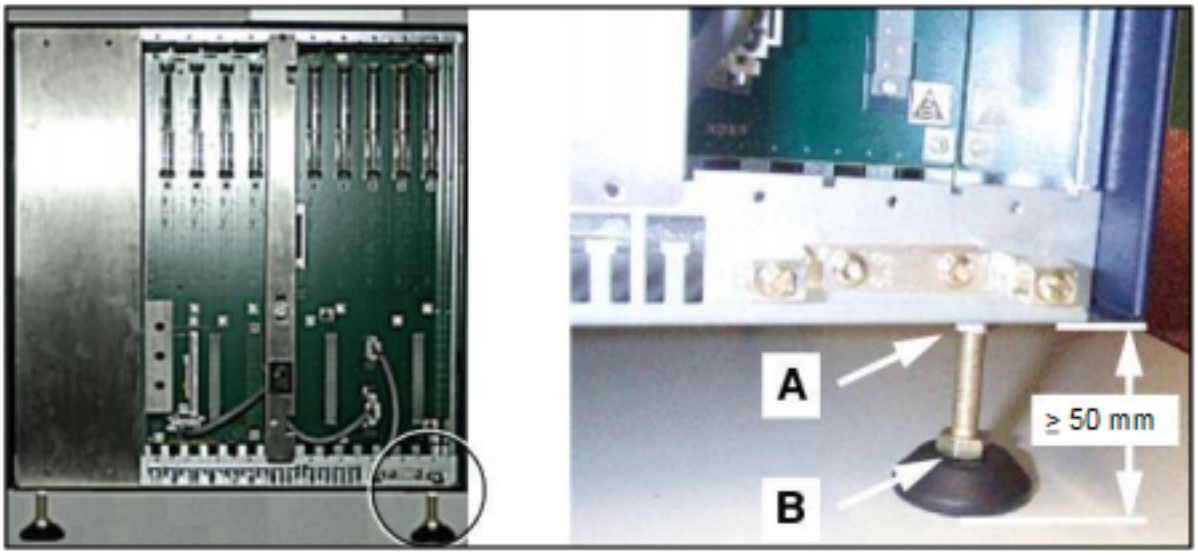
3) If necessary, set up the base box as follows:

a) Unscrew lock nut [A] on one of the feet using an open-end wrench (wrench size = 13 mm).

b) Adjust the height of the foot by turning the screw nut [B] so that the base box is steady and the minimum clearance is observed.

c) Fix the foot in position by tightening the lock nut [A].

d) If necessary, repeat steps a through c for more feet until the base box is level and the minimum clearance from the base box is maintained.



4) Place the expansion box on top of the base box.

The feet of system boxes are provided with recesses. When placing the expansion box on top of the base box, ensure that these recesses are placed precisely on top of the screw heads in the four corners of the base box.

5) Check that the space between the expansion box and the base box is at least 50 mm.

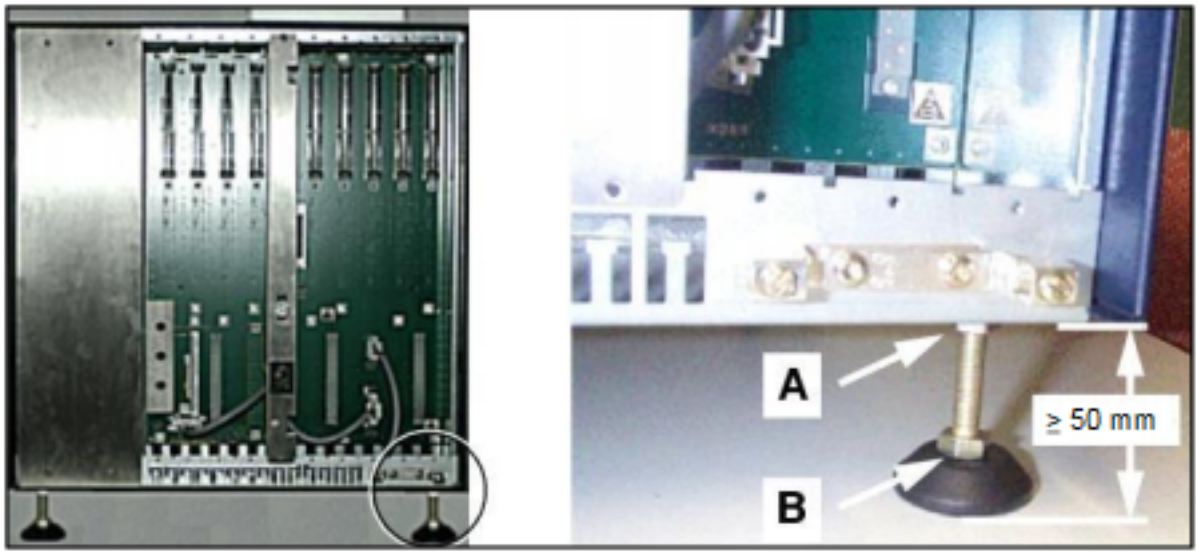
6) If necessary, set up the expansion box in the following way:

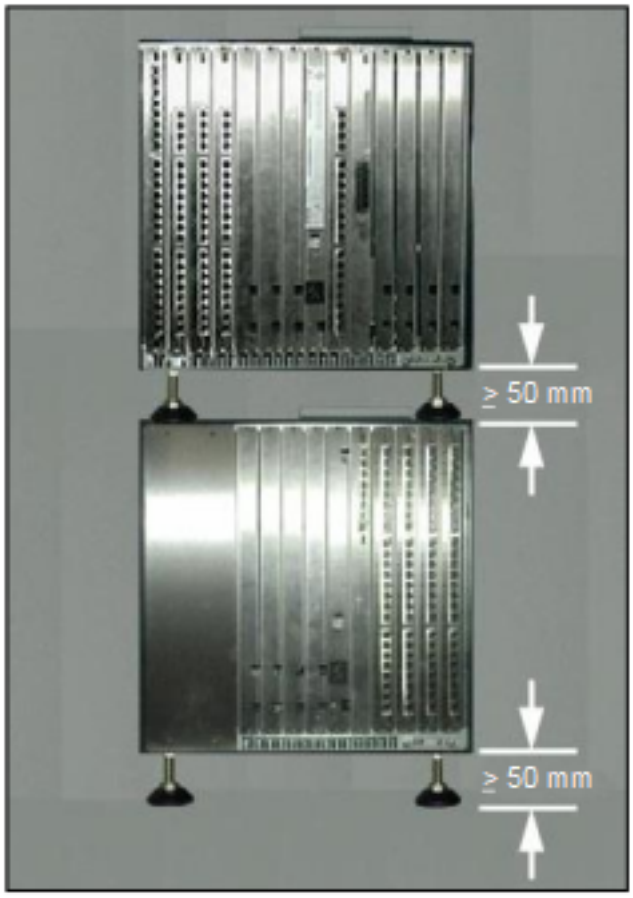
a) Unscrew lock nut [A] on one of the feet using an open-end wrench (wrench size = 13 mm).

b) Adjust the height of the foot by turning the screw nut [B] so that the expansion box is steady and the minimum clearance is observed.

c) Fix the foot in position by tightening the lock nut [A].

d) If necessary, repeat steps a through c for more feet until the expansion box is level and the minimum clearance from the base box is maintained.





5.1.1.3 Two-box System: How to Set Up the System Boxes Side by Side

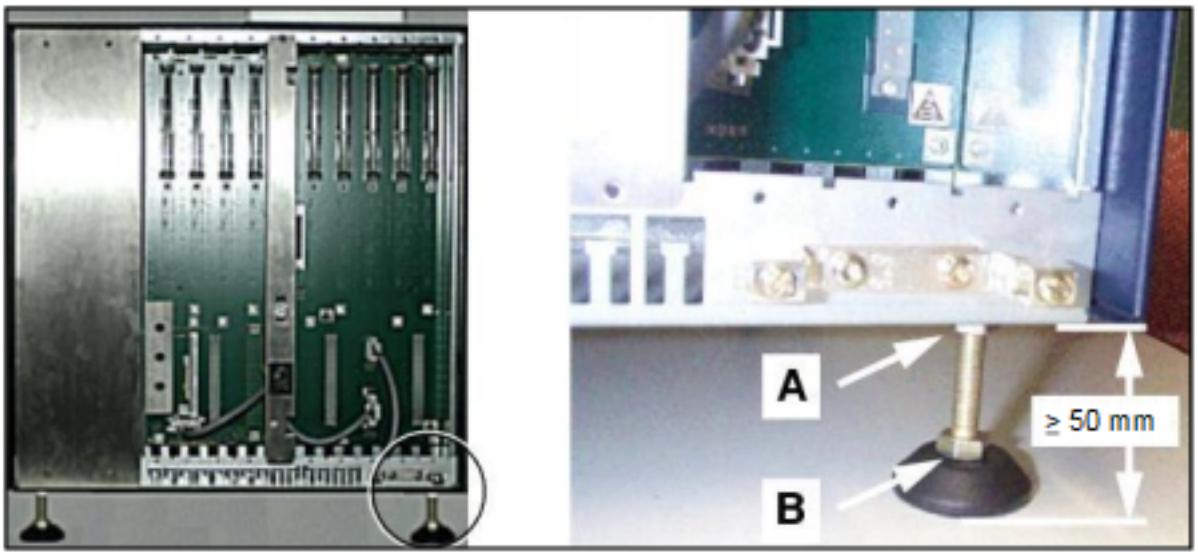
Prerequisites

The prerequisites for selecting the installation site for a standalone installation were taken into account (see Prerequisites for the Installation on page 28).

The front and rear plastic covers are not attached to the system boxes.

Step by Step

1) Place the base box at the installation site and make sure that it is level and stable.
2) Check that the space between the base of the base box and the ground is at least 50 mm.
3) If necessary, set up the base box as follows:
   a) Unscrew lock nut [A] on one of the feet using an open-end wrench (wrench size = 13 mm).
   b) Adjust the height of the foot by turning the screw nut [B] so that the base box is steady and the minimum clearance is observed.
   c) Fix the foot in position by tightening the lock nut [A].
   d) If necessary, repeat steps a through c for more feet until the base box is level and the minimum clearance from the base box is maintained.



4) Place the expansion box next to the base box.
5) Check that the space between the base of the expansion box and the ground is at least 50 mm.

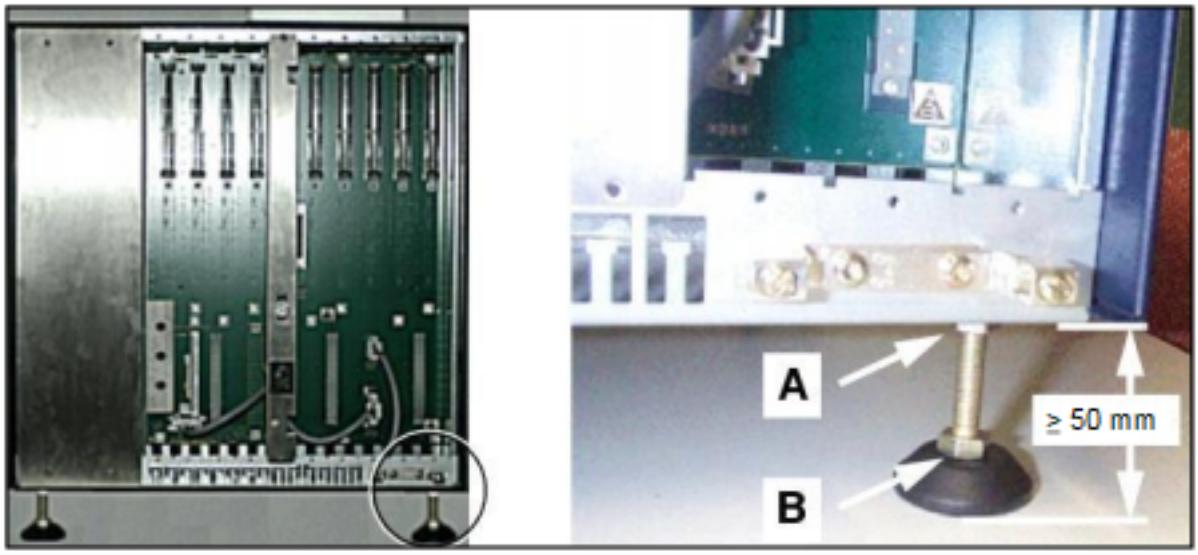
6) If necessary, set up the expansion box in the following way:

a) Unscrew lock nut [A] on one of the feet using an open-end wrench (wrench size = 13 mm).

b) Adjust the height of the foot by turning the screw nut [B] so that the expansion box is steady and the minimum clearance is observed.

c) Fix the foot in position by tightening the lock nut [A].

d) If necessary, repeat steps a through c for more feet until the expansion box is level and the minimum clearance is maintained.



5.1.2 19” Rack-mount Installation

OpenScape Business X8 is a modular communication system that can be mounted as a one-box system (base box) or a two-box system (base box + expansion box) in a 19-inch rack.

5.1.2.1 How to Mount a System Box in a 19-inch Rack

Prerequisites

The prerequisites for selecting the installation site for a 19” rack-mount installation were taken into account (see Prerequisites for the Installation on page 28).

The front and rear plastic covers are not attached to the system box.

Two cabinet-specific support brackets (with an ultimate load > 40 kg) are available. These must be provided by the 19-inch cabinet supplier).

NOTICE: The use of cabinet floors is not permitted to prevent overheating.

The cabinet-specific screws required for attaching the support and angle brackets to the 19-inch rack are available.

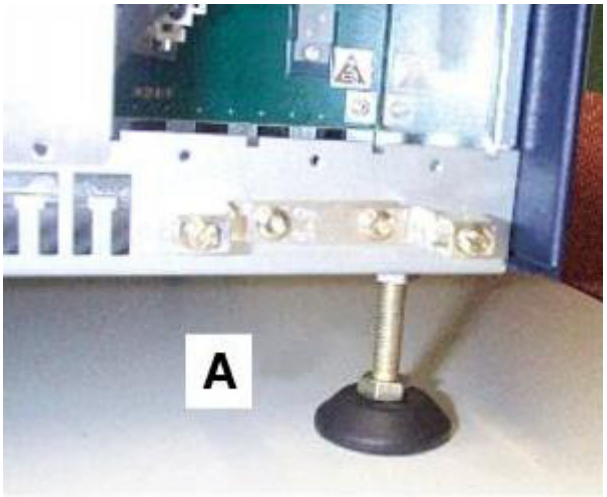
Step by Step

1) Remove the four feet of the system box:

a) Unscrew lock nut [A] on one of the feet using an open-end wrench (wrench size = 13 mm).

b) Unscrew the foot completely.

c) Repeat steps a and b for the remaining three case feet.



2) Attach the two supplied angle brackets [B] to the sides of the system box using the screws provided.

3) Attach a right-handed and a left-handed support bracket [C] to the 19-inch rack using the screws provided.

4) Lift the system box into the 19-inch rack and place it on the the two support brackets [C]. Slide the system box into the 19-inch rack until the front edge of the system box is flush with the front of the 19-inch frame.

CAUTION: General risk of injury or accidents in the workplace

Never attempt to lift a system box into a 19-inch rack without assistance.

---

5) Use the two angle brackets [B] and the screws provided to attach the system box to the 19-inch rack.

6) Repeat steps 1 through 6 if you want to install an expansion box.

5.2 Patch Panels (Optional)

For a 19'' rack-mount installation of the OpenScape Business X8 communication system, the telephones, trunks, etc., can be connected via the external patch panel.

Patch Panel S30807-K6143-X

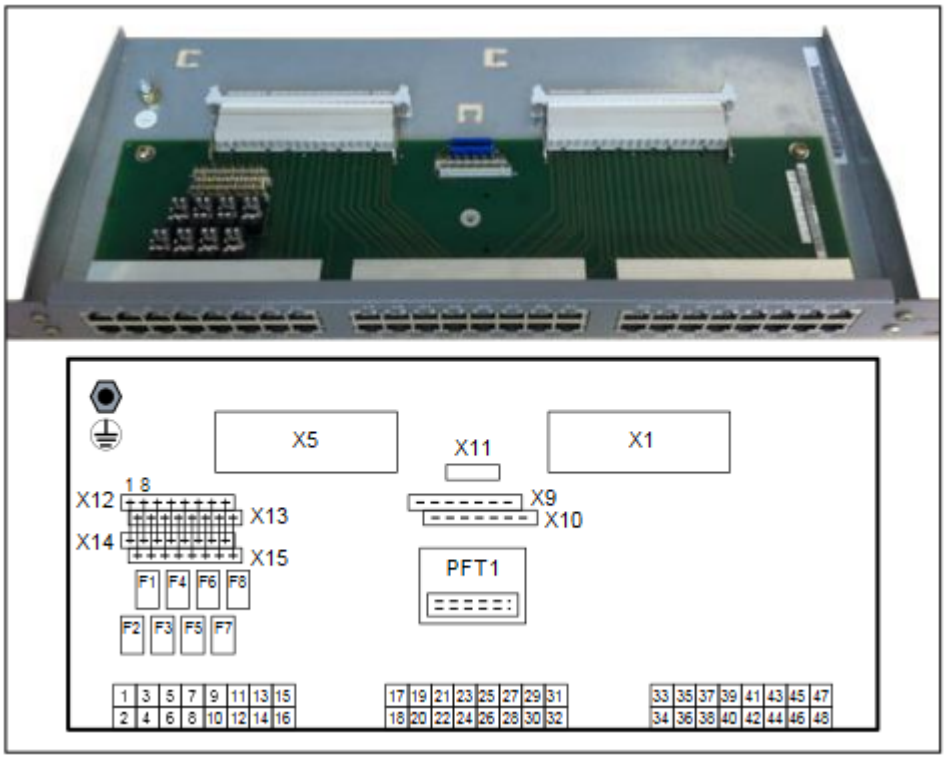


Figure 5: Patch Panel S30807-K6143-X

Main Features

- Two SIVAPAC connectors (X1, X5) for connection to the backplane of the communication system via CABLUs (prefabricated cabling units)

  Using jumper wire, bridges must be inserted between the terminal strips X12 and X14 and between the terminal strips X13 and X15. The contact between the SIVAPAC connector X5 and the first eight RJ45 jacks is only set up when wire bridges are present.

  When jumpering telephones, trunks, etc. directly to the terminal strips X12 and X13, no wire bridges are needed.
- 48 RJ45 jacks (1 to 48) for the connection of telephones, trunks, etc.

Table 1: Patch Panel S30807-K6143-X - Assignment of the RJ45 Jacks

Pin	Signal
4	a
5	b
The RJ45 jacks each have two wires.	

- Eight slots for surge arresters (ÜSAGs) (F1 to F8)

NOTICE:

Fire hazard due to surge voltage

In the case of line lengths exceeding 500 m and where the lines exit the building, analog and digital subscriber line modules 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.

INFO: X9, X10, X11 and PFT1 are not be used with OpenScape Business.

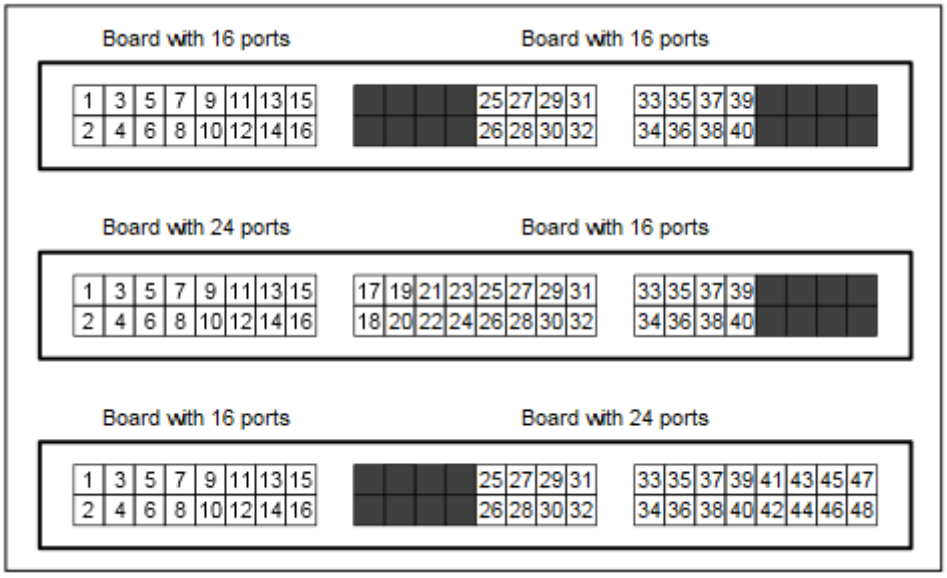


Figure 6: Patch Panel S30807-K6143-X – Usage of the 48 RJ45 Jacks

The above figure shows the use of the 48 RJ45 jacks depending on the number of interfaces of the connected peripheral boards.

S_0 Patch Panel C39104-Z7001-B3

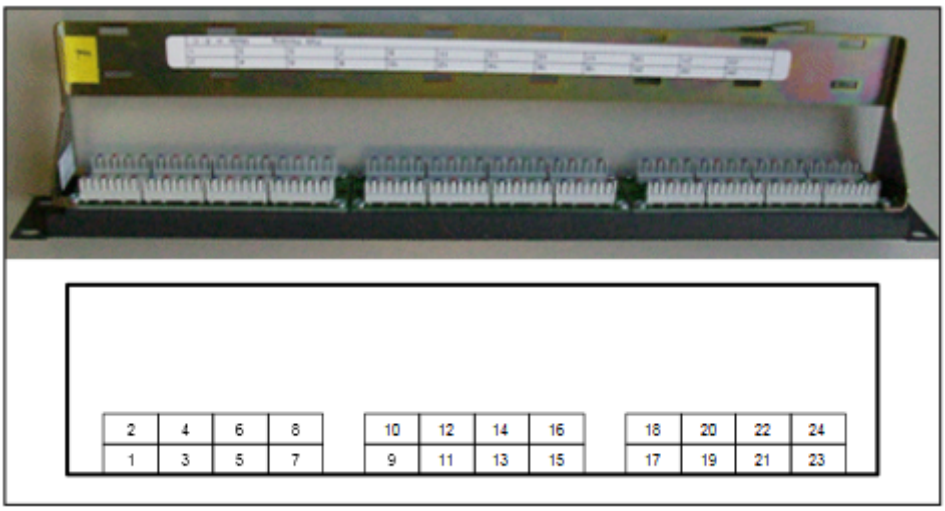


Figure 7: S_0 Patch Panel C39104-Z7001-B3

Main Features

- 24 RJ45 jacks (1 to 24) for the connection of ISDN telephones, ISDN trunks, etc.

  The connection to the backplane of the communication system is made via open-end cables which must be manually attached to the S_0 patch panel.

Table 2: S_0 Patch Panel C39104-Z7001-B3 - Assignment of the RJ45 Jacks

Pin	Signal	
	Trunk connection/ Networking	Station connection
3	Transmit +	Receive +
4	Receive +	Transmit +
5	Receive –	Transmit –
6	Transmit –	Receive –
Each of the RJ45 jacks must have four wires.		

NOTICE: If you use patch panels from a third-party vendor, you must observe the manufacturer's instructions for installation and protective grounding.

5.2.1 How to Mount a Patch Panel in a 19-inch Rack

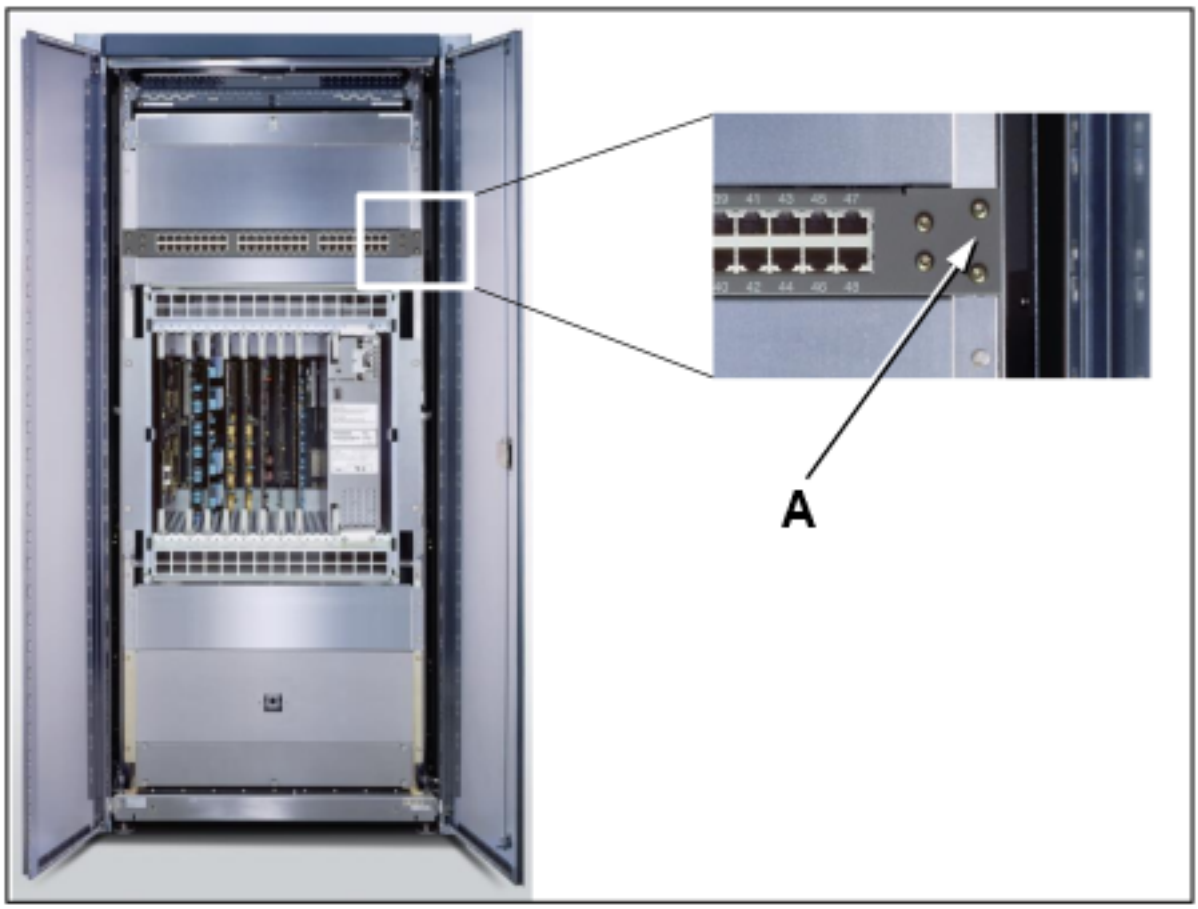
Prerequisites

The prerequisites for selecting the installation site for a 19” rack-mount installation were taken into account (see Prerequisites for the Installation on page 28).

Cabinet-specific screws for attaching the patch panel to the 19-inch' rack are available.

Step by Step

Lift the patch panel into the 19'' rack and attach it to the 19-inch rack with the screws [A] provided for this purpose.



5.3 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.

WARNING:

Risk of electric shock through contact with live wires

- Use separate ground wires to provide protective grounding for the system boxes of the OpenScape Business X8 communication system and possibly any main distribution frames and patch panels being used. Connect the system boxes of your communication system, your main distribution frame and your patch panels to the ground wire before starting up the system and connecting telephones and lines.
- Make sure that the ground wires are protected and strain-relieved (minimum conductor cross section = 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.

5.3.1 Protective Grounding for Standalone Installations

The system boxes of the communication system and any main distribution frames used are grounded via the equipotential bonding strip of the building, via a main ground busbar or via a ground field, for example.

5.3.1.1 How to Provide Protective Grounding for the Main Distribution Frame MDFU

Prerequisites

A ground connection with a resistance of less than 2 ohms exists. Examples: equipotential bonding strip of the building, main ground busbar, ground field

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 system boxes of the OpenScape Business X8 communication system and possibly any main distribution frames being used. Connect the system boxes of 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 are protected and strain-relieved (minimum conductor cross section = 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.

The grounding of the system boxes 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 ground terminal of the base box of the communication system as indicated in the following figure.

2) Provide strain relief for the ground wire by securing it to the base box with a cable tie.

3) Use a 12 AWG/2.5 mm^2 thick wire (solid or stranded copper) with a max. length of 39 meters (126 feet) to connect the ground terminal of the base box with the ground terminal of the main external distribution frame MDFU. To avoid confusion, you may use any color except green/yellow.

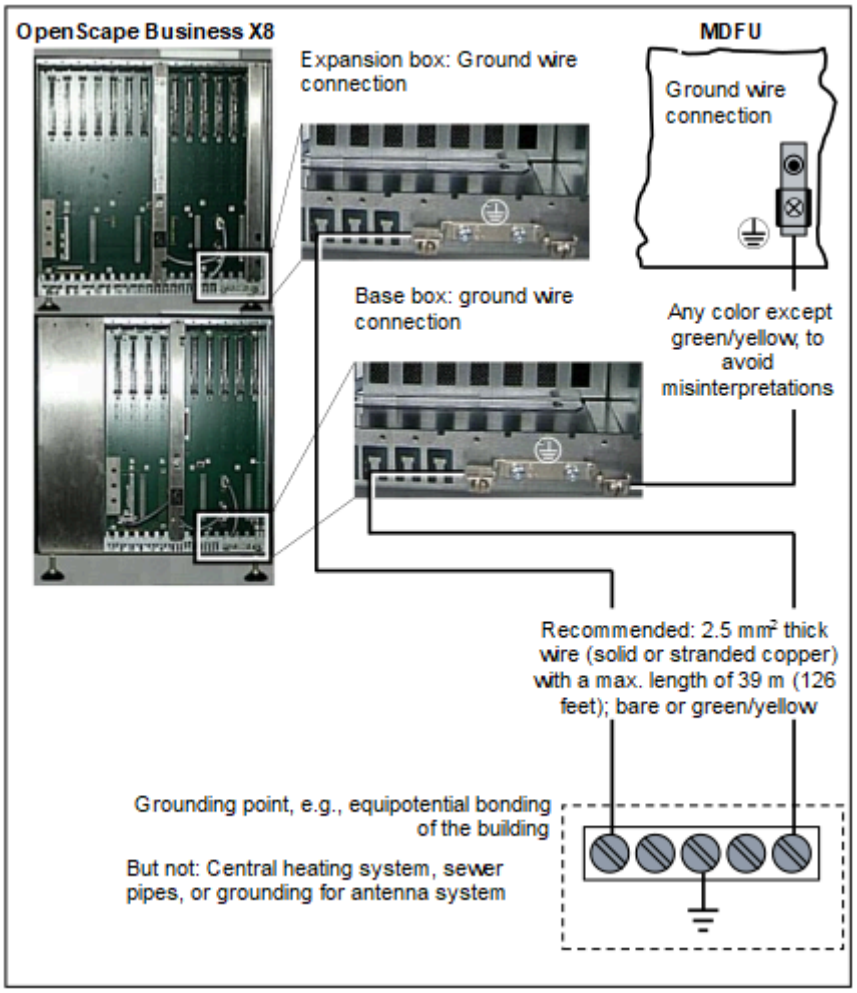
4) If an expansion box is present: Attach a separate ground wire to the ground terminal of the expansion box of the communication system.

5) If an expansion box is present: Provide strain relief for the ground wire by securing it to the expansion box with a cable tie.

6) Select one of the following options:

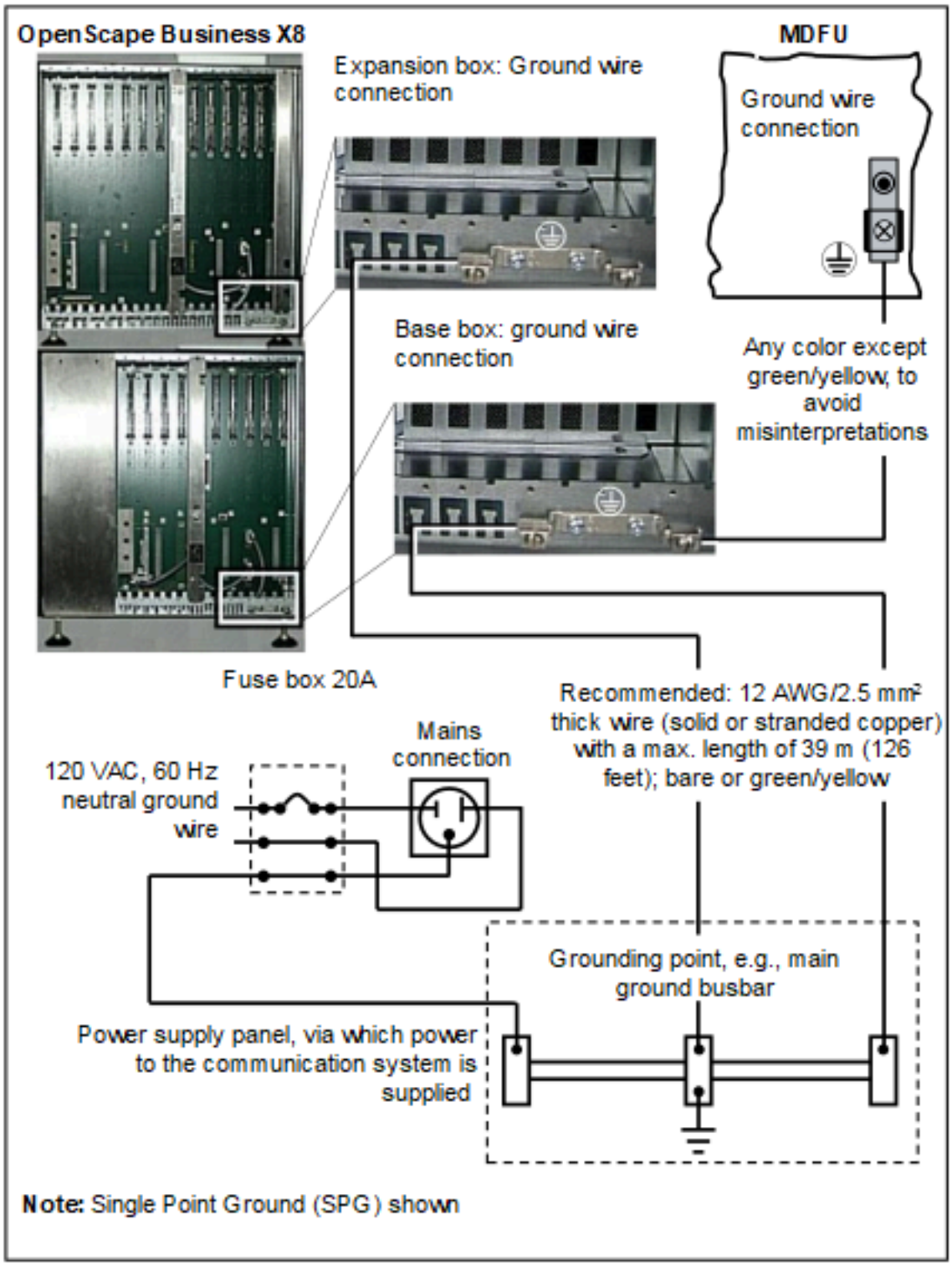
- **Not for U.S. and Canada:** Connect the separate ground wire(s) of the system box(es) with the grounding point (e.g., the equipotential bonding strip of the building) as illustrated in the conceptual diagram in the figure

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



- **For U.S. and Canada only:** Connect the separate ground wire(s) of the system box(es) with the grounding point (e.g., the main ground busbar,

ground field) as illustrated in the conceptual diagram in the figure below. Make sure that all ground wires laid are protected and strain-relieved.



5.3.1.2 How to Check the Grounding

Prerequisites

The system box or system boxes of the communication system are not yet connected to the low-voltage network via the power cable.

Each individual system box of the communication system as well as any main distribution frames 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 MDFs used is working properly.

Step by Step

1) Check the ohmic resistance on the 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 a system box of the communication system.
2) Repeat the measurement for all additional system boxes of the communication system.
3) Check the ohmic resistance between the system boxes of the communication system and the main distribution frame(s).

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

If you obtain some other measurement 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.

5.3.2 Protective Grounding for 19” Rack-mount Installations

The system boxes of the communication system and any patch panels used are grounded via the equipotential bonding strip of the 19’’ rack.

5.3.2.1 How to Provide Protective Grounding for the Communication System and the Patch Panel

Prerequisites

A ground connection with a resistance of less than 2 ohms exists. Examples: equipotential bonding strip of the building, main ground busbar, ground field

The 19-inch rack is grounded by a separate ground conductor (green/yellow). The 19-inch rack is equipped with an equipotential bonding strip at which the system boxes of the communication system and the patch panels can be separately grounded.

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 system boxes of the OpenScape Business X8 communication system and possibly any patch panels being used. Connect the system boxes of your communication system and your patch panels to the ground wire before starting up the system and connecting telephones and lines.
- Make sure that the ground wires are protected and strain-relieved (minimum conductor cross section = 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 a ground wire cannot be protected.

The grounding of the system boxes 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.

NOTICE:

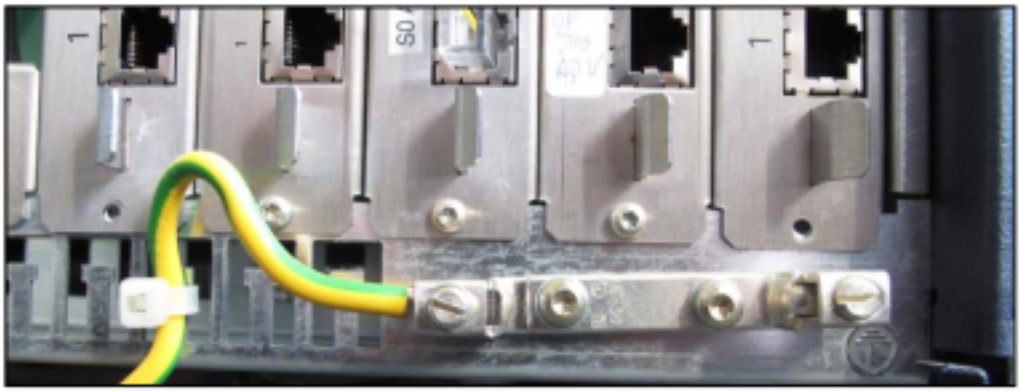
The listed requirements apply if you are using patch panels from another vendor.

A protective grounding of the S_0 patch panel (C39104-Z7001-B3) is not required.

Proceed as follows to ensure protective grounding:

Step by Step

1) Attach a separate ground wire to the ground terminal of the base box of the communication system as indicated in the following figure.



2) Provide strain relief for the ground wire by securing it to the base box with a cable tie.

3) Use a 12 AWG/2.5 mm^2 thick wire (solid or stranded copper) with a max. length of 39 meters (126 feet) to connect the ground terminal of the base box with the ground terminal of the patch panel (S30807-K6143-X). To avoid confusion, you may use any color except green/yellow.

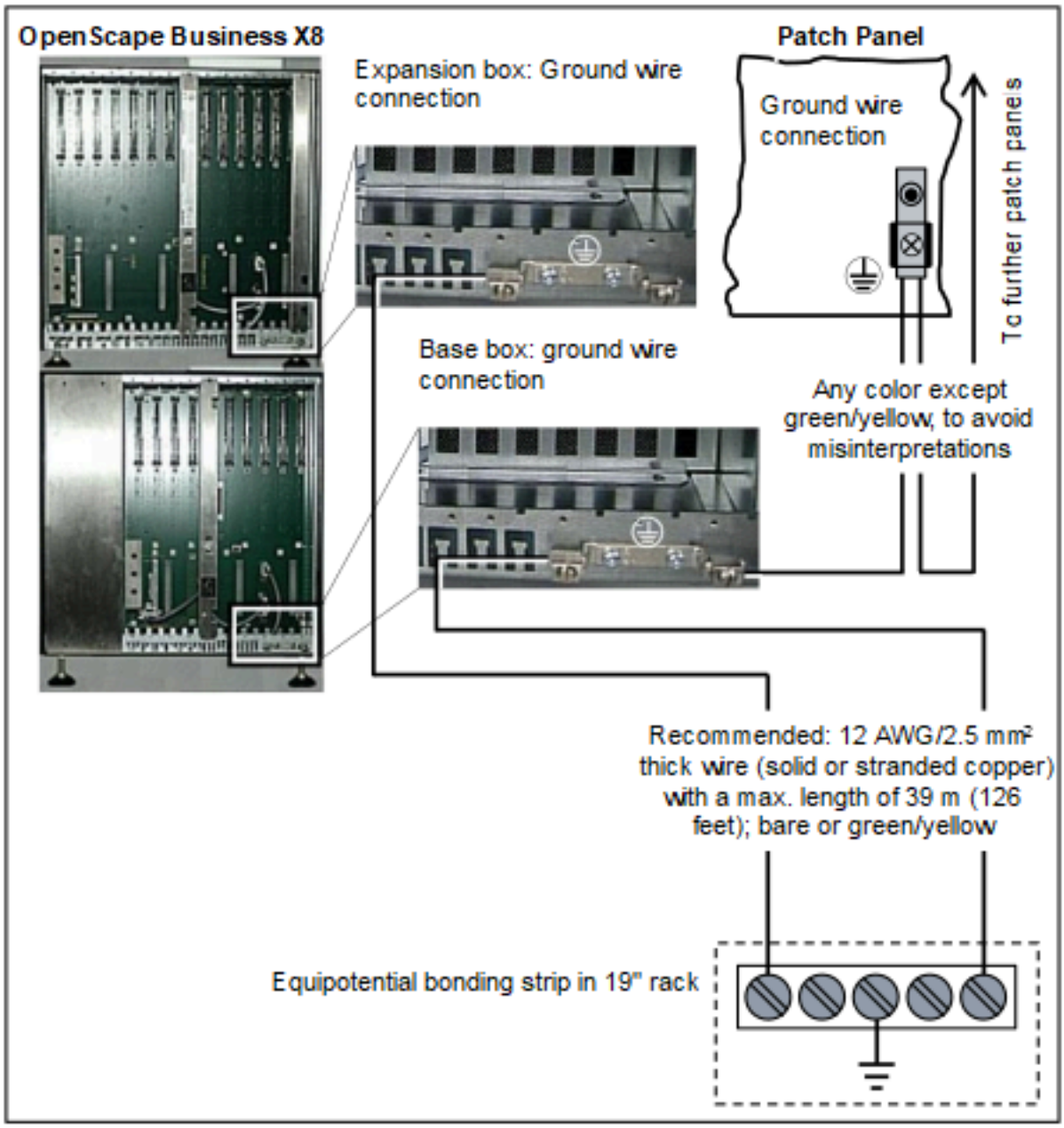
4) If an additional patch panel (S30807-K6143-X) is present: Use a 12 AWG/2.5 mm^2 thick wire (solid or stranded copper) with a max. length of 39 meters (126 feet) to connect the ground terminals of the patch panels with each other. To avoid confusion, you may use any color except green/yellow.

5) If an expansion box is present: Attach a separate ground wire to the ground terminal of the expansion box of the communication system.

6) If an expansion box is present: Provide strain relief for the ground wire by securing it to the expansion box with a cable tie.

7) Connect the separate ground wire(s) of the system box(es) with the equipotential bonding strip in the 19-inch rack as shown in the conceptual

diagram in the figure below. Make sure that all ground wires laid are protected and strain-relieved.



5.3.2.2 How to Check the Grounding

Prerequisites

The system box or system boxes of the communication system and all other devices in the 19-inch rack are not connected to the low-voltage network through power cables.

Each individual system box of the communication system as well as any patch panels have been properly grounded using separate ground wires.

The 19-inch rack is grounded by a separate ground conductor (green/yellow).

Run the following test before startup to make sure that the protective grounding for the communication system and the patch panels used is working properly.

Step by Step

1) Check the ohmic resistance on the ground connection to the communication system:
   a) The first measurement is taken between the ground contact of a grounded power outlet of the home installation and the equipotential bonding strip in the 19-inch rack.
   b) The second measurement is taken between the equipotential bonding strip in the 19-inch rack and a system box of the communication system.
   c) Repeat the second measurement for all additional system boxes of the communication system.

2) Check the ohmic resistance between the system boxes of the communication system and the patch panels.

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

If you obtain some other measurement 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.

5.4 Configuration Notes

The configuration notes include information on the board slots in the base box and expansion box, the initialization of the boards, the distribution of the PCM highways in the base box and the expansion box and the board installation.

5.4.1 Board Slots in the Base Box

The base box provides nine slots for peripheral boards (slots 1 to 5 and 7 to 10). A fixed slot is assigned to the OCCL or OCCLA mainboard (slot 6). Depending on your requirements, up to three LUNA2/LUNA3 power supply units can be used in the base box.

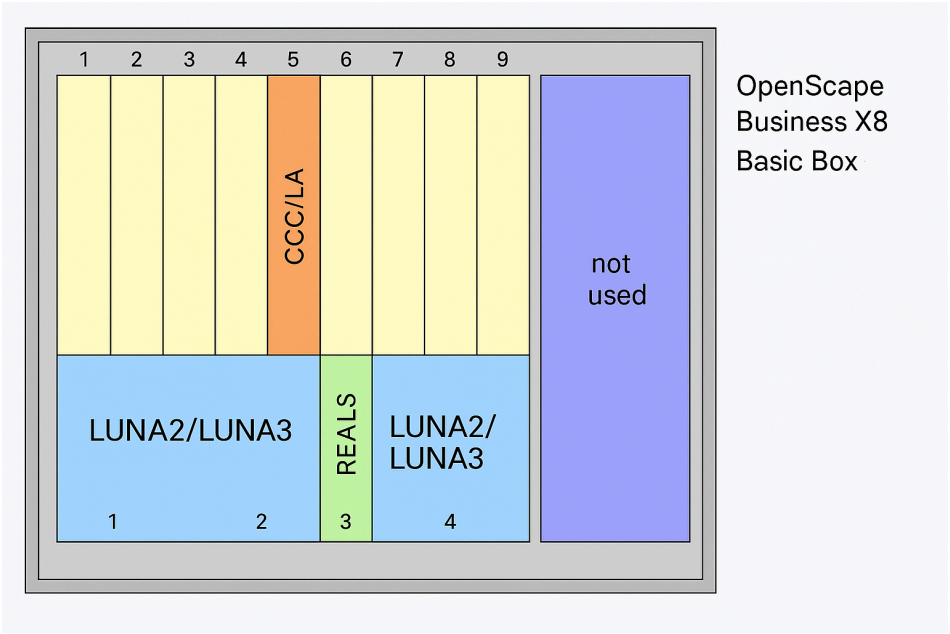


Figure 8: OpenScape Business X8 – Board Slots in the Base Box

5.4.2 Board Slots in the Expansion Box

The expansion box provides thirteen slots for peripheral boards (slots 1 to 6 and 8 to 14). Depending on your requirements, up to four LUNA2/LUNA3 power supply units can be used in the expansion box.

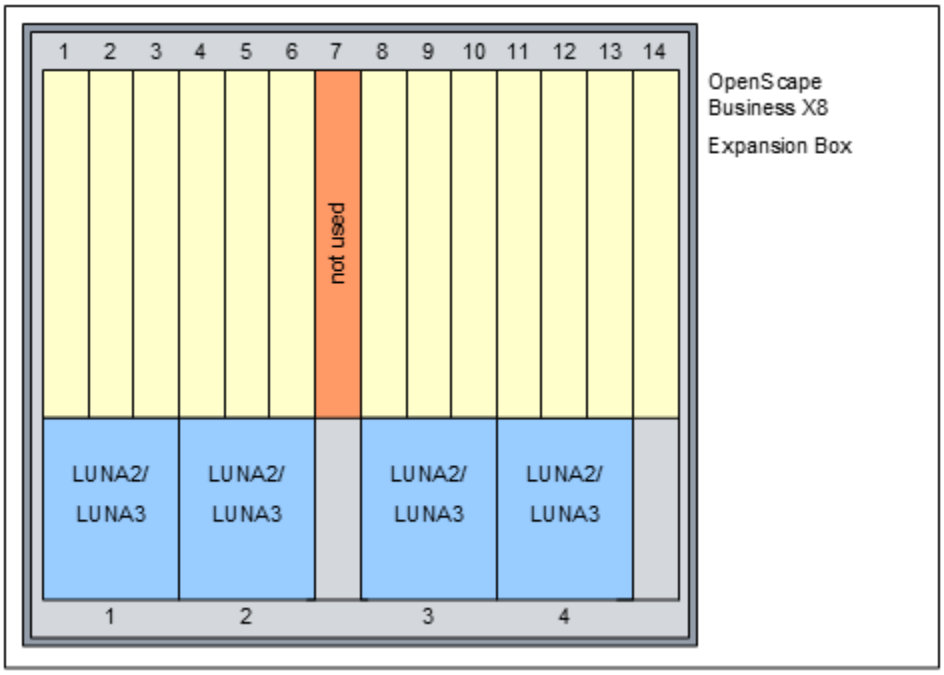


Figure 9: OpenScape Business X8 – Board Slots in the Expansion Box

5.4.3 Special Board Slots

The following boards are used in special slots.

DBSAP

The DBSAP board is part of the expansion box shipment and is plugged into the corresponding backplane connector of the expansion box by factory.

LUNA2/LUNA3

The slots for the LUNA2/LUNA3 are located in the lower part of the shelf of a system box. The base box has three slots and the expansion box has four slots.

NOTICE:

LUNA2/LUNA3 may only be plugged in or out when the system is switched off (switch position = DC-OFF).

The slots of the power supply units must be covered with outer panels before the communication system is started up.

REALS

The slot for the REALS board is located in the lower part of the shelf of the base box.

The slots of the power supply units and the slot of the REALS board must be covered with outer panels before the communication system is started up.

For more detailed information, see the relevant board description.

5.4.4 Initializing the Boards

The system software detects and initializes the boards in ascending order, starting with the lowest installation position the first time the system starts up.

The board interfaces are initialized in the sequence indicated by the arrow in the following figure.

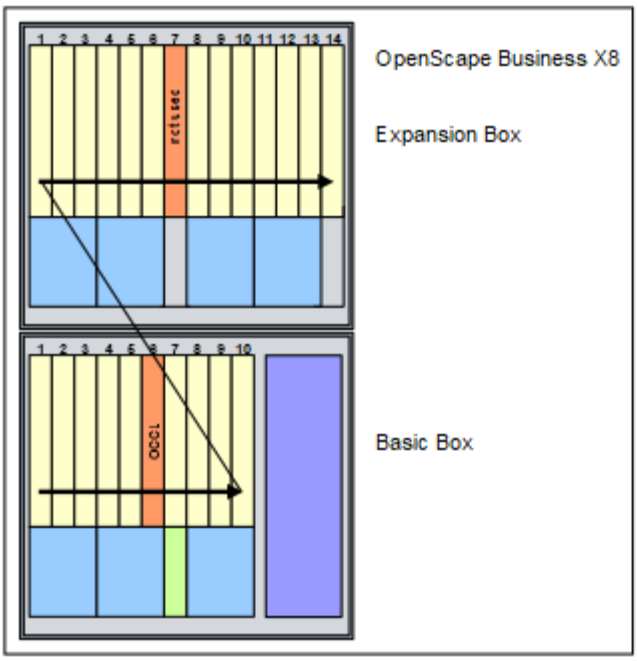


Figure 10: OpenScape Business X8 - Initialization of the Boards

The system activates all connected boards in the following situations:

- The maximum configuration of the communication system has not yet been reached.

  While sequentially scanning the slots, the system software checks whether the maximum number of stations or trunks has been exceeded. If it has, the board is not activated.
- At least one B channel is available for the slot in the case of trunk boards.

  Only the number of B channels available in the communication system is put into operation.

5.4.5 Distribution of the PCM Highways in the Base Box

The base box provides two PCM highway trunk groups with 2 x 4 PCM highways for each peripheral board slot. There are 32 time-division multiplex channels available for each PCM highway. If all of these channels are busy, no further call requests can be accepted.

To guarantee that the system operates without blocking, make sure when performing the configuration that the boards on a PCM segment do not require more than the number of time-division multiplex channels available.

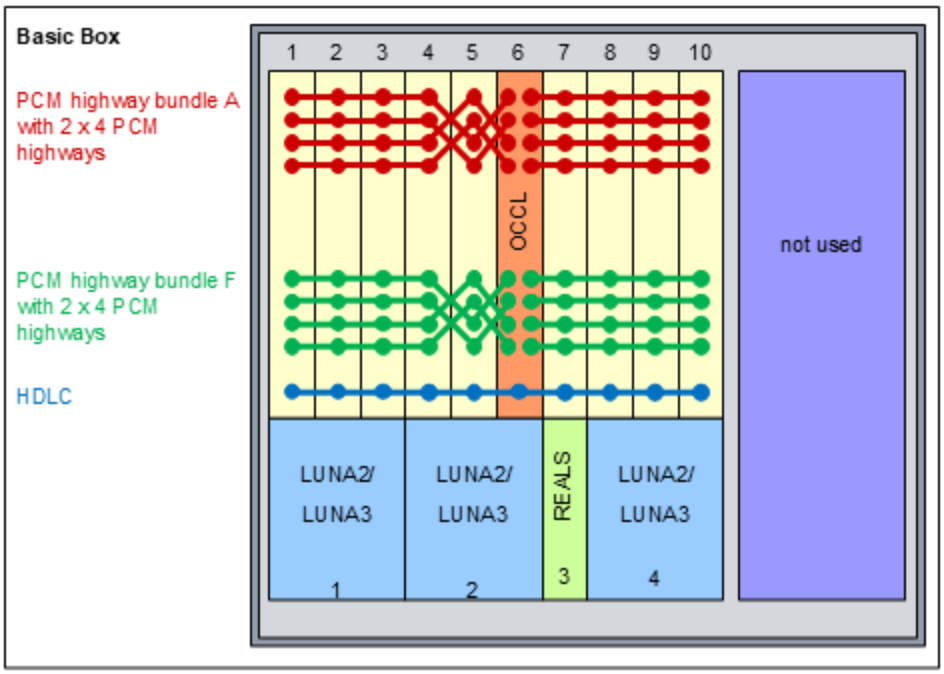


Figure 11: OpenScape Business X8 – PCM Highways in the Base Box

The PCM highway bundles in the base box are used by peripheral boards according to the following rules:

- One-box System
  - Bundle A's PCM highway

    With the exception of boards DIUT2, DIUN2 and DIU2U, the peripheral boards only use the PCM highways of trunk group A.

    128 time-division multiplex channels (4 PCM highways) are available on the PCM segment for board slots 1 to 5 and on the PCM segment for board slots 7 to 10.
  - PCM highway trunk group F

    The peripheral boards DIUT2, DIUN2 and DIU2U use the PCM highways of trunk group F.

    128 time-division multiplex channels are thus available for these boards on the PCM segment for board slots 1 to 5 and on the PCM segment for board slots 7-10.

    If more than the 2 x 128 time-division multiplex channels from PCM highway trunk group F are required because of the configuration with these boards, the communication system will automatically resort to time-division multiplex channels from PCM highway trunk group A. However, only complete boards are activated on the other trunk group. The remaining time-division multiplex channels of PCM highway trunk group F remain free.
- Two-box system

  All peripheral boards use the PCM highways from trunk group A only.

5.4.6 Distribution of the PCM Highways in the Expansion Box

The expansion box provides a PCM highway bundle with 2 x 4 PCM highways for each peripheral board slot. There are 32 time-division multiplex channels available for each PCM highway. If all of these channels are busy, no further call requests can be accepted.

To guarantee that the system operates without blocking, make sure when performing configuration that the boards on a PCM segment do not require more than the number of time-division multiplex channels available.

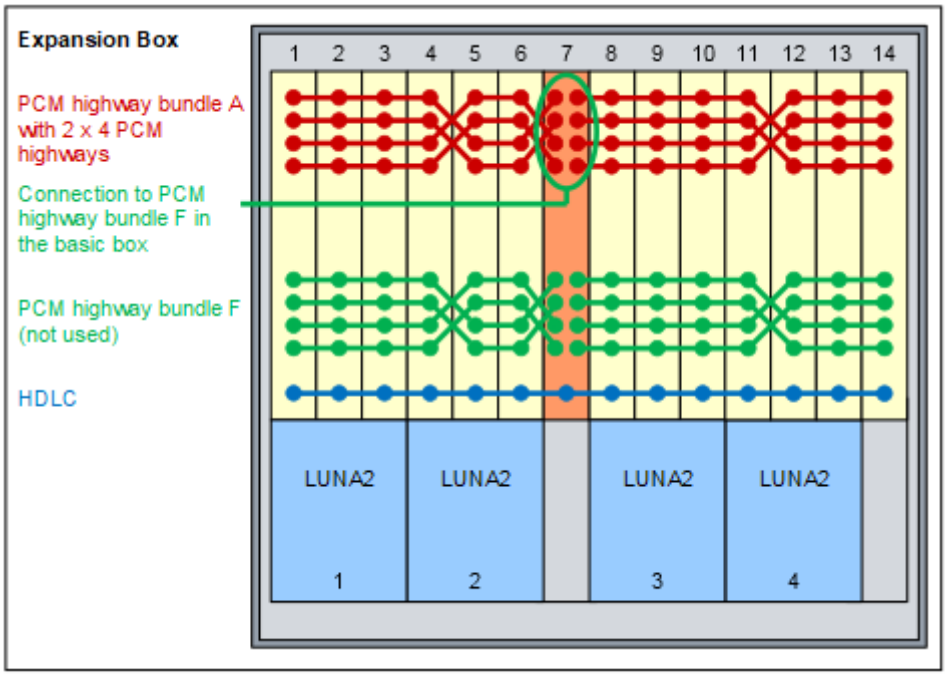


Figure 12: OpenScape Business X8 – PCM Highways in the Expansion Box

All peripheral boards in the expansion box use the PCM highways from trunk group A only.

128 time-division multiplex channels (4 PCM highways) are available on the PCM segment for board slots 1 to 6 and on the PCM segment for board slots 8 to 14.

PCM highway bundle F is not used.

5.4.7 Time-division Multiplex Channels of the Peripheral Boards

Each peripheral board requires a different number of time-division multiplex channels to execute call requests. OpenScape Business X8 provides these time-division multiplex channels in the form of PCM highways.

OpenScape Business X8 provides PCM highway trunk groups with 2 x 4 PCM highways for each peripheral board slot. There are 32 time-division multiplex channels available for each PCM highway. If all of these channels are busy, no further call requests can be accepted. To guarantee that the communication system operates without blocking, make sure when performing configuration

that the boards on a PCM segment do not require more than the number of time-division multiplex channels available.

When assigning time-division multiplex channels to the peripheral boards, a distinction is made between the following types of assignment:

- Static assignment

  Time-division multiplex channels are assigned statically for trunk and tie-traffic boards. This ensures that all calls can be processed.

  NOTICE: The TMDID board only uses the first half of a PCM segment, which means that up to 64 channels are available per PCM segment for TMDID static time-division multiplex channels. To guarantee that the communication system operates without blocking when using the TMDID, the boards on a PCM segment must not occupy more than 64 static time-division multiplex channels.

  Examples for a PCM segment:

  2 x TMDID + 1 x DIU2U = 64 static time-division multiplex channels = approved equipment

  1 x TMDID + 1 x TMANI + 1 x DIUT2 = 76 static time-division multiplex channels = unapproved equipment

  1 x TMDID + 2 x SLMO2 = 8 static and 96 dynamic time-division multiplex channels = approved equipment

- Dynamic assignment

  Time-division multiplex channels are subject to dynamic assignment in subscriber line modules. The channels are seized with every call and released at the end of each call. The current number of time-division multiplex channels required is determined by the number of active stations.

- Static/dynamic assignment

  For boards with S_0 interfaces, the way in which the time-division multiplex channels are assigned depends on the actual use of the individual S_0 interfaces. The channels are assigned statically if the S_0 interface is used for the ISDN trunk connection (ISDN trunk). The channels are assigned dynamically if the S_0 interface is used for the ISDN station connection.

For details on the number of time-division multiplex channels required by the various peripheral boards, see *OpenScape Business X5/X8 Service Documentation, Appendix - Hardware Expansion*,

5.4.8 Board Installation

Peripheral boards can be inserted and removed while the power is connected (hot swappable). Always use the board wrench for removing and inserting boards.

The mainboard (OCCL or OCCLA) must not be pulled out when the system is energized. In this case, the system must be first disconnected from the mains.

5.4.8.1 How to Insert a Board

Prerequisites

The front plastic cover of the system box is not attached.

A free board slot is available.

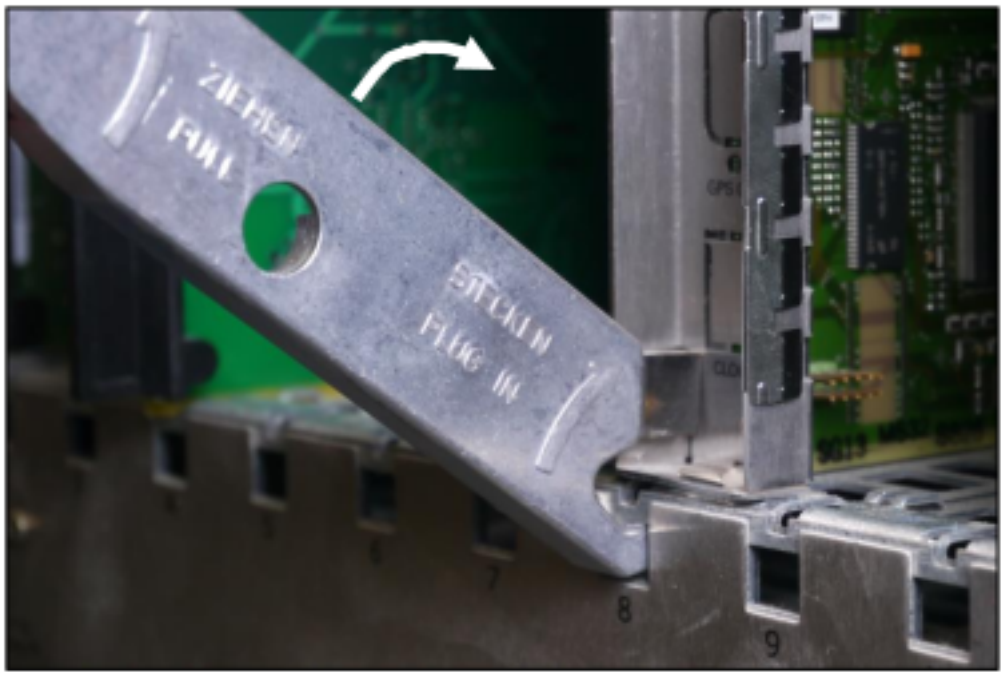
The specifications on the distribution of the PCM highways in the system boxes were taken into account.

NOTICE: Always wear an antistatic wristband when handling boards.

The ESD measures for protecting electrostatically sensitive devices must be observed and followed (see Warnings: Note on page 15)

Step by Step

1) Using its guide rails slide the board into the system box until it stops.
2) Insert the tip of the board wrench marked "Plug-In" into the bottom opening in the front cover of the board.
3) Lever the board into the board shelf of the system box by pushing the board wrench upwards.



5.4.8.2 How to Remove a Board

Prerequisites

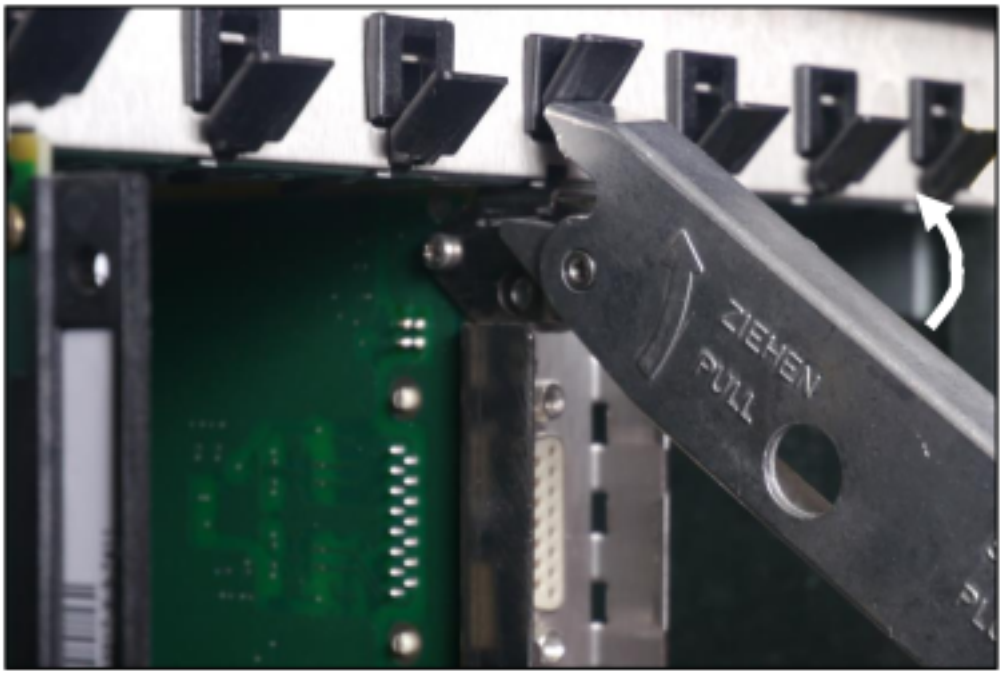
The front plastic cover of the system box is not attached.

NOTICE: Always wear an antistatic wristband when handling boards.

The ESD measures for protecting electrostatically sensitive devices must be observed and followed (see Warnings: Note on page 15)

Step by Step

1) Insert the tip of the board wrench marked “Pull” into the top opening on the front cover of the board to be removed.
2) Lever the board out of the board shelf of the system box by pushing the board wrench upwards.



3) Pull the board out of the system box over the guide rails.

5.4.8.3 How to Install Shielding Covers

By installing a shielding cover, you can ensure that unused board slots or slots that are equipped with peripheral boards that only have plastic covers are adequately shielded. The following boards are affected: STMD3, TMDID, TMEW2, SLMU, SLMAV8N, SLMAV24N.

Prerequisites

The front plastic cover is not attached to the system box.

Step by Step

1) Insert the two bottom pins on the shielding cover into the openings provided for this purpose on the shelf.

2) Press the shielding cover towards the board shelf until it snaps into place.

5.5 Backplanes of the System Boxes

The backplanes provide the connection between the central control board OCCL, the peripheral boards and the LUNA2/LUNA3 power supplies; they also provide connectors for telephones, trunks, etc.

5.5.1 Backplane of the Base Box

The backplane of the base box provides the connection between the central control board OCCLA, the peripheral boards and the LUNA2/LUNA3 power supplies; it also provides connectors for telephones, trunks, etc.

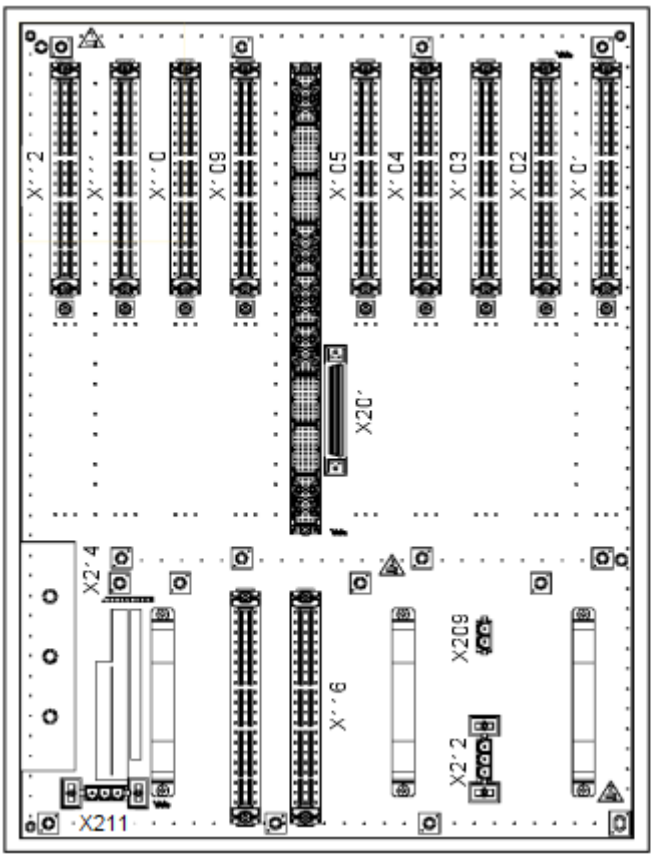


Figure 13: OpenScape Business X8 – Backplane of the Base Box

Table 3: OpenScape Business X8 – Connections on the Backplane of the Base Box

Connection	Function
X101 to X105, X109 to X112	SIVAPAC connectors for picking up the signals from the peripheral boards in slots 1 to 5 and 9 to 12 An external main distribution frame or patch panels are connected via CABLUs (Cabling Units = prefabricated cabling units) or open-end cables. The connection of the S_0 patch panel is made through an open-ended cable. The following connector panels can be plugged into the SIVAPAC connectors: • Connector panel with CHAMP jack for connecting an external main distribution frame or patch panel using CABLUs. • Connector panels with 8 and 24 RJ45 jacks for direct connection of telephones, trunks, etc.

Connection	Function
X116	SIVAPAC connectors for picking up the signals from the REALS board An external main distribution frame or patch panels are connected through an open-ended cable (24 DA): • S30267-Z196-A100: 10 m length • S30267-Z196-A250: 25 m length
X201	68-pin DB68 jack for connecting the cable to the expansion box (i.e., to the DBSAP board)
X209	DC port
X211, X212	AC power

5.5.2 Expansion Box Backplane

The backplane of the expansion box provides the connection between the peripheral boards and the LUNA2/LUNA3 power supplies; it also provides connectors for telephones, trunks, etc.

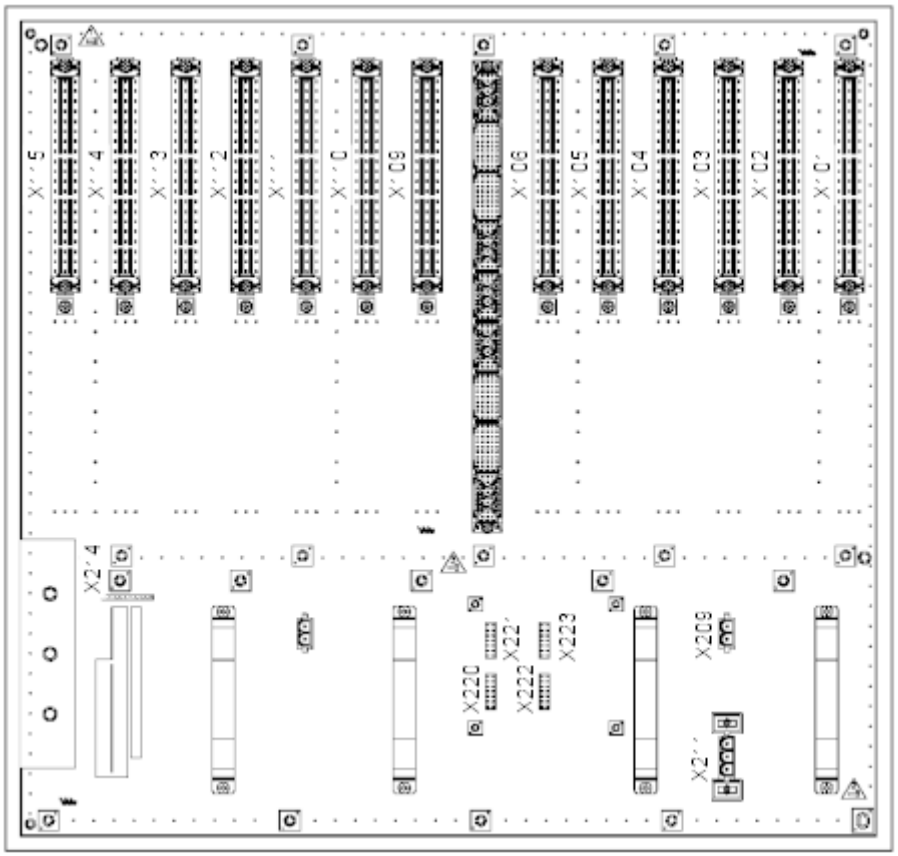


Figure 14: OpenScape Business X8 – Expansion Box Backplane

Table 4: OpenScape Business X8 – Connections on the Backplane of the Expansion Box

Connection	Function
X101 to X106, X109 to X115	SIVAPAC connectors for picking up the signals from the peripheral boards in slots 1 to 6 and 9 to 15 An external main distribution frame or patch panels are connected via CABLUs (Cabling Units = prefabricated cabling units) or open-end cables. The connection of the S_0 patch panel is made through an open-ended cable. The following connector panels can be plugged into the SIVAPAC connectors: • Connector panel with CHAMP jack for connecting an external main distribution frame or patch panel using CABLUs. • Connector panels with 8 and 24 RJ45 jacks for direct connection of telephones, trunks, etc.
X209	DC port
X211	AC power
X220 to X223	Connections for plugging in the DBSAP board DBSAP has a 68-pin DB-68 jack for connecting the connection cable to the base box (X201).

5.5.3 Connector or Shielding Panels for Backplanes

Connector panels with CHAMP jacks (for connecting the main distribution frame or a patch panel via CABLUs) and connector panels with RJ45 jacks (for direct connection of telephones, trunks, etc.) can be plugged into the SIVAPAC connectors on the backplanes of the base and extension boxes. Shielding panels are installed to ensure adequate shielding of the backplane for boards whose signals are not picked up via connector panels.

Connector Panel with CHAMP Jack (NPPSC, S30807-Q6626-X)

Connector Panel with 24 RJ45 Jacks (NPPAB, S30807-Q6622-X)

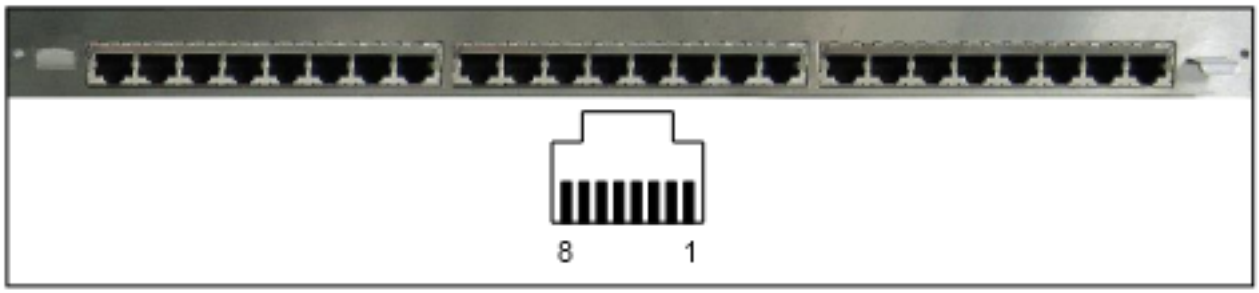


Table 5: Connector Panel with 24 RJ45 Jacks - Pin Assignments of the RJ45 Jacks

Pin	Signal
4	a
5	b
The RJ45 jacks have two wires.	

Connector Panel with eight RJ45 Jacks (NPPS0, S30807-Q6624-X)

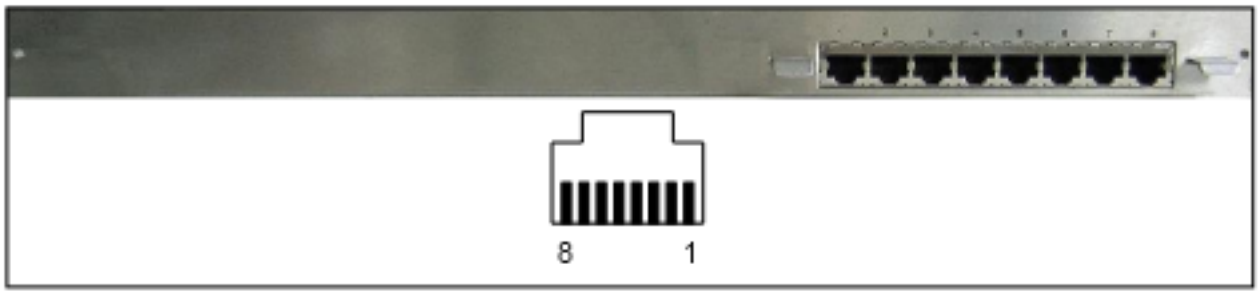


Table 6: Connector Panel with 8 RJ45 Jacks - Pin Assignments of the RJ45 Jacks

Pin	Signal	
	Trunk connection/ Networking	Station connection
3	Transmit +	Receive +
4	Receive +	Transmit +
5	Receive –	Transmit –
6	Transmit –	Receive –
The RJ45 jacks have four wires.		

Shielding Panel (C39165-A7075-C44)

5.5.3.1 How to Mount Connector or Shielding Panels

Prerequisites

The back plastic cover is not attached to the system box.

Step by Step

Select one of the following options:

- If you want to install a connector panel, press it onto the desired SIVAPAC connector on the backplane.

  Attach the connection panel to the system box with the two screws included in the delivery package.
- If you wish to install a shielding panel, run any existing CABLUs through the cable guides.

  Attach the shielding panel to the system box with the two screws included in the delivery package.

5.5.4 Connection to Backplanes

The backplanes of the base box and the expansion box provide connectors for phones, trunks, etc. The connection can be made via an external main distribution frame or via external patch panels. The direct connection to the backplane can be made via connector panels with RJ45 jacks.

5.5.4.1 How to Connect the Connection Cable between the Base and Expansion Box (Optional)

The connection cable (C39195-Z7611-A10) ensures that the expansion box receives HDLC, PCM and clock signals from the base box.

Prerequisites

The back plastic covers of the system boxes are not attached.

The DBSAP board (S30807-Q6722-X) is installed on the backplane of the expansion box.

Step by Step

1) Plug one of the cable connectors into the 68-pin DB68 jack X201 of the base box.
2) Plug the other cable connector into the 68-pin DB68 jack of the DBSAP board.
3) Use cable ties to secure both ends of the connecting cable to the system boxes.

5.5.4.2 How to Attach a Connection Cable to the External Main Distribution Frame (Optional)

Several different options are available to connect the backplane to the main distribution frame or any other external main distribution frame. These depend on which peripheral boards occupy which slots and on the connector panels used.

Prerequisites

WARNING: Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system and all main distribution frames before connecting telephones and lines.

The back plastic cover is not attached to the system box.

Step by Step

1) Select the appropriate connection cable depending on the peripheral board and the connector panel used.

If		Then
Peripheral board	**Connector panel**	**Connection cable**
STMD3 TMANI TMDID TMEW2 SLMAV8N	–	Connection to the MDFU-E or another external main distribution frame: open-end cable (24 DA) with SIVAPAC socket (backplane): • S30267-Z196-A100: 10 m length • S30267-Z196-A250: 25 m length
	Connector panel with CHAMP jack	Connection to external main distribution frame: cable with CHAMP connector
SLMU SLMAV24N	–	Connection to the external main distribution frame: open-end cable (24 DA) with SIVAPAC socket (backplane): • S30267-Z196-A100: 10 m length • S30267-Z196-A250: 25 m length

If		Then
Peripheral board	**Connector panel**	**Connection cable**
	Connector panel with CHAMP jack	Connection to external main distribution frame: cable with CHAMP connector

2) Plug the connection cable into the desired backplane connector.
3) Attach the cable to the system box using cable ties.
4) Select one of the following options to connect to any external main distribution frame:
   - If you use an external main distribution frame and an open-end cable, connect the cable to the desired splitting/jumper strip in the external main distribution frame.
   - If you use an external main distribution frame with CHAMP connectors and a CHAMP cable, insert the connector into the desired CHAMP jack of the external main distribution frame.
5) Attach the connection cable to the external main distribution frame using cable ties.

5.5.4.3 How to Install the Connection Cables to the Patch Panel (Optional)

To connect the backplane with the patch panel, CABLUs (24 DA) with SIVAPAC connectors in lengths of 2 m (S30267-Z333-A20) and 5 m (S30267-Z333-A50) are available.

Prerequisites

WARNING: Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system and all patch panels before connecting telephones and lines.

The back plastic cover is not attached to the system box.

Step by Step

1) Plug the connection cable into the desired backplane connector.
2) Attach the cable to the system box using cable ties.
3) Plug the connection cable into the desired connector of the patch panel.

   For information on the assignment of the RJ45 jacks of the patch panel S30807-K6143-X, see Patch Panels (Optional) on page 68.
4) Attach the connection cable to the patch panel using cable ties.

5.5.4.4 How to Install the Connection Cables to the S_0 Patch Panel (Optional)

To connect the backplane (SIVAPAC connector) with the S_0 patch panel, open-ended cables (24 DA) in lengths of 10 m (S30267-Z196-A100) and 25 m (S30267-Z196-A250) are available.

Prerequisites

WARNING: Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system before connecting telephones and lines.

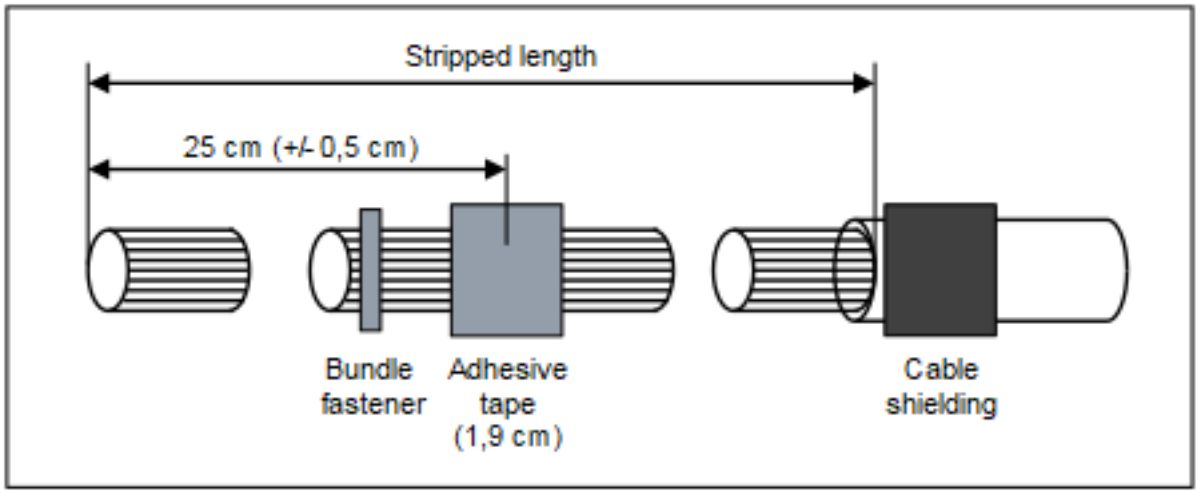
The back plastic cover is not attached to the system box.

Step by Step

1) Plug the connection cable into the desired backplane connector.

2) Attach the cable to the system box using cable ties.

3) Strip the cable wires (stripping length = 60 cm (+/– 0.5 cm)).



4) Strip the cable shield of the cable over a length of about 3 cm. Cut the drain wire to about 2.5 cm and fix it on the cable shield by wrapping it with tape (at least 1.5 times around).

5) Use a standard wiring tool for laying the cable wires on the S_0 patch panel. Twist the wire pairs before laying them (see figure below).

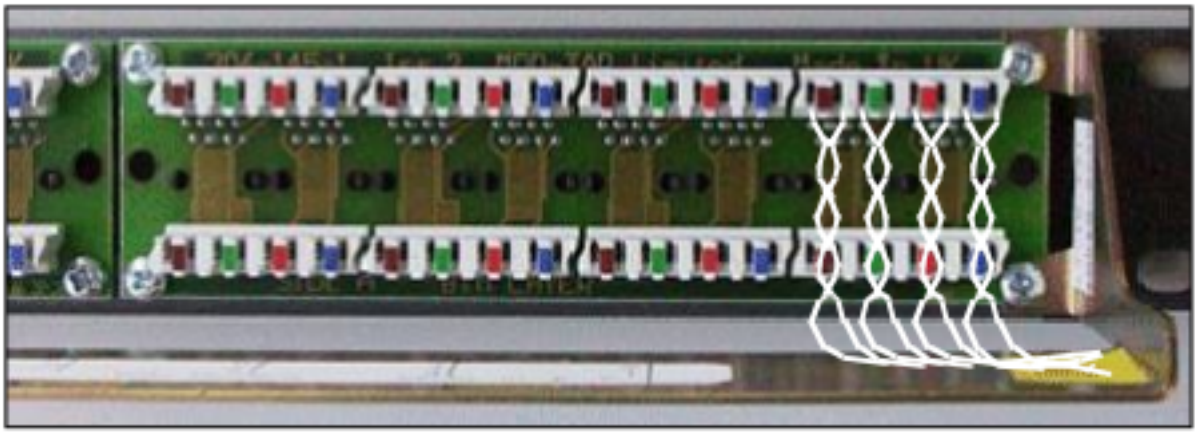


Table 7: Color codes for the open-end cable

Color Group	Pair	A-wire	B-wire
1	1	white/blue	
			blue/white
	2	white/orange	
			orange/white
	3	white/green	
			green/white
	4	white/brown	
			brown/white
	5	white/gray	
			gray/white
2	6	red/blue	
			blue/red
	7	red/orange	
			orange/red
	8	red/green	
			green/red
	9	red/brown	
			brown/red
	10	red/gray	
			gray/red
3	11	black/blue	
			blue/black
	12	black/orange	

Color Group	Pair	A-wire	B-wire
			orange/black
	13	black/green	
			green/black
	14	black/brown	
			brown/black
	15	black/gray	
			gray/black
4	16	yellow/blue	
			blue/yellow
	17	yellow/orange	
			orange/yellow
	18	yellow/green	
			green/yellow
	19	yellow/brown	
			brown/yellow
	20	yellow/gray	
			gray/yellow
5	21	purple/blue	
			blue/purple
	22	purple/orange	
			orange/purple
	23	purple/green	
			green/purple
	24	purple/brown	
			brown/purple

For information on the assignment of the RJ45 jacks of the S_0 patch panel C39104-Z7001-B3 for the station connection and the trunk connection, see Patch Panels (Optional).

6) Attach the connection cable to the S_0 patch panel using cable ties.

5.6 Trunk Connection

The OpenScape Business X8 communication system offers different options for trunk connections and thus for access to the public communication network.

You can select the trunk connection or connections required for your communication system from the following options:

- ISDN point-to-point connection and ISDN point-to-multipoint connection via S_0 interface (not for U.S. and Canada)

- ISDN Primary Rate Interface via the S_{2M} Interface (not for U.S. and Canada)
- ISDN Primary Rate Interface via the T1 interface (not for U.S. and Canada)
- Trunk connection with CAS protocol via CAS interface (for selected countries only)
- Analog trunk connections

5.6.1 How to Set up an ISDN Point-to-Point or ISDN Point-to-Multipoint Connection via an S_0 Port (Not for U.S. and Canada)

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system as well as all main distribution frames and patch panels before connecting telephones and lines.

A protective grounding of the S_0 patch panel (C39104-Z7001-B3) is not required.

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.

OpenScape Business X8 is equipped with at least one STMD3 board.

During startup, the S_0 interface must be configured as an ISDN point-to-point or ISDN point-to-multipoint connection.

An ISDN point-to-point or point-to-multipoint connection is available.

Step by Step

Connect the desired S_0 port with NTBA of the ISDN point-to-point or ISDN multipoint connection.

Select one of the following options to do this:

- If the connection is to be made via the external main distribution frame MDFU, connect the NTBA connection cable to the desired splitting strip/ jumper strip in the MDFU-E.
- If the connection is to be made via the external S_0 patch panel, connect the NTBA connection cable to the desired RJ45 jack of the S_0 patch panel.
- If the connection is to be made via the backplane of a system box (i.e., via a connector panel with eight RJ45 jacks), connect the NTBA connection cable to the desired RJ45 jack of the desired connector panel.

5.6.2 How to Set up an ISDN Primary Rate Interface via an S_{2M} Port (Not for U.S. and Canada)

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system as well as all main distribution frames and patch panels 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.

OpenScape Business X8 is equipped with at least one DIUT2 board.

One ISDN Primary Rate Interface is available.

Step by Step

Connect the desired sub-D connector in the front panel of the desired board with the NTPM of the ISDN Primary Rate Interface.

5.6.3 How to Set up the ISDN Primary Rate Interface via a T1 Interface (For U.S. and Canada Only)

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system as well as all main distribution frames and patch panels 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.

OpenScape Business X8 is equipped with at least one DIUT2 board.

One Channel Service Unit (CSU) that is approved as per FCC Part 68 and that satisfies the ANSI directive T1.403 is available. The T1 interface must not be directly connected to the PSTN (Public Switched Telephone Network).

It is essential that one CSU be installed between the communication system and the digital trunk connection. The CSU provides the following features for OpenScape Business X8: Isolation and overvoltage protection of the communication system, diagnostic options in the event of a malfunction (such as signal loopback, application of test signals and test patterns), line-up of the output signal in compliance with the line lengths specified by the network provider. A CSU is not a delivery component of the OpenScape Business X8 communication system.

One ISDN Primary Rate Interface is available.

Step by Step

Connect the desired sub-D connector in the front panel of the desired board with the Channel Service Unit (CSU).

5.6.4 For Selected Countries Only: How to Set up a Trunk Connection via an E1-CAS Interface

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system as well as all main distribution frames and patch panels 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.

OpenScape Business X8 is equipped with at least one TMCAS2 or TMCAS board.

A trunk connection with the CAS protocol is available.

Step by Step

Connect the desired CAS interface in the front panel of the desired board with the NT of the trunk connection.

5.6.5 How to Set up an Analog Trunk Connection

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system as well as all main distribution frames and patch panels 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 TMANI and TMDID boards 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 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.

OpenScape Business X8 is equipped with at least one TMANI or TMDID board.

For the U.S. and Canada only: A protector as per UL 497A or CSA C22.2 No. 226 is available. The installation regulations require analog trunks to be connected using approved protectors as per UL 497A or CSA C22.2 No. 226.

An analog trunk connection with MSI (main station interface) signaling procedures (ground-start and loop-start signaling) is available.

Step by Step

Connect the desired a/b port of the desired board with the TAE socket of the analog trunk connection.

Select one of the following options to do this:

- If the connection is to be made via the external main distribution frame MDFU, connect the TAE connection cable to the desired splitting strip/ jumper strip in the MDFU.
- If the connection is to be made via the external patch panel, connect the TAE connection cable to the desired RJ45 jack of the patch panel.
- If the connection is to be made via the backplane of a system box (i.e., via a connector panel with 24 RJ45 jacks), connect the TAE connection cable to the desired RJ45 jack of the desired connector panel.

5.7 Connection of phones and devices

The OpenScape Business X8 communication system offers various options for connecting phones and devices.

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

- Direct connection of ISDN phones (not for U.S. and Canada)
- Connection of ISDN phones via the S_0 bus (not for U.S. and Canada)
- Connection of $U_{P0/E}$ phones
- Connection of analog phones and devices

NOTICE: Only one analog device can be connected to an a/b interface.

5.7.1 How to Connect ISDN Phones Directly (Not for U.S. and Canada)

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system as well as all main distribution frames and patch panels before connecting telephones and lines.

A protective grounding of the S_0 patch panel (C39104-Z7001-B3) is not required.

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

Only for the station connection interfaces: In the case of line lengths exceeding 500 m and where the lines exit the building, the STMD3 board 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 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.

OpenScape Business X8 is equipped with at least one STMD3 board.

The S_0 ports used must be configured at startup as an internal S_0 connection.

The ISDN phones to be connected must have a separate power source, e.g., via a power adapter. It is not possible to obtain power via the S_0 ports of the STMD3 board.

Step by Step

1) Connect the desired S_0 port with the ISDN telephone.

Select one of the following options to do this:

- If the connection is to be made via the external main distribution frame MDFU-E, connect the ISDN phone connection cable to the desired splitting strip in the MDFU-E.
- If the connection is to be made via the external S_0 patch panel, connect the ISDN phone connection cable to the desired RJ45 jack of the S_0 patch panel.
- If the connection is to be made via the backplane of a system box (i.e., via a connector panel with eight RJ45 jacks), connect the ISDN phone connection cable to the desired RJ45 jack of the desired connector panel.

INFO: Refer to the installation instructions of the phone to be connected.

2) If present, connect any further ISDN phones to the communication system by the same method.

5.7.2 How to Connect ISDN Phones via the S_0 Bus (Not for U.S. and Canada)

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system as well as all main distribution frames and patch panels before connecting telephones and lines.

A protective grounding of the S_0 patch panel (C39104-Z7001-B3) is not required.

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

Only for the station connection interfaces: In the case of line lengths exceeding 500 m and where the lines exit the building, the STMD3 board 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 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.

OpenScape Business X8 is equipped with at least one STMD3 board.

The S_0 ports used must be configured at startup as an internal S_0 connection.

The ISDN phones to be connected must have a separate power source, e.g., via a power adapter. It is not possible to obtain power via the S_0 ports of the STMD3 board.

Every individual ISDN phone (ISDN stations) must be assigned a unique Multiple Subscriber Number (MSN). This assignment must be made in the configuration menu of the ISDN station.

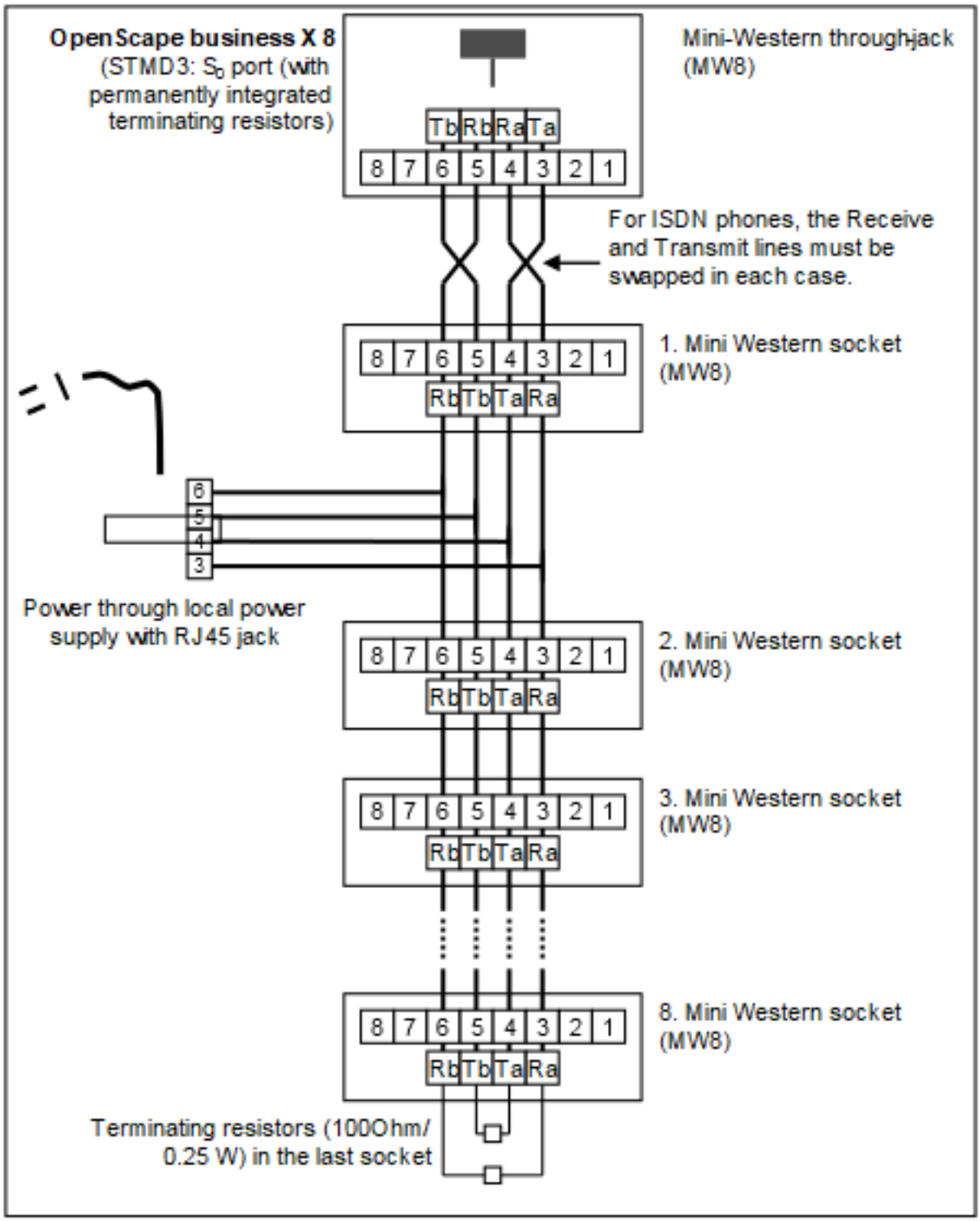
Step by Step

1) Connect the desired S_0 port with the Mini Western socket of the S_0 bus.

Select one of the following options to do this:

- If the connection is to be made via the external main distribution frame MDFU, connect the connection cable of the Mini Western socket of the S_0 bus to the desired splitting strip in the MDFU.
- If the connection is to be made via the external S_0 patch panel, connect the connection cable of the Mini Western socket of the S_0 bus to the desired RJ45 jack of the S_0 patch panel.
- If the connection is to be made via the backplane of a system box (i.e., via a connector panel with eight RJ45 jacks), connect the connection cable of the Mini Western socket of the S_0 bus to the desired RJ45 jack of the desired connector panel.

2) Complete the wiring as shown in the following diagram.



3) Install terminating resistors (100 Ohm/0.25 W) in the last socket of the S_0 bus.

4) Make sure that terminating resistors are only connected to the two ends of the S_0 bus. No terminating resistors are required for the other sockets of the S_0 bus.

INFO: Since terminating resistors are already integrated into OpenScape Business X8, the communication system forms one end of an S_0 bus.

INFO: Refer to the installation instructions of the phone to be connected.

5.7.3 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 the system boxes of your communication system as well as all main distribution frames and patch panels 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 SLMO2 and SLMO8 boards 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 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.

OpenScape Business X8 is equipped with at least one SLMU board.

Step by Step

1) Connect the desired $U_{P0/E}$ port with the $U_{P0/E}$ phone.

Select one of the following options to do this:

- If the connection is to be made via the external main distribution frame MDFU, connect the $U_{P0/E}$ phone connection cable to the desired splitting strip/jumper strip in the MDFU.
- If the connection is to be made via the external patch panel, connect the connection cable of the $U_{P0/E}$ telephone to the desired RJ45 jack of the patch panel.
- If the connection is to be made via the backplane of a system box (i.e., via a connector panel with 24 RJ45 jacks), connect the $U_{P0/E}$ phone connection cable to the desired RJ45 jack of the desired connector panel.

INFO: Refer to the installation instructions of the phone to be connected.

2) If present, connect any further $U_{P0/E}$ phones to the communication system by the same method.

5.7.4 How to Connect Analog Telephones and Devices

Prerequisites

WARNING:

Risk of electric shock through contact with live wires

Use separate ground wires to provide protective grounding for the system boxes of your communication system as well as all main distribution frames and patch panels 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 SLMAV8N and SLMAV24N boards 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 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.

OpenScape Business X8 is equipped with at least one SLMAV8N or SLMAV24N board.

Step by Step

1) Connect the desired a/b port to be connected to the analog device (phone, fax, modem, loudspeaker, etc.).

Select one of the following options to do this:

- If the connection is to be made via the external main distribution frame MDFU, connect the connection cable of the analog phone or device to the desired splitting strip/jumper strip in the MDFU.
- If the connection is to be made via the external patch panel, connect the connection cable of the analog telephone or device to the desired RJ45 jack of the patch panel.
- If the connection is to be made via the backplane of a system box (i.e., via a connector panel with 24 RJ45 jacks), connect the connection cable of the analog telephone or device to the desired RJ45 jack of the desired connector panel.

2) If present, connect any further analog phones or devices to the communication system by the same method.

5.8 Closing Activities

To complete the installation, the M.2 SSD or SDHC card must be inserted, and a visual inspection must be performed. Furthermore, for standalone installations, all system boxes of the communication system must be closed with the plastic covers provided for this purpose. Finally, the system is 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 power supply 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

5.8.1 How to Insert the M.2 SSD or the SDHC Card (system with OCCM)

The M.2 SSD or the SDHC card contains the OpenScape Business communication software and must be mounted/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.

5.8.2 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

Disconnect all power supply circuits of the communication system before starting to perform a visual inspection:

- Disconnect the battery voltage, supply voltage (LUNA2/LUNA3) and line voltage.
- Disconnect the line cords of any connected battery pack or any connected batteries.
- Disconnect all power plugs of the communication system.

NOTICE:

Always wear an antistatic wristband when handling boards.

The ESD measures for protecting electrostatically sensitive devices must be observed and followed (see Warnings: Note).

The front and rear plastic covers are not attached to the system boxes.

Step by Step

1) Disconnect all power supply circuits of the communication system.
2) Make sure that the communication system is de-energized.
3) Make sure that the M.2 SSD or SDHC card is correctly inserted. The write protection of the SDHC card must be disabled (switch directed toward metal contacts).
4) Check that all boards are secure.

   If requires, verify that the boards involved have been inserted properly (see How to Insert a Board).
5) 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.

6) Check to ensure that the shielding covers are properly installed for unused board slots or slots that are equipped with peripheral boards that only have plastic covers.

   If required, install the missing shielding covers (see How to Install Shielding Covers).

7) Verify that the slots for the LUNA2/LUNA3 power supplies and the REALS board inside the base box are covered by an outer panel.

   If necessary, attach the missing outer panel.

8) Verify that the slots for the LUNA2/LUNA3 power supplies and the REALS board inside the expansion box (if available) are covered by an outer panel.

   If necessary, attach the missing outer panel.

9) Check for the presence of shielding panels on the backplane for boards that do not have connector panels.

   If necessary, install the missing shielding panel (see How to Mount Connector or Shielding Panels).

10) Check whether a separate ground wire is connected to the ground terminal of each system box.

    If required, perform the separate grounding of all system boxes (see Protective Grounding for Standalone Installations and Protective Grounding for 19'' Rack-mount Installations).

11) Make sure that any main distribution frames and/or patch panels being used are properly connected to the ground wire.

    If required, perform the separate grounding of all main distribution frames and/or patch panels (see Protective Grounding for Standalone Installations and Protective Grounding for 19'' Rack-mount Installations).

12) Check whether the nominal voltage of the mains power supply corresponds to the nominal voltage of the communication system (type plate).

Next steps

Only for standalone installations: close all system boxes of the communication system with the plastic covers provided for this purpose (see Only for Standalone Installations: How to Mount the Plastic Covers of a System Box on page 113).

5.8.3 Only for Standalone Installations: How to Mount the Plastic Covers of a System Box

For standalone installations, all system boxes must be closed with the provided plastic covers provided for this purpose before starting up the communication system.

Step by Step

1) Place the pins on the lower edge of a plastic cover into the guide slots on the front side of the base box.

2) Press the plastic cover towards the base box until it snaps into place.

3) Repeat steps 1 and 2 to mount the plastic cover on the back of the base box.
4) Repeat steps 1 through 3 to mount the plastic covers for the extension box, if any.

5.8.4 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.

---

6 Installing the Linux Server

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

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

Either the regular SLES 15 SP6/SP7 64 bit version optimized by the manufacturer of the server PC must be installed as the Linux operating system.

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

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

6.1 Prerequisites

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

Minimum Hardware Requirements

The server PC must satisfy the following minimum requirements:

- 64-bit capable
- Equipped for 24/7 operation
- Certified by the PC manufacturer for SLES 15 SP6/SP7 64 bit
- The communication software for OpenScape Business must be the only application running (excluding virus scanners)
- LAN connection with minimum speed of 100 Mbps
- keyboard, mouse, USB 2.0, DVD drive
- Screen resolution: 1024x768 or higher
- Recommended CPU families:

  - Intel Core i processors: 6th generation and higher and corresponding Xeon CPUs

  - AMD Ryzen processors

The server's category (*Basic, Standard, Advanced*) is defined by the *max number of users* each supports.

	Basic Server	Standard Server	Advanced Server
Max number of users	up to 50	up to 500	up to 1500

	Basic Server	Standard Server	Advanced Server
Processor cores / base clock speed per core	2/2,5 GHz or 4/2 GHz	2/3 GHz or 4/2,5 GHz	4/3,5 GHz or 6/3 GHz
RAM	4 GB	6 GB	8 GB
HDD / SSD	60 GB	200 GB	500 GB

Please note that if the Multimedia Contact Center is used, the Advanced Server must be used always.

Also, if the fax option is used, the Standard Server configuration is the minimum requirement.

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

Software

To install the Linux operating system on the server PC, the SLES 15 SP6/SP7 64 bit Linux version is required.

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

Some PC manufacturers offer their own optimized Linux installation disks for their server PC models. These can be used if they support the Linux version SLES 15 SP6 64 bit.

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

SLES 15 SP6/SP7 64 bit Certification

The server PC must be certified for SLES 15 SP6/SP7 64 bit.

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

`https://www.suse.com/yessearch/Search.jsp`

If no certification is available, the PC manufacturer must be asked whether the server PC is compatible with SLES 15 SP6/SP7 64 bit. If any additional hardware (e.g., a network or graphics card) that is incompatible with SLES 15 SP6/SP7 64 bit is installed, a suitable driver must be obtained from the card vendor, regardless of the certification. If no driver is available, the corresponding card must be replaced by a model that is compatible with SLES 15 SP6/SP7 64 bit.

Registering with Novell

Although the installation and operation of SLES 15 SP6/SP7 64 bit is possible without registering with Novell, registration at Novell is required in order to obtain security patches and software updates. To do this, you will need to create a customer account with Novell with the help of the activation code (see also Updates *on page 137*). It is recommended that the customer account be set up before the Linux installation.

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

Infrastructure

The internal network must satisfy the following conditions:

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

Internet Access

The server PC must have Internet access for:

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

OpenScape Business requires an Internet connection for:

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

Network Configuration

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

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

Parameters	Sample values
External DHCP server or Linux DHCP server	DHCP server of the Internet router (external)
DHCP address range	192.168.5.50 through 192.168.5.254
Subnet mask of the network or network segment	**255.255.255.0**
Fixed IP address of the Linux server This IP address must be outside the DHCP range.	**192.168.5.10**
Internet Router	192.168.5.1
Server with fixed IP address (optional), e.g., e-mail server	192.168.5.20
Clients with fixed IP address (optional) This IP address must be outside the DHCP range.	192.168.5.1 through 192.168.5.49
Default Gateway, i.e., the Internet router in the example	**192.168.5.1**

Parameters	Sample values
DNS Server (i.e., the Internet router in the example)	**192.168.5.1**
Domain name when using a DNS server (e.g., the Internet domain name	**customer.com**
Host name of OpenScape Business The name can be freely selected, but should be coordinated with the network administrator.	**comm_server**

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

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

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

6.2 Installation in a Virtual Environment

The communication software can run in a virtual environment.

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

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

The following virtualization software has been released:

- Details about VMware vSphere released versions including the latest patches are in the OpenScape Business Release Notes.

  For details on the hardware requirements of the physical server PC, refer to the "VMware Compatibility Guide and the "VMware Management Resource Guide" at www.vmware.com.

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

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

- Windows Server (2008 R2, 2012, 2012 R2) Hyper-V, including the latest patches.

  For details in the hardware requirements of the physical server PC, refer to technet.microsoft.com.

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

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

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

Parameters	VM Settings
Guest Operating System	SLES 15 SP6/SP7 64 bit
VM HD Capacity	Up to 50 users: 60 GB or more Up to 100 users: 100 GB or more Up to 500 users: 200 GB or more OpenScape Business Contact Center: 200 GB or more As of 500 users: 500 GB or more
Virtual Disk Mode	Default
Virtual Disk Format Type	Thin Provisioning (dynamic HD Capacity) or Thick Provisioning (fixed HD Capacity)
vCPUs	2 4 for OpenScape Business Contact Center or more than 500 users
vCPUs Shares (High/Normal)	High
vCPU Reservation	2 GHz
vCPU Limit	Unlimited
VM Memory	2 GB (recommended 4 GB) 6 GB for: - Fax as PDF - OpenScape Business Contact Center 8 GB for: - More than 500 users
VM Memory Shares (High/ Normal)	Normal
VM Memory Reservation	4 GB
VM Memory Limit	Unlimited

Parameters	VM Settings
Number of vNICs	1
VMware Manual MAC Used	NO
Virtual Network Adapter Support	YES, vmxnet3 driver
VMware Tools Installation	YES

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

The following VMware vSphere features are supported:

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

The following VMware vSphere features are not supported:

- Fault tolerance

The following Microsoft Hyper-V features are supported:

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

The screen saver for the virtual environment must be disabled.

6.2.1 VM Co-Residency and Quality of Service policy

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

- It is up to the parties responsible for deploying the Mitel VMs and managing the virtual environment to ensure the performance criteria is met. Uncertainty can be reduced by pre-deployment testing, baselining, and following the rules of Mitel VM Configuration and Resource Guide (VM R&C) including this policy.
- VMs with Mitel real time and mission critical applications shall be protected from other applications in the routing and switching network to ensure voice/ video network traffic get the needed bandwidth and protection from delay and jitter.
- VMs with Mitel real time and mission critical applications shall be protected from other applications when the virtualization host shares compute, storage, and network hardware among multiple application virtual machines (e.g. you cannot schedule Mitel real time.
- Adherence to Mitel Virtualization and Resource configuration rules (e.g. physical/virtual hardware sizing, co-residency policy, etc.) is required in order

to ensure Mitel VMs get the needed CPU, memory, storage capacity and storage/network performance.
- Mitel VMs shall not be hosted on the same HW with third-party VMs that have incomplete resource requirements defined.
- Host hardware shall be continuously monitored (e.g. by vCenter) and operated below 80% CPU usage with a %RDY value of 5% max.
- The total amount of RAM, Storage, and NW (including Storage Network) throughput shall not be exceed the capacity of the Host hardware (no over subscription).
- Even if the host processor is hyper-threading-capable and HT is enabled, a physical core shall only be counted once.
- vCPU Shares shall be configured to guarantee mission critical Mitel VMs (including real time VMs) are never starved for CPU time.
- Customers are responsible to fulfill the requirements, even if the VM is moved around in the environment, e.g. by manually re-configuring the CPU shares of a VM if it gets moved to another VM host or resource pool.
- Disaster Recovery plans need to take into account the additional resources required when failing over to fail over site (datacenter 2).

6.2.2 Time Synchronization of the Guest Operating System Linux

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

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

Step by Step

1) Right-click in the VMware client **vSphere Client** on the guest operating system Linux and select the menu item **Edit Settings**.
2) Under the **Virtual Machine Properties** on the **Options** tab, disable the option **Synchronize guest time with host** under the **VMware Tools** entry in the **Advanced** area.
3) Edit the NTP settings for the guest operating system Linux in the `./etc/ntp.conf` file as follows in accordance with the parameters shown in bold:

```
**********************************************

...

tinker panic 0

# server 127.127.1.0

# local clock (LCL)
```

```
# fudge 127.127.1.0 stratum 10

# LCL is unsynchronized

...

server 0.de.pool.ntp.org iburst

restrict 0.de.pool.ntp.org

restrict 127.0.0.1

restrict default kod nomodify notrap

...

************************************************
```

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

6.3 Linux Security Aspects and RAID Array

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

Firewall

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

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

NOTICE: Firewall settings for WAN Adapter in OpenScape Business S must be handled manually by the administrator of the Linux PC.

Virus Scanners

A virus scanner is not included in the Linux installation package. It is recommended to install a virus scanner. You can get more information from the Release Notes of the communication software if required.

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

Intrusion Detection System (AppsAmor)

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

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

Redundancy

Recommendations for Improving Reliability (Redundancy):

- Two hard disks in a RAID 1 array.
- Second power supply for the Linux server
- Uninterruptible power supply

  When using IP phones, the LAN switches and IP phones should also be connected to an uninterruptible power supply.

RAID1 Array

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

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

For specific details on performing an installation with a software RAID, see Initial Startup with a Software RAID on page 130.

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

6.4 Initial Startup without a Software RAID

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

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

Linux Partitions

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

Partition	Type	Size	File system	Mount	Note
Partition 1	Primary Partition	2 GB	Swap	swap	corresponds to the size of the working memory
Partition 2	Primary Partition	20 GB	Ext4	/	for the Linux operating system
Partition 3	Primary Partition	Rest[1]	Ext4	/home	For the communication software

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

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

6.4.1 How to Install and Configure SLES 15 SP6/SP7 without a Software RAID

NOTICE:

If the installation procedure will be executed in a Virtual Machine(VM), please refer to chapter Installing the Communication Software.

Prerequisites

The BIOS setup of the Linux server is set so that the server will boot from the .ISO file on USB stick.

To register with Novell, Internet access and the activation code are required.

Step by Step

1) Insert the SLES 15 .ISO file on USB stick in a USB port and boot up the system from the .ISO file.
The Startup window of the Linux installation appears.
2) Select **Installation** and press Enter.

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

3) In the **Language, Keyboard and Product Selection** window, select the country settings for the Linux operating system:
   a) Select **English (US)** as the user interface language from the **Language** drop-down list.
   b) Select the keyboard layout for the desired country from the **Keyboard Layout** drop-down list.
   c) Select **SUSE Linux Enterprise Server 15 SP6 or SP7** as product to install.
4) Read through the license agreement and accept the license terms by enabling the check box **I Agree to the License Terms** and then click **Next**.
5) The **Network Configuration** appears. If not, select **Network Configuration** in the **Registration** window.

   If you want to configure the network later click **Next**.
6) On the **Network Settings** window, configure the network card.
   a) Select the desired network card in the **Overview** window. The MAC address of the network card selected here is assigned later in the licensing process to the individual licenses. Click **Edit**.
   b) Enable the radio button **Statically assigned IP Address**.
   c) Under **IP Address**, enter the assigned IP address of the Linux server (for example, `192.168.5.10`).

      The IP address must conform to the IP address scheme of your internal network and must not have been assigned to any other network client, since this would otherwise result in an IP address conflict.
   d) Under **Subnet Mask**, enter the assigned subnet mask of the Linux server (for example, `255.255.255.0`).

      The subnet mask must match the IP address scheme of your internal network.
   e) Under **Hostname**, enter the assigned hostname of the Linux server (for example, `OSBiz-Booster`).

WARNING: The hostname must conform to the hostname scheme of your internal network and must not be assigned to any network clients, since this would result in an hostname conflict. The default hostname "localhost" cannot be used with OSBiz S / Booster Server and must be changed. The hostname configured in the network settings, must also be configured in network card setup.

   f) Click **Next**.
7) Specify the DNS server and the default gateway.
   a) In the **Network Settings** window, click on the **Hostname/DNS** tab.
   b) Enter the hostname of the DNS server under **Static Hostname**.

      The hostname must conform to the hostname scheme of your internal network and must not be assigned to other network clients, since this would result in an hostname conflict. The default hostname "localhost" cannot be used with OSBIZ S / Booster Server and must be changed.

      In case the field remains empty or it is a localhost, "sles15_OSBIZS" is added automatically as the default static hostname, during the OSBIZ S

installation process. This value can be changed later on during OSBIZ S startup via yast under the **Network Settings** > **Hostname/DNS** tab.

c) Enter the domain name of the DNS server under **Domain Name**.

The domain name must be unique, since this would otherwise result in an domain name conflict.

d) Enter the IP address of the DNS server under **Name Server 1**.

If no DNS server is available in the internal network, enter the IP address of the internet router (for example, `192.168.5.1`).

e) In the **Network Settings** window, click on the **Routing** tab.

f) Select **Add** and under **Default Gateway** enter the IP address of the Internet router (for example, `192.168.5.1`) and select the ethernet device from the drop-down list.

8) Click **Next**.

9) In the **Registration** window, select **Register System ia scc.suse.com**, enter your email address and registration code and click **Next**.

10) In the **Extension and Module selection** window select the following extensions and modules: Basesystem Module, Containers Module, Desktop Applications Module, Development Tools Module, Legacy Module, Server Applications Module

11) Click **Next**.

12) In the **System Role** window, select **SLES with GNOME** and click **Next**.

13) In the **Suggested Partitioning** window it is proposed to first run the Guided Wizard to create boot and swap partitions automatically. To do so, select **Guided Setup**.

14) In the **Select Hard Disk(s**) window select **Remove even if not needed** for both selections and click **Next**.

15) In the **FileSystem type** select **Ext4** as file system for both Root and Home partitions. Enable options **Propose Separate Swap Partitions** and **Enlarge to RAM size for Suspend** and click **Next**.

16) A new layout is proposed in **Suggested Partitioning** window. Click **Expert Partitioner > Start with current proposal**.

Delete only root (/) and home (/home) partitions. Preserve only swap and boot partitions. Select the partition to be deleted, click on **Delete** and confirm the delete operation by clicking **Yes**.

17) Create the partition for the Linux operating system.

a) Click on device `/dev/sda` and select **Add Partition**.

b) Under **Custom Size**, enter the partition size 20GB and click **Next**.

The minimum size of the Linux operating system partition is 15GB and the recommended is 20GB.

c) In **Add Partition Role** window, select the **Operating System** role and click **Next**.

d) Select **Ext4** under **Format device**, select **/** in **Mount device** and click **Next**.

18) Create the partition for the communication software.

a) Click on device `/dev/sda` and select **Add Partition**.

b) Select **Maximum Size** if you prefer to use the remaining space of the hard disk or under Custom Size to enter the partition size and click **Next**.

The minimum size of the communication software partition is 40GB.

c) In **Add Partition on /dev/sda** window, select the **Data and ISV Applications** role and click **Next**.

d) Select **Ext4** under **Format device**, select **/home** in **Mount device** and click **Next** and **Accept**.

19) In the **Clock and Time Zone** window, select the correct region and time zone.

To adjust date and time or to configure an NTP server (for a uniform time base), proceed by clicking the **Other Settings** button. Click **Next** when finished.

20) In the **Local Users** window, add a user and password and click **Next**.

21) In the **Password for the System Administrator "root"** window, enter the password for the system administrator with the "root" profile in the **Password for the root User** and **Confirm Password** fields and then click **Next**.

The password should comply with conventional security policies. It must have at least 8 character, at least one lowercase letter, at least one uppercase letter, at least one number and at least one special character.

22) In the **Installation Settings** window click **Software**.

a) Enable **32-Bit Runtime Environment**.

b) Enable **DHCP and DNS Server**.

c) Click on **Details** and then in the **Search** field type `tcpdump` and select the package **tcpdump**.

d) Click on **Details** and in the search field type `docker`. Select the packages: **docker**, **docker-bash-completion**, **docker-rootless-extras**

e) Click **Accept**.

NOTICE: The above packages are mandatory for a successful installation of the SLES 15 SP6/SP7, except the docker packages (step 22d) which are mandatory for SLES 15 SP7 only. The **DHCP and DNS Server** package is required to install, even when they are not utilized as servers on OpenScape Business S.

---

23) To open the SSH port (the SSH port is closed by default for security reasons), in the **Installation Settings** window, under the **Security** section, click on **Open** at the **SSH port will be blocked** field.

24) Click **Install** again to confirm the installation.

The **Installation Settings** window is an overview of the components that are going to be installed. Before completing the installation, you can make any necessary changes from this window.

After the installation is completed, the computer is rebooted into the installed system.

6.4.2 How to upgrade from SLES 12 SP5 to SLES 15 SP6/SP7

Prerequisites

OpenScape Business latest V3R4 system. If OpenScape Business is not upgraded to the V3R4 latest, please proceed to a Software Update.

Installed OpenScape Business system on a SLES 12 SP5.

If an older version is used, an upgrade to SLES 12 SP5 is needed first. This chapter describes the upgrade of a full operational OpenScape Business system installed on SLES 12 SP 5 to SLES 15 SP6/SP7.

NOTICE: It is strongly recommended, following recommendations in the SUSE SLES 15 Upgrade Guide, to make a clean / fresh installation instead of using the Upgrade mechanism.

With fresh installation, you will still be able to restore your existing OpenScape Business Backup from the previous version in the new installed systems based on SLES 15 SP6/SP7.

It is observed that the Upgrade mechanism may cause problems to some settings of Linux, which may be critical for OpenScape Business functionality.

If a Virtual Machine is used (e.g. ESXi), it is recommended to create a new VM, instead of using the VM used as SLES 12 SP5. Otherwise, additional problems may exist when Host OS (e.g. ESCi) complains about the installed Linux version of guest (VM is initially created for SLES 12 and now it will run SLES 15).

In a clean / fresh install option in VM, the ALI (Locking ID) of system will be changed and a re-host of old license is mandatory.

Step by Step

1) Perform a software update of OpenScape Business to V3R4 version.
2) Back up all OpenScape Business Server. To do so, follow the instructions on How to Perform a Data Backup.
3) Uninstall OpenScape Business Server. To do so, follow the instructions on How to Uninstall the Communication Software.
4) Insert the SLES 15 SP6/SP7 installation USB and boot.
5) Perform a fresh installation of SLES 15 SP6/SP7.
6) After system upgrades to SLES 15 SP6/SP7, install OpenScape Business Server version that supports SLES 15 SP6/SP7.

NOTICE: Use the same partitioning as in SLES 12 SP5. Also, the file system needs to be the same for SLES 12 and SLES 15, otherwise the backup cannot be imported.

---

7) Restore all OpenScape Business Server data.

6.4.3 How to upgrade from SLES 15 SP6 to SLES 15 SP7

Upgrade from SLES15 SP6 to SLES15 SP7 can be done either offline or online through yast. Both ways are described below.

Prerequisites

Installed OpenScape Business system on a SLES 15 SP6. Upgrade to SLES 15 is madatory since SLES 12 is not supported for version OpenScape Business V3R4 FR3.

NOTICE: As a general safety precaution, it is recommended to perform a full system backup beforehand.

Offline upgrade

Step by Step

1) Perform a software update of OpenScape Business to latest V3R4 version.

2) Insert USB stick with the *.iso of SLES 15 SP7.

3) Reboot SLES machine and select machine **Startup through USB stick.**

4) Select **Upgrade**.

5) On **Language and Keyboard Selection**, choose the appropriate language and click **Next**.

6) On **Select for Update**, choose the **SLES 15 SP6** partition for update and click **Next**.

7) On the **SUSE Linux Enterprise Server 15 SP7 License Agreement**, agree with the terms and click **Next**.

8) On **Previously Used Repositories**, remove all repositories (default action) and click **Next**.

9) On **Extension and Module Selection**, select the following six modules and click **Next**:

a) Basesystem Module
b) Containers Module
c) Desktop Applications Module
d) Development Tools Module
e) Legacy Module
f) Server Applications Module

10) On **Add-On Product Installation**, verify that the six modules listed in the previous step are present and click **Next**.

11) On **Installation Settings**, review the upgrade options from SP6 to SP7.

In the **Packages** section, a red message appears stating “Cannot solve all conflicts”. Click **Manual intervention is required**.

12) When notified about the **rsyslog** utility, select the de-installation of **rsyslog** and click **OK**, then **Try Again**.

OpenScape Business uses **syslog-ng** for logging.

13) Review all patterns that will be installed.

If Docker packages were not installed on SLES 15 SP6, install them as described below. These packages are mandatory for OpenScape Business on SLES 15 SP7.

a) Click **Search** and enter **docker** in the search field, then click **Search**.

b) Select the following packages:

- docker
- docker-bash-completion
- docker-rootless-extras

c) Click **Accept**.

14) After all conflicts are resolved, click **Update** to start the upgrade procedure.

15) On the **Confirm Update** window, click **Start Update**.

It is important to install the docker packages. If for any reason the step for docker packages has been missed , a notification in visible at the landing page of WBM. Then user can install them via yast following these steps:

- Search for the Package Sources application and open it.
- In Page Sources pop up window select all package sources and close the window.
- Search for YaST Software Management and open it. Type 'docker' in the search field and select for installation these three packages: docker, docker-bash-completion, docker-rootless-extras.
- Click Accept.

Online upgrade

For detailed information on how to upgrade from SP6 to SP7 online, follow the instructions in the official SUSE documentation: https://documentation.suse.com/sles/15-SP7/html/SLES-all/cha-upgrade-online.html

Follow the steps as they are described in chapter 5.4 Upgrading with the online migration tool (YaST). Have in mind that SUSE licenses are needed to proceed with the online procedure.

NOTICE: Offline procedure is highly recommended. It is more clear and straight forward. Online procedure requires a higher lever of Linux expertise.

6.5 Initial Startup with a Software RAID

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

Proceed as follows:

1) Disable the BIOS RAID (optional)

If a RAID array is to be set up via a software RAID, any integrated RAID BIOS that may be present on the motherboard of the server PC must be first disabled in the BIOS.

2) Install and configure SLES 15 SP6/SP7 with a software RAID

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

Linux Partitions

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

Partition	Type	Size	File system	Mount	Note
Partition 1	Primary Partition	2 GB	Swap	swap	corresponds to the size of the working memory
Partition 2	Primary Partition	20 GB	Ext4	/	for the Linux operating system
Partition 3	Primary Partition	Rest[2]	Ext4	/home	For the communication software

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

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

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

6.5.1 How to Deactivate the BIOS RAID

Prerequisites

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

Step by Step

1) Restart the PC. During the startup, you will see whether the BIOS RAID has been enabled. If the BIOS RAID is not enabled, skip to step 3.

2) Disable the active BIOS RAID:

a) Press the appropriate key combination at the right time during the startup to enter BIOS RAID setup. The combination will be shown to you during the startup (e.g., CTRL M for LSI MegaRAID BIOS).

b) Clear the BIOS RAID configuration. Example for LSI MegaRAID BIOS: Management Menu > Configure > Configuration Menu > Clear Configuration.

c) Exit the setup of the BIOS RAID and restart the PC.

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

3) Disable the SATA RAID configuration in the BIOS setup of the PC:
   a) Press the appropriate key (e.g., F2 or Del) at the right time during the startup to enter BIOS setup of the PC.
   b) Disable the SATA RAID. Example for a Phoenix BIOS: Advanced > Advanced System Configuration > SATA RAID Disabled.
   c) Save your changes and exit the BIOS setup of your PC (with the F10 key, for example).
4) Restart the PC.

Next steps

Install and configure SLES 15 with a software RAID.

6.5.2 How to Install and Configure SLES 15 SP6/SP7 with a Software RAID

Prerequisites

Any possibly existing hardware RAID is disabled.

The BIOS setup of the Linux server is set so that the server will boot from the .ISO file.

To register with Novell, Internet access and the activation code are required.

Step by Step

1) Insert the SLES 15 .ISO file on USB stick in a USB port and boot up the system from the .ISO file. The Startup window of the Linux installation appears.
2) Select the menu item **Installation** and confirm this by pressing the Enter key.
3) In the **Language, Keyboard and License Agreement** window, select the country settings for the Linux operating system:
   a) Select **English (US)** as the user interface language in the **Language** drop-down list.
   b) Select the keyboard layout for the desired country from the **Keyboard Layout** drop-down list.
4) Read through the license agreement and accept the license terms by enabling the check box **I Agree to the License Terms**. Then click **Next**.
5) In the **Registration** window, select **Register System via scc.suse.com**, enter you email address and registration code and click **Next**.

> **INFO:** If you want to skip registration select **Skip Registration**, then click on **OK** in the **Warning** window that appears and finally click on **Next**. For your by skipping the registration you will not be able to have access to the update repositories. However you can register after the installation or visit customer service.

6) In the **Add On Product** window, click on **Network Configuration**.

> **NOTICE:** If you want to configure the network later click on **Next**.

7) On the **Network Settings** window, configure the network card.

a) Select the desired network card in the **Overview** window. The MAC address of the network card selected here is assigned later in the licensing process to the individual licenses. Click on **Edit**.

b) Enable the radio button **Statically assigned IP Address**.

c) Under **IP Address**, enter the assigned IP address of the Linux server (for example, `192.168.5.10`).

The IP address must conform to the IP address scheme of your internal network and must not have been assigned to any network client, since this would otherwise result in an IP address conflict.

d) Under **Hostname**, enter the assigned hostname of the Linux server (for example, `OSBiz-Booster`).

The hostname must conform to the hostname scheme of your internal network and must not have been assigned to any other network client, since this would otherwise result in an hostname conflict.

e) Under **Subnet Mask**, enter the assigned subnet mask of the Linux server (for example, `255.255.255.0`).

The subnet mask must match the IP address scheme of your internal network.

f) Then click **Next**.

8) Specify the DNS server and the default gateway.

a) In the **Network Settings** window, click on the **Host name/DNS** tab.

b) Enter the hostname of the DNS server under **Hostname**.

The hostname must conform to the hostname scheme of your internal network and must not have been assigned to any other network client, since this would otherwise result in an hostname conflict.

c) Enter the domain name of the DNS server under **Domain Name**.

The domain name must be unique, since this would otherwise result in an domain name conflict.

d) Enter the IP address of the DNS server under **Name Server 1**.

If no DNS server is available in the internal network, enter the IP address of the Internet router (for example, `192.168.5.1`).

e) In the **Network Settings** window, click on the **Routing** tab.

f) Under **Default Gateway**, enter the IP address of the Internet router (for example, `192.168.5.1`).

9) Click on **Next**.

10) In the **Add On Product** window, click on **Next**.

11) In the **System Role** window, select **Default System** and click on **Next**.

12) In the **Suggested Partitioning** window, select **Expert Partitioner...**

13) Partition the two hard disks:

a) Navigate in the **System View** menu tree to **Hard Disks** > **sda** (first hard disk of the software RAID).

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

c) Partition the first hard disk by using the **Add Partition** button.

Use the following data for the partitioning:

Partition 1	Primary Partition	2 GB	Role: Swap Format Swap Mount Point = swap, fstab Option = Device name
Partition 2	Primary Partition	0.5 GB	Role: Operating System Format Ext4 Mount Point = /boot **NOTICE:** This partition must be created only in the first drive.
Partition 3	Primary Partition	20 GB	Role: Operating System Format Ext4 /
Partition 4	Primary Partition	Rest	Role: Data and ISV Applications Format Ext4 /home

d) Navigate in the **System View** menu tree to **Hard Disks** > **sdb** (second hard disk of the software RAID).

e) Complete steps 13b. and 13c. for the second hard disk as well.

NOTICE: No boot partition needs to be created in the second hard drive.

14) Specify the software RAID settings:

a) Select the menu item **RAID** and click on **Add RAID**.

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

c) Select the two partitions sda3 and sdb2 in the **Available Devices** area on the left and transfer them with **Add** to the **Selected Devices** area on the right.

d) Click on **Next**.

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

f) In the next window select **Operating System** and click **Next**.

g) In the next window, select **Ext4** as format and the mount point "/" for the first RAID device (/dev/md0) and click **Finish**.

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

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

j) Select the two partitions sda4 and sdb3 in the **Available Devices** area on the left and transfer them with **Add** to the **Selected Devices** area on the right.

k) Click on **Next**.

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

m) In the next window, select **Data and ISV Applications** and click **Next**.

n) In the next window, select **Ext4** as format and the mount point "/home" for the second RAID device (/dev/md1) and click **Finish**.

15) Click on **Accept** and **Next**.

The partitioning data is saved; the actual partitioning of the hard disk occurs later.

16) In the **Clock and Time Zone** window, select the correct region and time zone.

To adjust date and time or to configure an NTP server (for a uniform time base), proceed by clicking the **Other Settings** button. Click **Next** when finished.

17) In the **Local Users** window, add a user and password and click **Next**.

18) In the **Password for the System Administrator "root"** window, enter the password for the system administrator with the "root" profile in the **Password for the root User** and **Confirm Password** fields and then click on **Next**.

The password should comply with conventional security policies. It must have at least 8 character, at least one lowercase letter, at least one uppercase letter, at least one number and at least one special character.

19) In the **Installation Settings** window, click **Install**, and confirm the installation by clicking **Install** again.

The **Installation Settings** window is an overview of the components that are going to be installed. Before completing the installation, you can make any necessary changes here.

After the installation routine has finished, the computer is rebooted into the installed system.

In order to select an appropriate screen resolution:

- Click on **Applications** in the task bar.
- Then in the menu tree, click on **Settings** > **Displays**.
- In the **Displays** window, click on the **Unknown Display**

- In the **Unknown Display** pop up window that appears select the appropriate resolution from the **Resolution** drop-down list and then click on **Apply**.
- Finally, in the confirmation pop up window that appears click on **Keep Changes**.

6.6 Configuring a Uniform Time Base

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

The following variants are possible as a time base:

- **SNTP server on the internal network (recommended)**

  If possible, an existing SNTP server on the internal network should be used. If this is the case, the IP address, URL or DNS name of the SNTP server is required.
- **SNTP Server on the Internet**

  If Internet access is available and set up, an SNTP server from the Internet can also be used. In this case, the URL or DNS name of the SNTP server is required.
- **OpenScape Business X5/X8 as an SNTP server**

  Alternatively, the OpenScape Business X5/X8 communication system can be used as an SNTP server. This requires the OpenScape Business X5/X8 to be connected to the Central Office via ISDN lines and the system time to be obtained from the CO. In this case, OpenScape Business X5/X8 must be first set up for use as an SNTP server (see the Administrator Documentation), and the IP address of the OpenScape Business X5/X8 must then be entered in Linux as an SNTP server.

The IP phones receive the date & time automatically from the OpenScape Business S softswitch or from the OpenScape Business X5/X8 communication system. The date and time on the client PCs on which the OpenScape Business communications clients are installed must be synchronized with the OpenScape Business S softswitch or the OpenScape Business X5/X8 communication system (see the operating system instructions of the client PCs for details).

6.6.1 How to Configure an SNTP Server

Step by Step

1) Click on **Applications** in the task bar.
2) In the menu tree, click on **Tools** > **YaST**.
3) Enter the password for the root user and click **Continue**. The YaST2 Control Center is opened.
4) Click **System** in the menu tree.
5) In the **System** area, click on **Date and Time**.
6) Click **Change**.
7) Activate the **Synchronize with NTP Server** option.

8) Specify an NTP server:

- **SNTP server on the internal network** (recommended)

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

  Select the desired SNTP server from the **NTP Server Address** list or enter the URL or DNS name of the SNTP server directly into the list box.

9) Select the **Save NTP configuration** check box.

10) Click **Configure**.

11) Activate the **Now and On Boot** option.

12) Click **OK** followed by **Accept**.

13) Close the window with **OK**.

14) Close the **YaST2Control Center**.

6.7 Updates

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

The installation and operation of the commercial SLES 15 SP6/SP7 64 bit version is possible without registration. However, it is still important to register with Novell in order to obtain security patches and software updates.

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

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

- **Updates during the Linux installation (recommended)**

  During the Linux installation, updates and patches can be downloaded online from the Novell Download Server.

  Exception: Service Packs may not be installed.
- **Updates after installing Linux and before installing the communication software**

  After the Linux installation, updates and patches can be downloaded manually from the Novell Download Server using YaST (Software - Online Updates).

  Exception: Service Packs may not be installed.
- **Updates after installing the communication software**

  After the installation of the communication software, updates and patches can be downloaded automatically from the Novell Download Server. When performing these updates, any updates and patches that require a reboot of the Linux server (interactive updates) must be skipped. After every 2 or 3

update processes, it is recommended that a manual be started so that the skipped, interactive updates are also installed.

The corresponding settings are made using YaST (Software - Online Updates).

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

NOTICE: During a SLES online update Linux's Yast administration tool prompts to remove either rsyslog or syslog-ng. You must only remove the rsyslog package as the syslog-ng package is used in the OpenScape Business S tracing feature.

6.7.1 How to Enable Automatic Online Updates

Step by Step

1) Click on **Applications** in the task bar.
2) In the menu tree, click on **System Tools** > **YaST**.
3) Enter the password for the root user and click **Continue**. The **Administrator Settings** window is opened.
4) Click on **Online Update Configuration**.
5) Enable the **Automatic Online Update** check box and then select **daily**, **weekly** or **monthly** as the interval.
6) Select the **Skip Interactive Patches** check box.
7) Click **OK**.
8) Close the **Administrator Settings**.

6.7.2 How to Enable Online Updates Manually

Step by Step

1) Click on **Applications** in the task bar.
2) In the menu tree, click on **System Tools** > **YaST**.
3) Enter the password for the root user and click **Continue**. The **Administrator Settings** window is opened.
4) Click on **Online Update** and you will see a list of the available patches (**Needed Patches**) that are required under the **Summary** area. If you already have all the latest patches installed, this list will be empty; otherwise select all the check boxes that appear.
5) Click on **Accept** to start the manual online update. The window will close automatically after the update.
6) Close the **Administrator Settings**.

6.7.3 Configuring the SLES 15 YaST2 Online Update

During the Online Update procedure, two rules must be followed to maintain the stability of the communication system.

Repositories configuration

Run the following commands via PuTTY and verify they executed successfully. These commands add specific SLES modules to the repositories list.

```
suseconnect -p sle-module-desktop-applications/15.6/x86_64
suseconnect -p sle-module-development-tools/15.6/x86_64
suseconnect -p sle-module-legacy/15.6/x86_64
```

Online Update Packages

The Online Update mechanism collects packages and patches via SUSE repositories. When there are conflicts with packages, YaST2 Online Update shows warnings.

In a clean install of OpenScape Business, some packages are locked to ensure the system's stability.

Do not update or remove these locked packages.

If a warning prompts you to remove a locked package, select **Do not install patch** in the conflict resolution window.

NOTICE: For further information on SLES Online updates, please refer to the corresponding SUSE documentation: *SUSE Linux Enterprise Server Administration Guide, chapter 7 "YaST online update"*.

6.8 Server Software Backup and Restore

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

After the initial startup and prior to each manual update, it is strongly recommended to use an appropriate backup tool to create a full backup of the server PC, including all relevant partitions. In the event of a fatal error following an update, the server PC can then be fully restored to its previous state.

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

If the entire server PC is backed up, the data of the communication software will be included in this backup. If only the operating system is backed up, the data of the communication software must be also backed up on a regular, recurring schedule.

7 Initial Setup for OpenScape Business X

This chapter describes the initial setup of OpenScape Business X. 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 X (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 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

7.1 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 in the customer LAN.
- The communication system has not yet been connected to the LAN.
- Internet access is available through an Internet Service Provider, LAN with rooter or WAN connection.
- 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 IP Address Scheme).
- A dial plan (also called a numbering plan) is present and known (see Dial Plan).

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:

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

  The following web browsers are supported:

  – Microsoft Internet Explorer
  – Microsoft Edge
  – Mozilla Firefox
  – Google Chrome

  For the supported browser versions, see *Software release notes*.

  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:

  At least 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.

7.2 Components

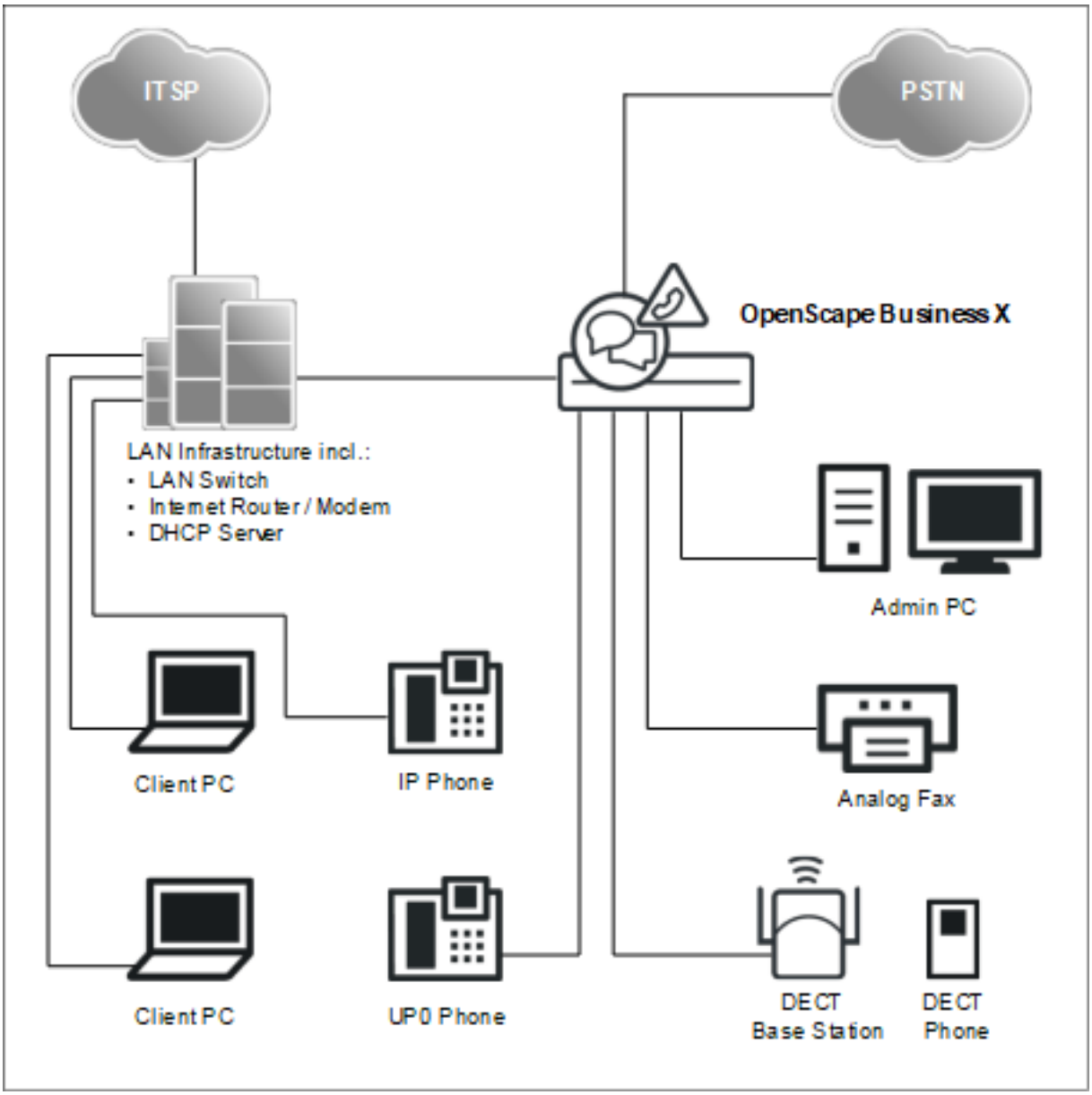
The various components of the installation example are described and outlined below. The initial Setup is described based on an installation example.

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).



7.3 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**	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.

7.4 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)**

7.5 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 Admin PC should be connected to the ADMIN ports with IP address 192.168.2.1 for the Initial Setup, to avoid address conflicts.

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.

7.5.1 How to Start 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. OpenScape Business does not provide a power on/off switch.

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 Service 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).

7.5.2 How to Connect the Admin PC to the Communication System

Prerequisites

The communication system is ready for use.

Use the ADMIN port for first integration into LAN.

IP addresses in the LAN are known.

IP address of the communication system in the LAN in known.

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.

NOTICE: You can also connect the admin PC to the LAN port "Admin" of the communication system, but you will then need to assign a fixed IP address in the range 192.168.2.xxx (e.g., 192.168.2.40) and the network mask 255.255.255.0 to the admin PC. The communication system has the IP address 192.168.2.1 via the LAN port "Admin" - important for WBM access!

7.5.3 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.

7.6 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.

7.6.1 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.

7.6.2 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.

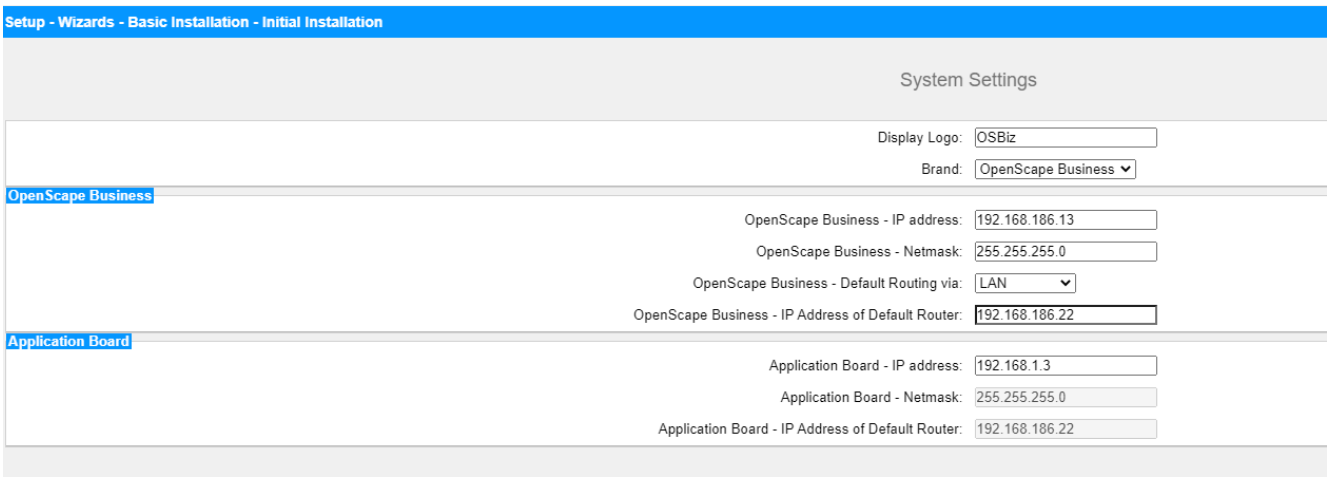
In addition, you can specify the IP address of your default router, e.g., the IP address of the Internet router.

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 on page 143).

7.6.2.1 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

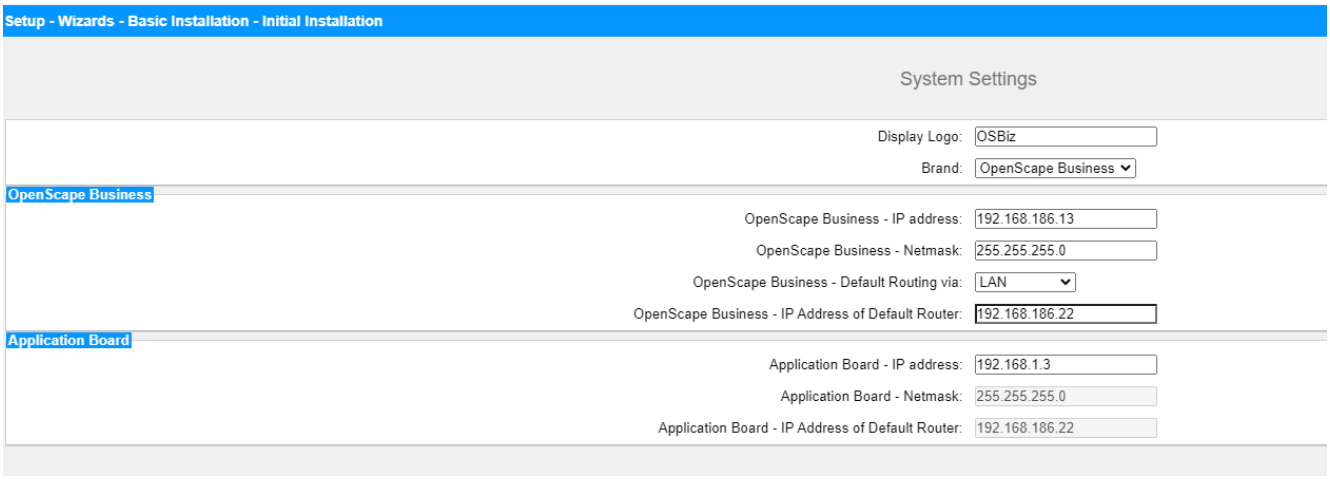
Edit IP addresses (if required) or configure DHCP.

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

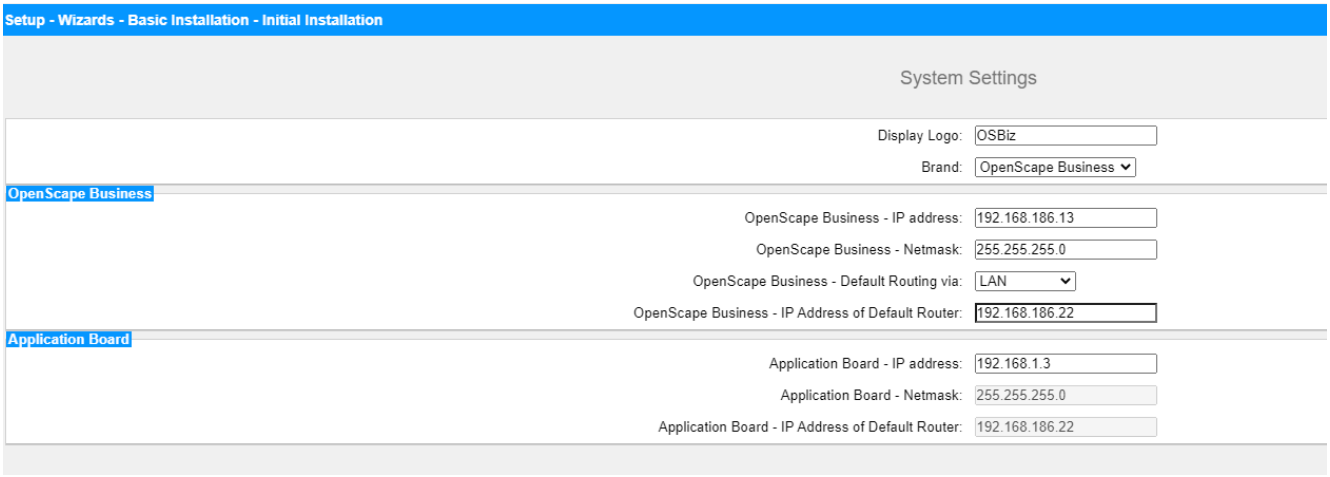
Next steps

Configure DHCP.

7.6.2.3 How to Specify the Device Name

Prerequisites

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



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.

7.6.3 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.

7.6.3.1 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

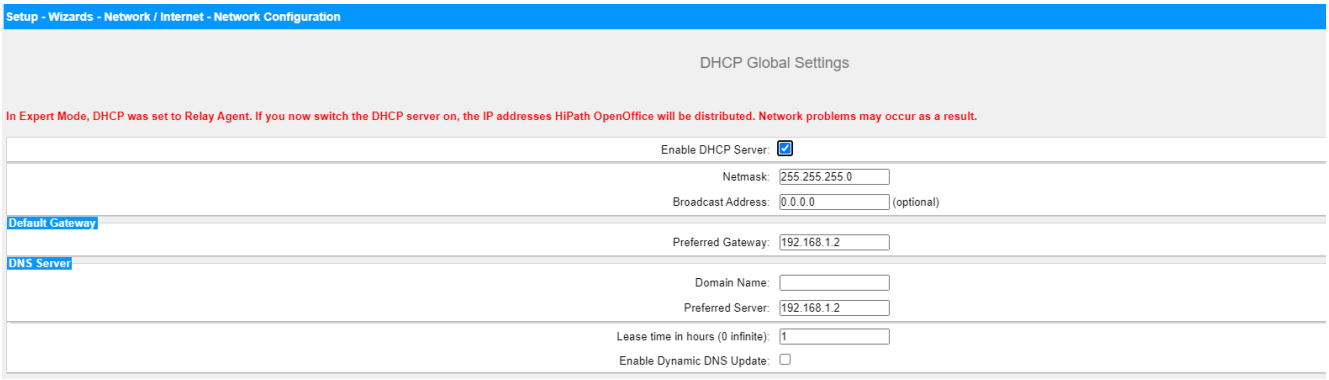
Configure country and time settings.

7.6.3.2 How to Enable and Configure the Internal DHCP Server

Prerequisites

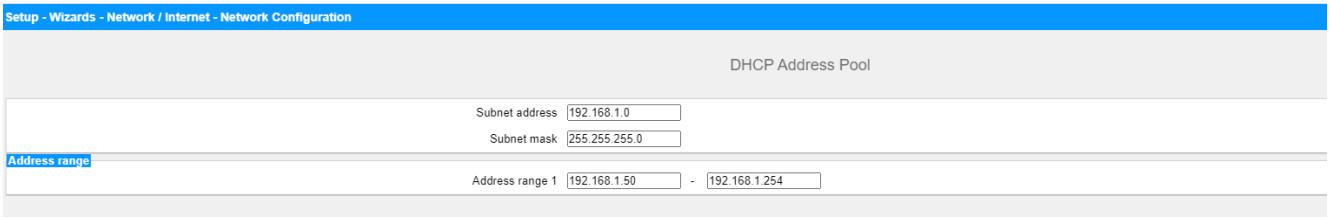
The external DHCP server (e.g., the DHCP server of the Internet router) has been disabled in the internal network.

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`

   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.

7.6.4 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

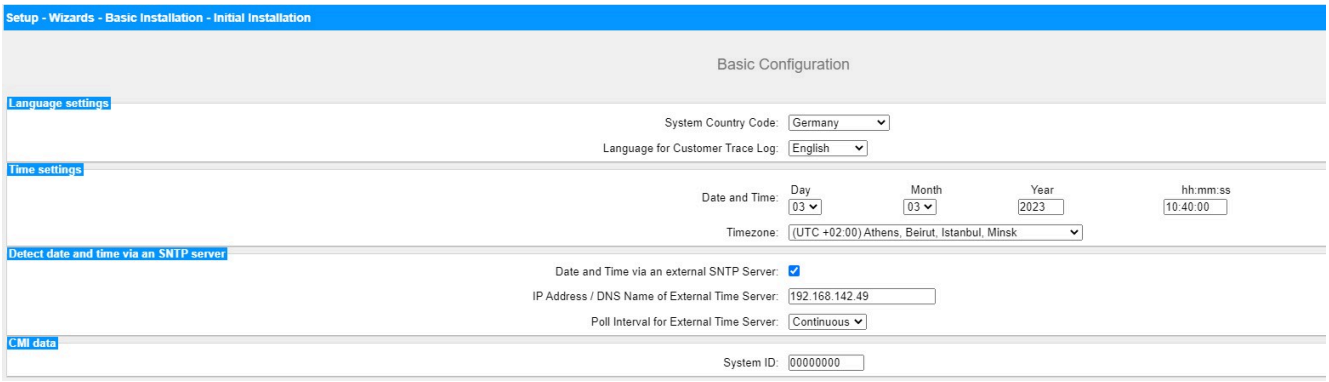
  The communication system and IP stations (IP phones, client PCs) should have a uniform time base (date and time). This time base can be provided by an SNTP server. The SNTP server can be located on the internal network or the Internet.

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).

7.6.4.1 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)

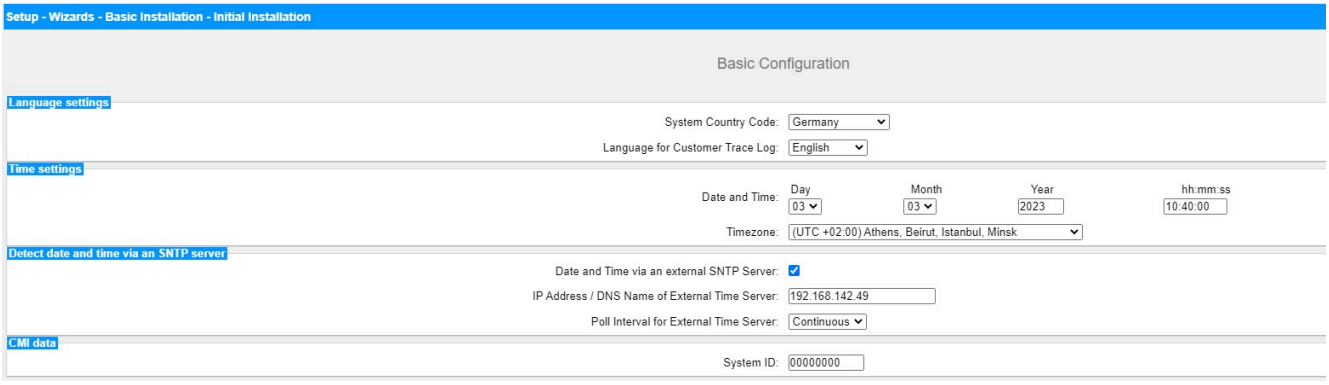
or

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

7.6.4.2 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.

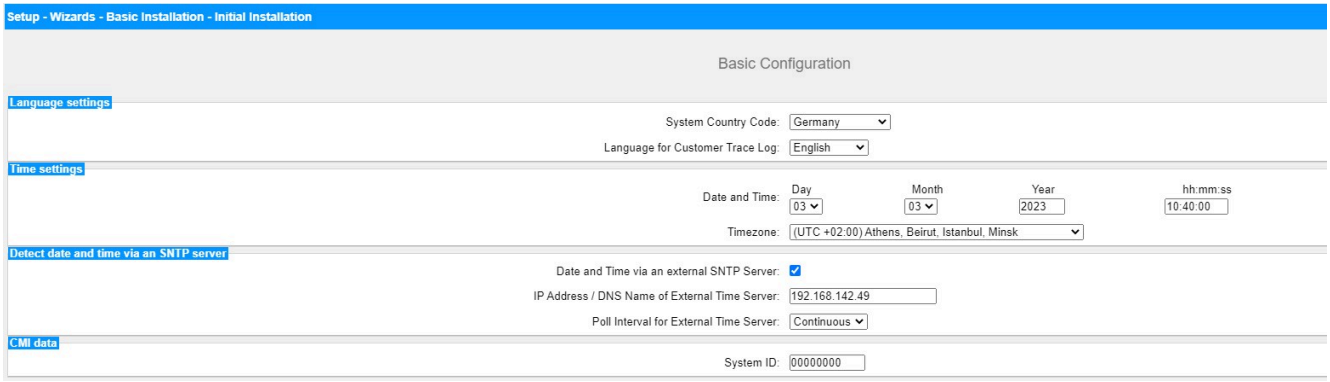
Next steps

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

7.6.4.3 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.

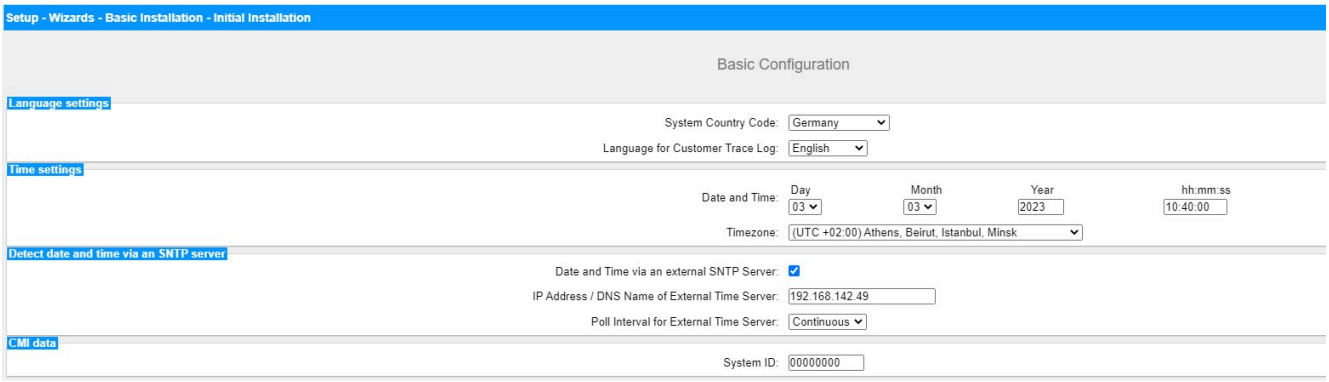
Next steps

Specify UC solution.

7.6.4.4 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.

7.6.5 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**

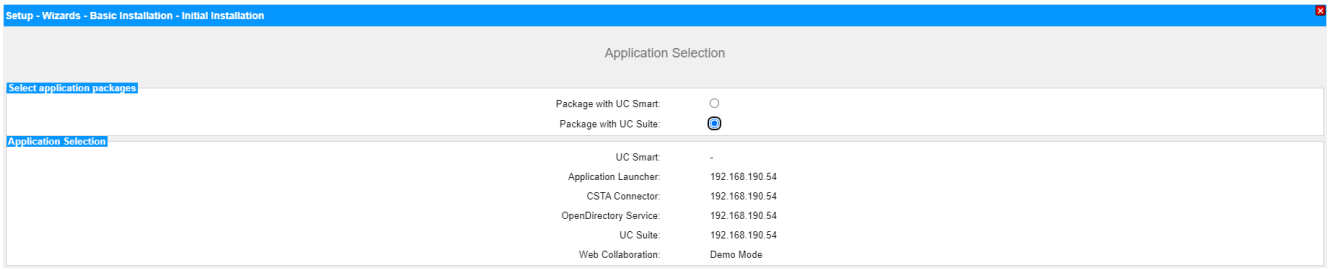
  The UC solution UC Suite is integrated on the OpenScape Business X mainboard.

7.6.5.1 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, click **Package with UC Smart**.
2) If you want to use the UC solution UC Suite, click on **Package with UC Suite**.
3) Click on **OK & Next**.
4) The **Initial installation** wizard is closed. Click **Finish**.
5) 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.

7.6.6 Connecting the Communication System to the Customer LAN

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

7.6.6.1 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.

Next steps

Start the basic configuration.

7.7 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.

7.7.1 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.

7.7.2 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

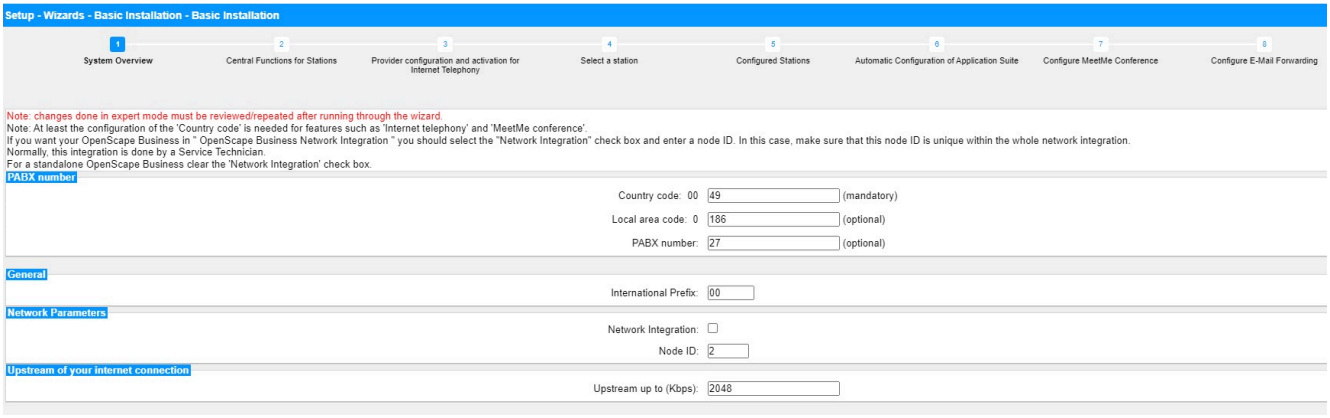
   If OpenScape Business is to be networked with other OpenScape Business systems, networking must be enabled, and OpenScape Business must be assigned a node ID. Every OpenScape Business must have a unique node ID in the network.

7.7.2.1 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 **System Overview** 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

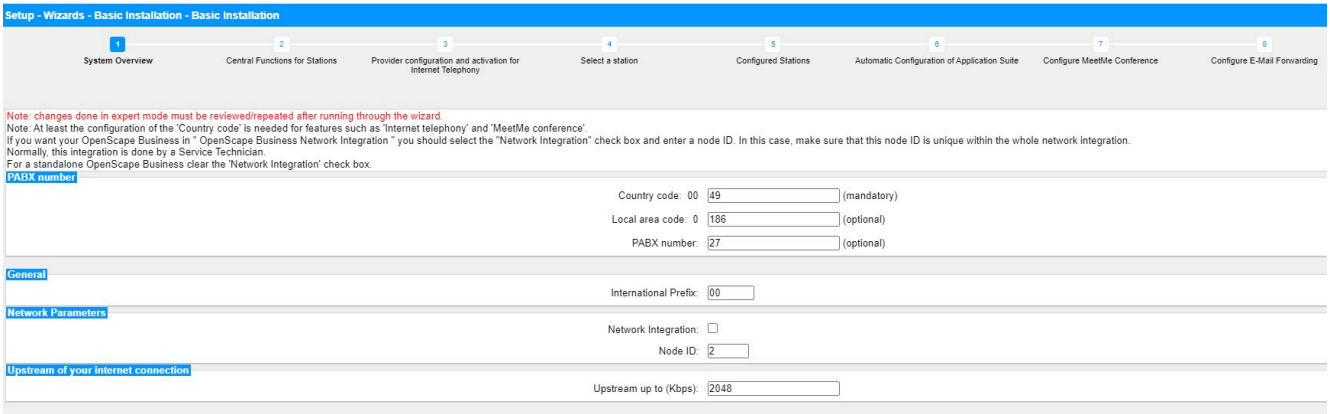
Activate or deactivate networking

7.7.2.2 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 **System Overview** 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.

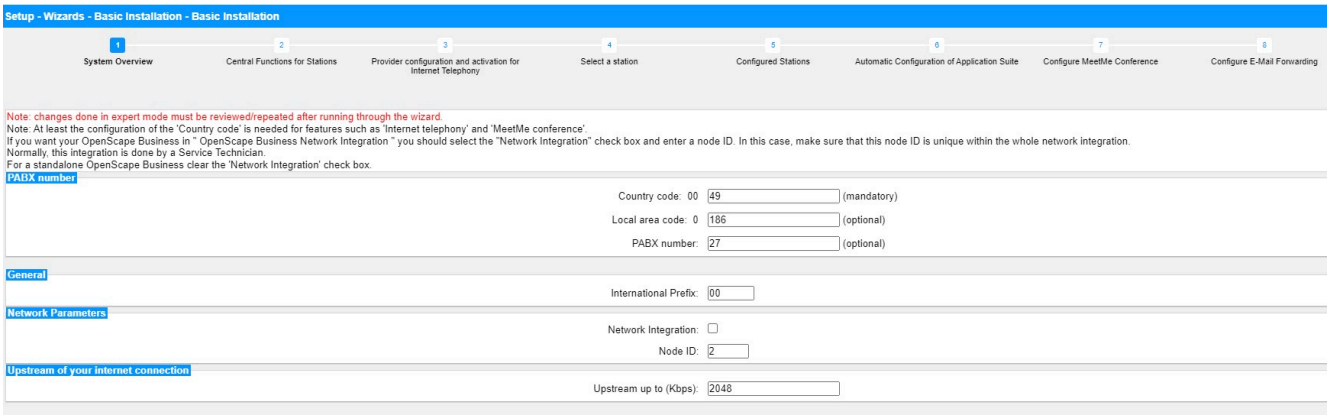
Next steps

Activate or deactivate networking

7.7.2.3 How to Activate or Deactivate Networking

Prerequisites

You are in the **System Overview** 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.

7.7.3 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.

7.7.3.1 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**.

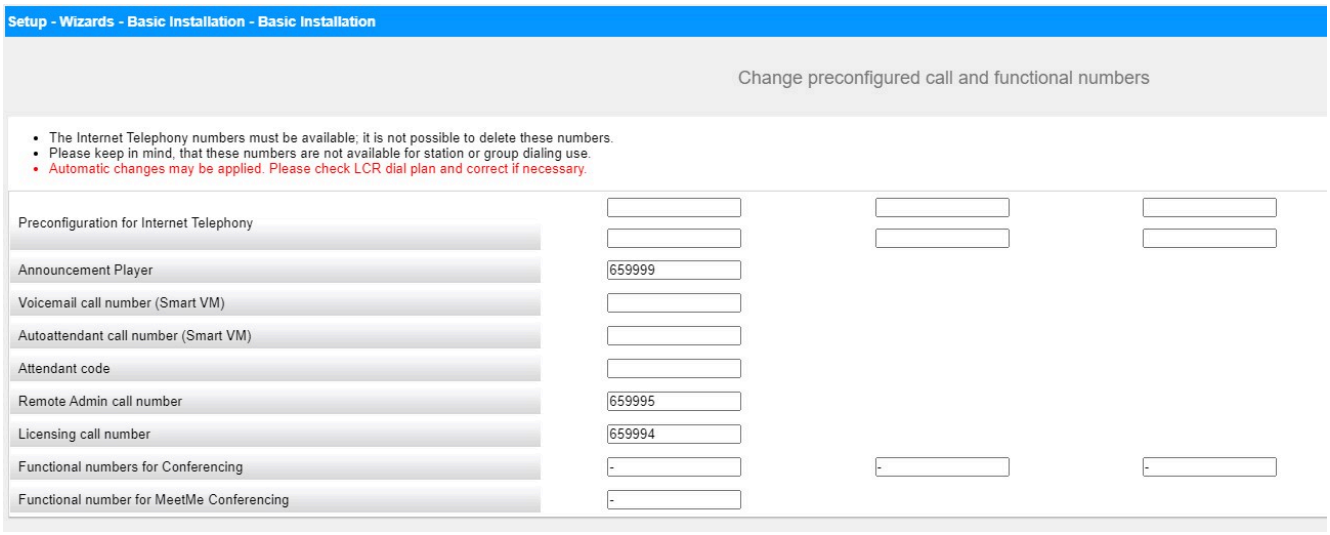
7.7.3.2 How to Delete all Call Numbers

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**.

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

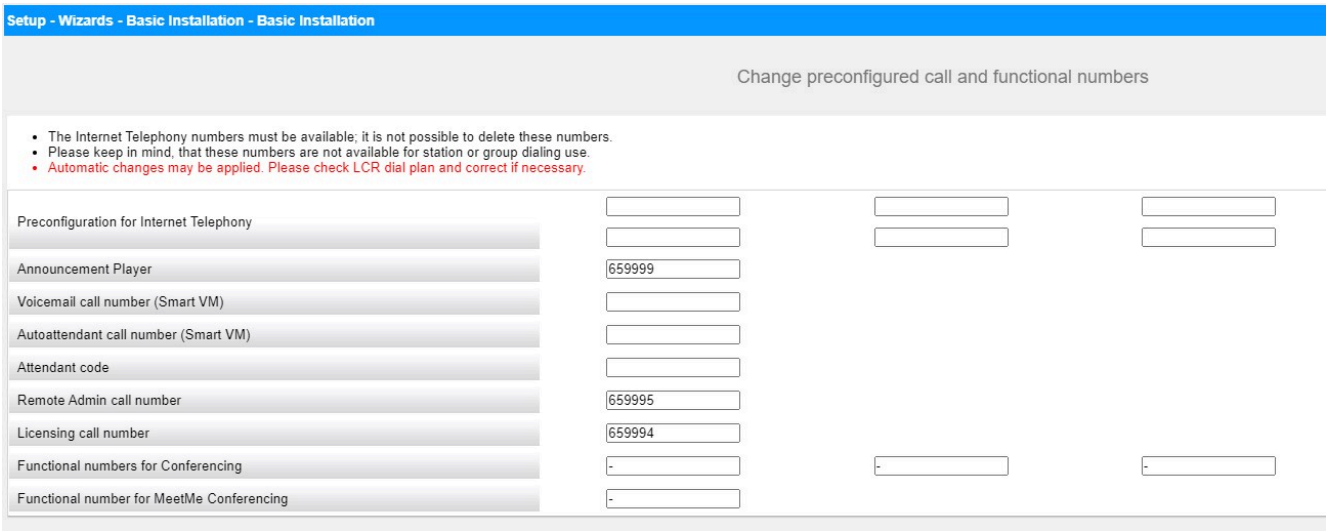
Prerequisites

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**.

7.7.3.4 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**.

7.7.3.5 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.

7.7.4 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.

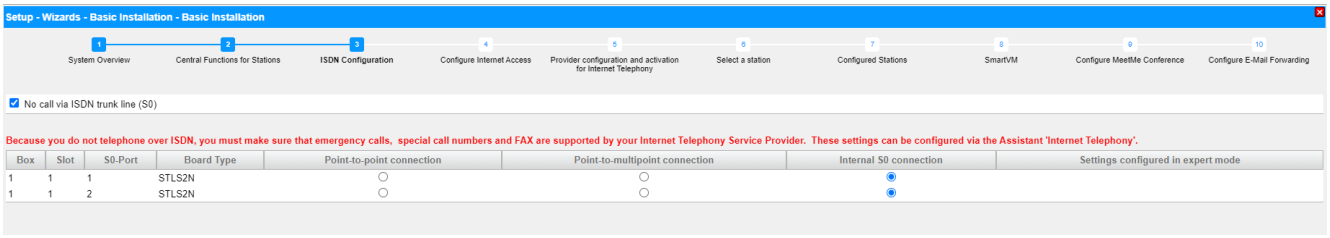
Other options for trunk connections

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.

7.7.4.1 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.

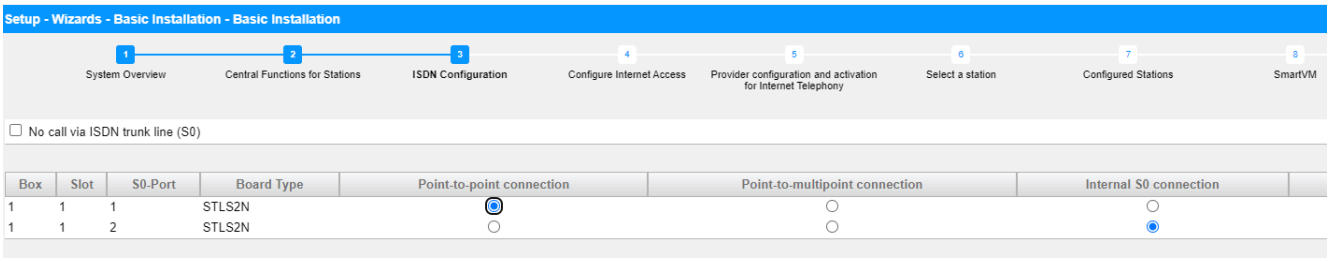
Next steps

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

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

Prerequisites

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



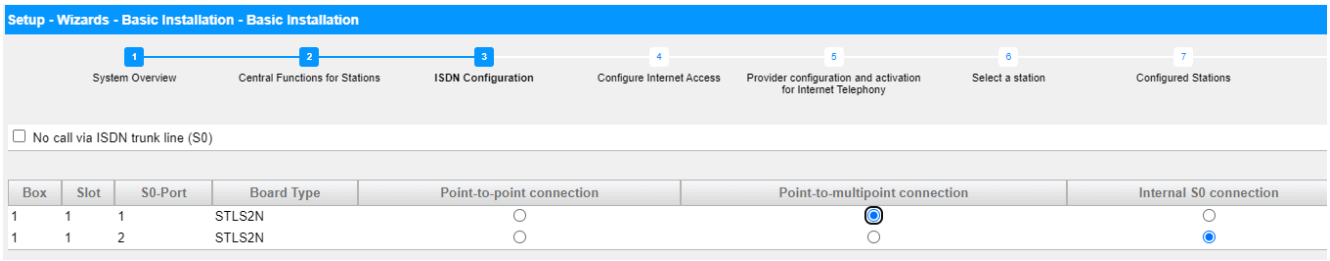
Step by Step

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**.

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

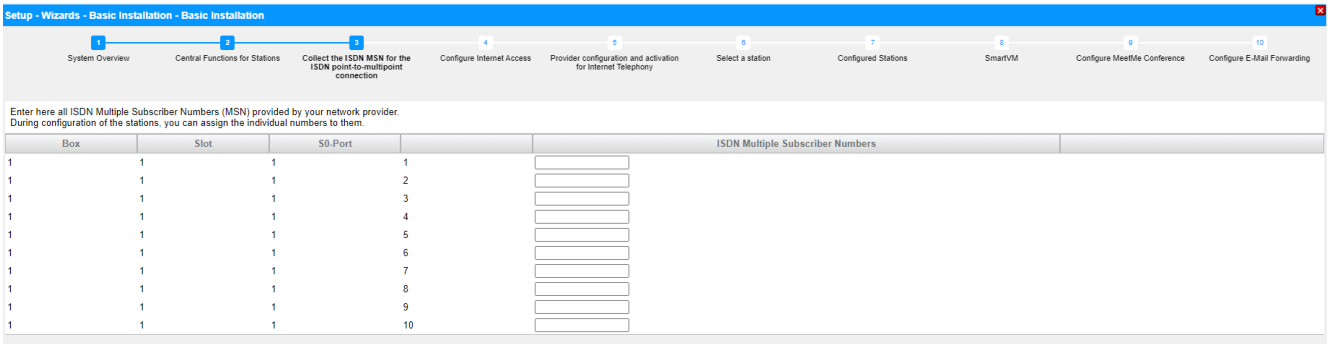
Prerequisites

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**.

7.7.4.4 How to Deactivate the ISDN Configuration

Prerequisites

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

Step by Step

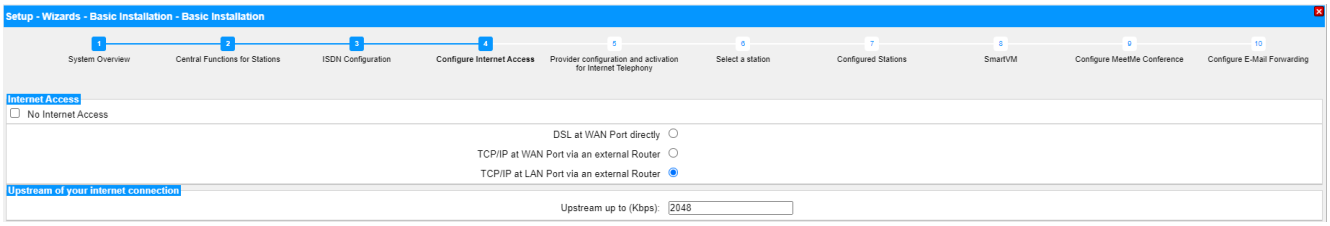
1) Select the **No call via ISDN trunk line (S0)** check box.

> **NOTICE:** Calls can also be conducted via an Internet Telephony Service Provider; see Internet Telephony on page 180.

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

7.7.5 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:

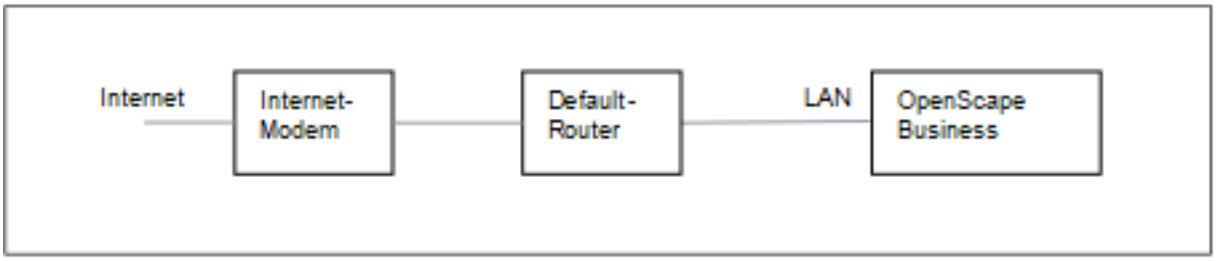
  – **Internet access via an external Internet router at the WAN port**

    (**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.

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

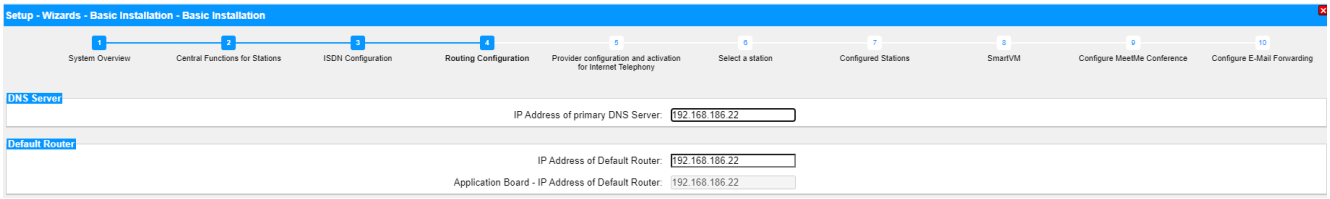
Prerequisites

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**.

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

Prerequisites

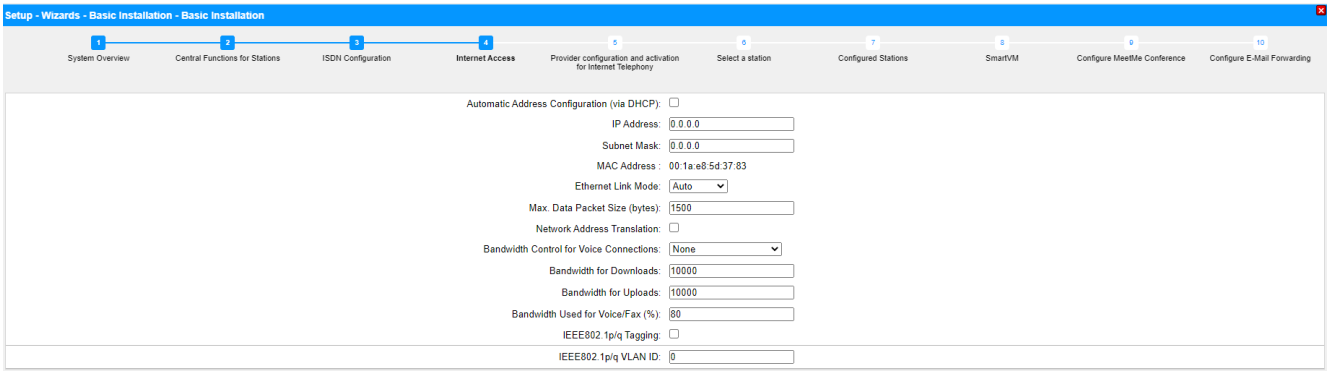
The communication system must be connected to the LAN segment of the customer LAN in which the Internet router is located via the LAN interface "WAN".

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**.

7.7.5.3 How to Configure Internet Access via a Preconfigured ISP

Prerequisites

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

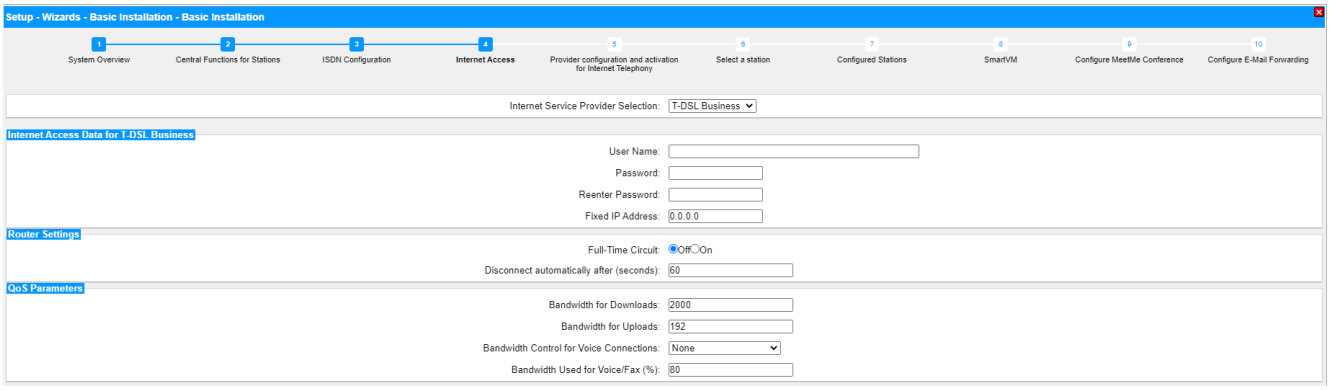
Your ISP's Internet access data is available (for example, user account, password, bandwidth for upload and download, etc.).

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**.

7.7.5.4 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**.

7.7.5.5 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.	

Field	Description	Value from ISP
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 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**.

7.7.5.6 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**.

7.7.6 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 **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

Internal call number	Name	DID
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).

7.7.6.1 How to Configure a Predefined ITSP

Prerequisites

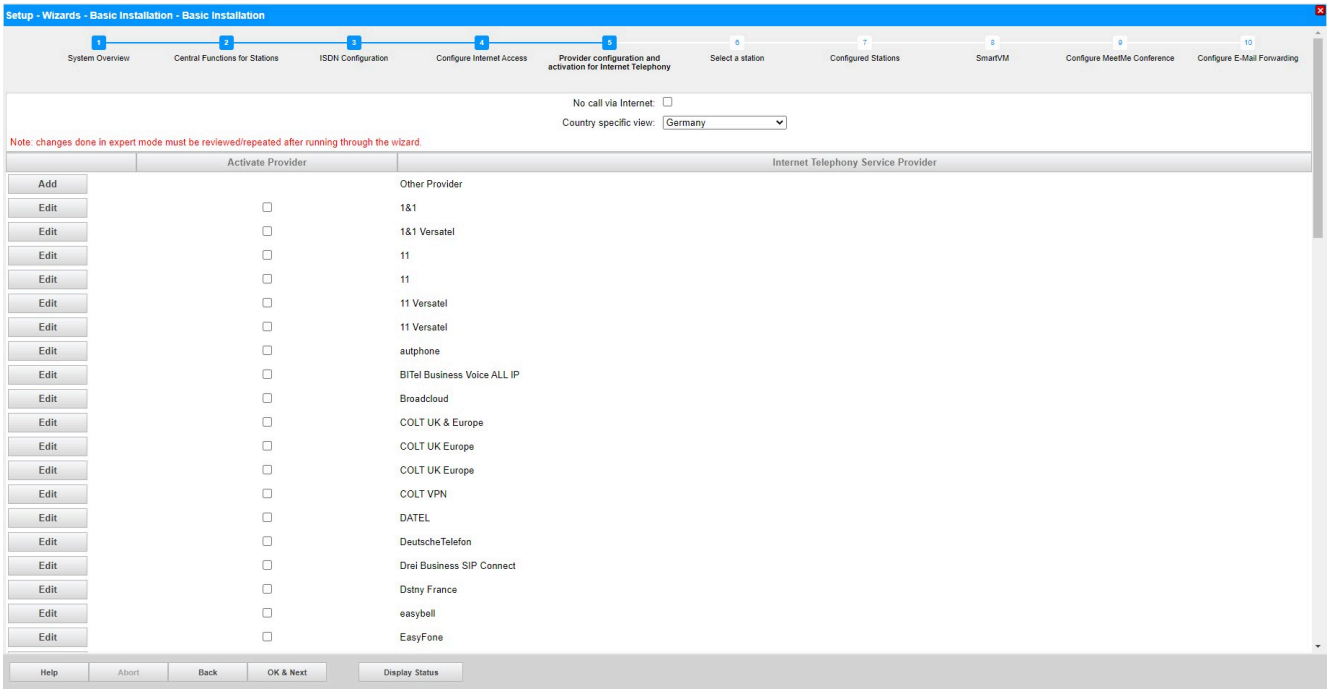
You are in the **Provider configuration and activation for Internet Telephony** window.

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

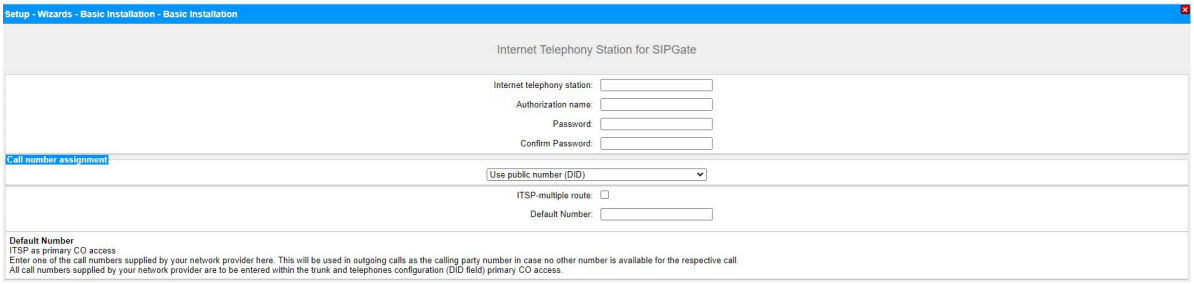
configured under each ITSP. You can activate a maximum of 8 ITSPs. Click **OK** when finished.

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.

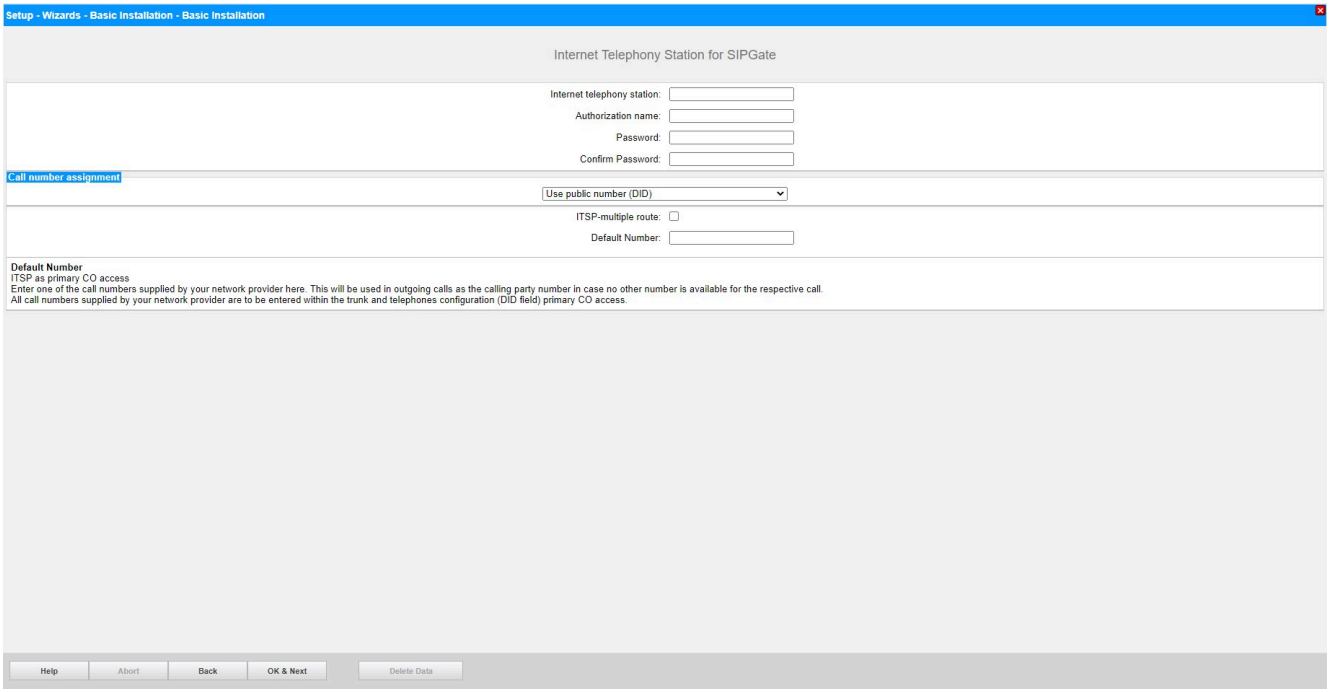
9) Enter the authorization name in the **Authorization name** field. You received this data from your ITSP. If you have not received any authorization name, enter the same data you entered under **Internet Telephony Station**.

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 (CalIno) / 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.

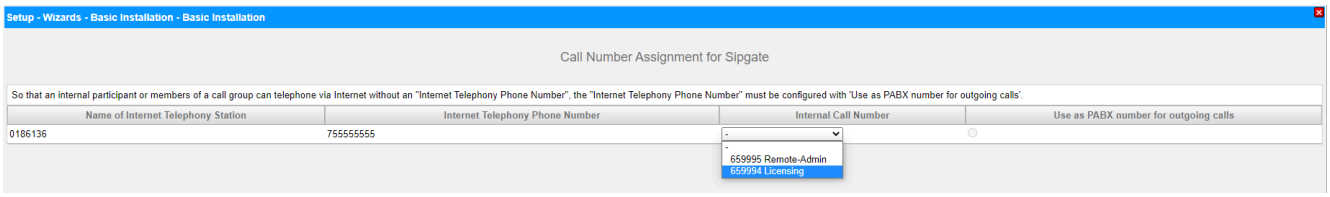
14) Click on **OK & Next**.

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**.

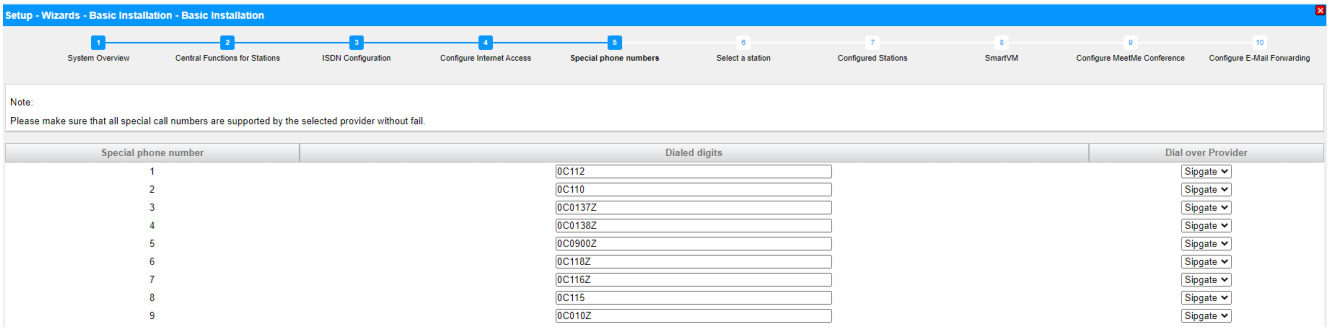
22) If you did not activate the full-time circuit when setting up your Internet access, you can now do this here. Without a permanent connection (full-time circuit), you cannot receive calls over the Internet. If the full-time circuit has already been set up, the fields described under a) to c) will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

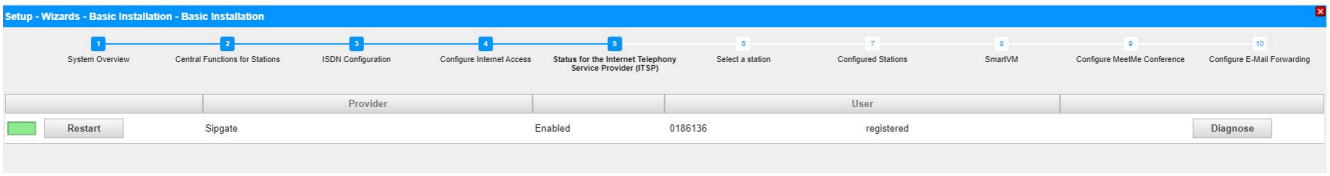
- 0 to 9: allowed digits
- -: Field separator
- X: Any digit from 0 to 9
- N: Any digit from 2 to 9
- Z: One or more digits to follow up to the end of dialing
- C: Simulated dial tone (can be entered up to three times)

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**.

7.7.6.2 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.

7.7.7 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

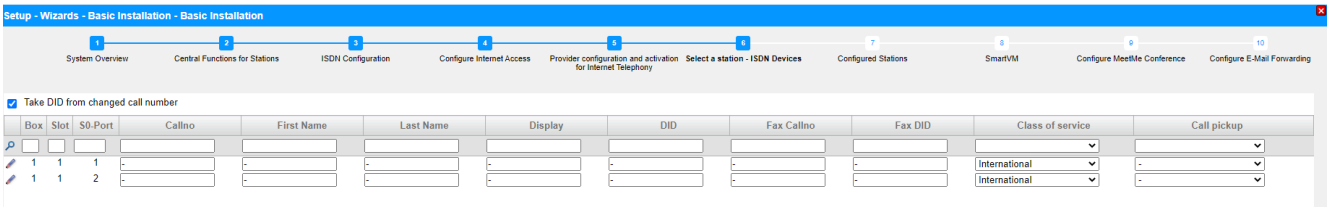
IP and SIP stations include LAN phones or WLAN phones, for example.

7.7.7.1 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.

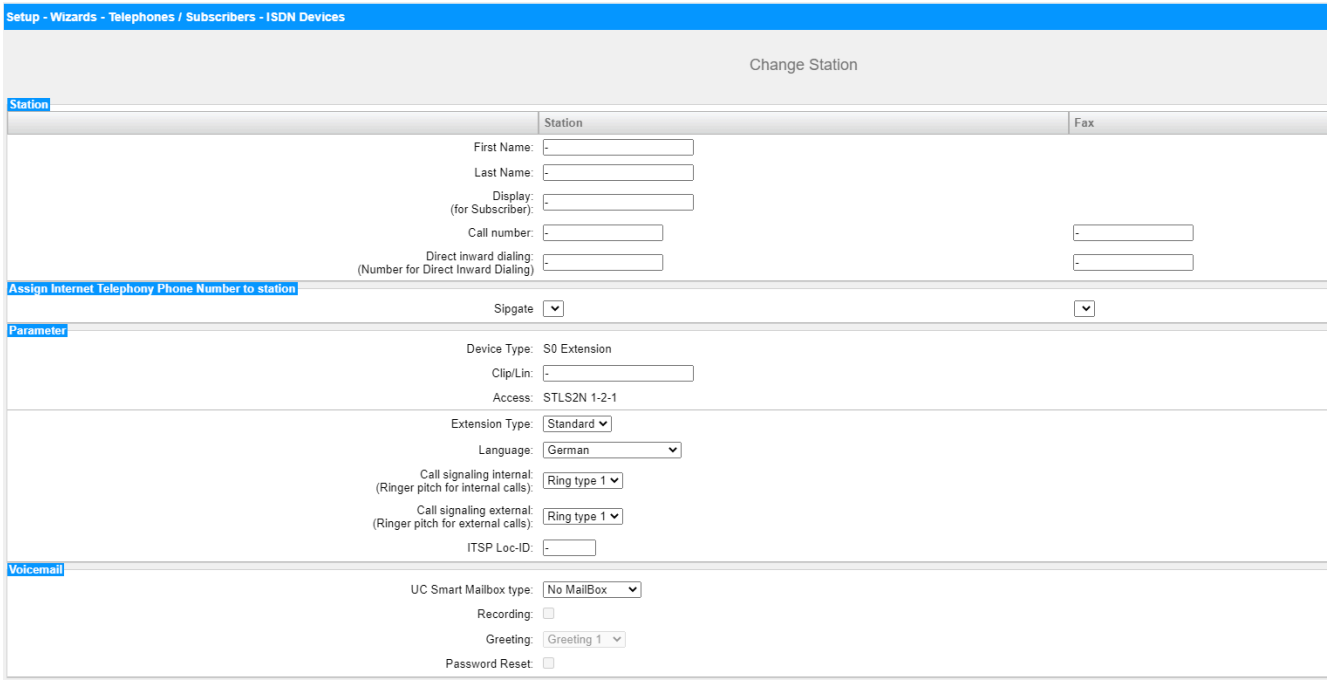
b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.

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.

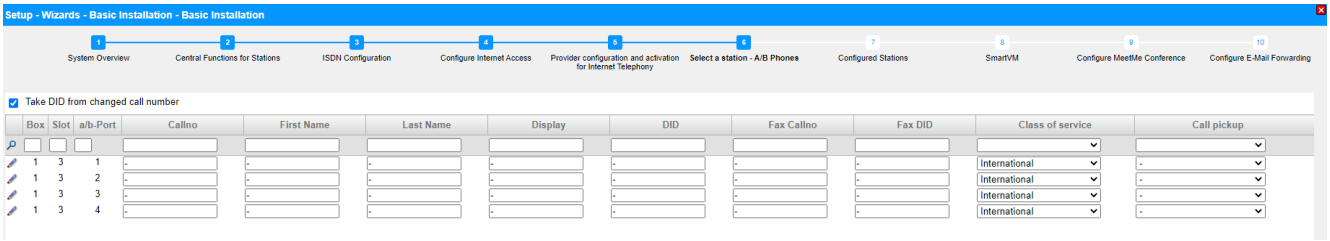
9) Click on **OK & Next**.

7.7.7.2 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:

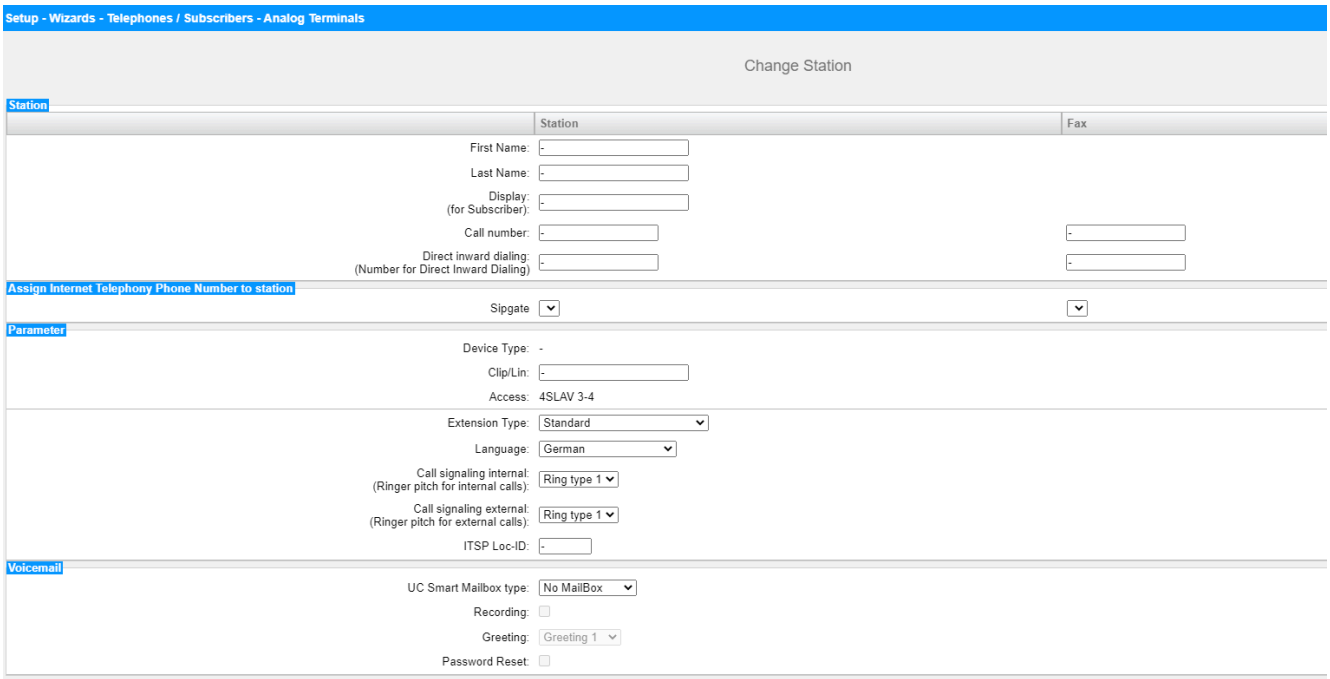
  Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

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.

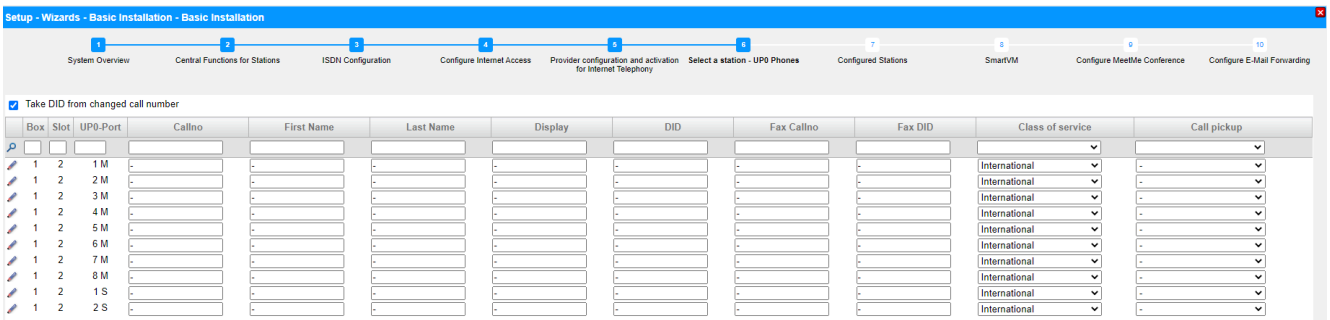
9) Click on **OK & Next**.

7.7.7.3 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:

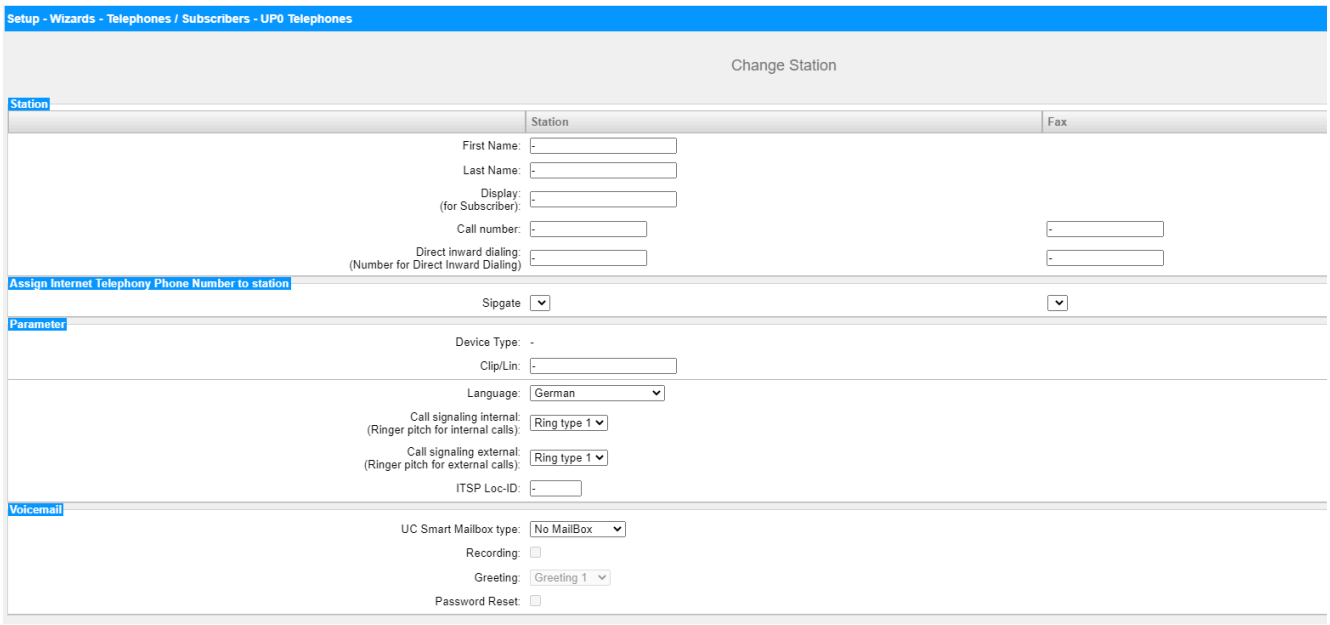
     Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
   - For point-to-point and point-to-multipoint connections:

     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.

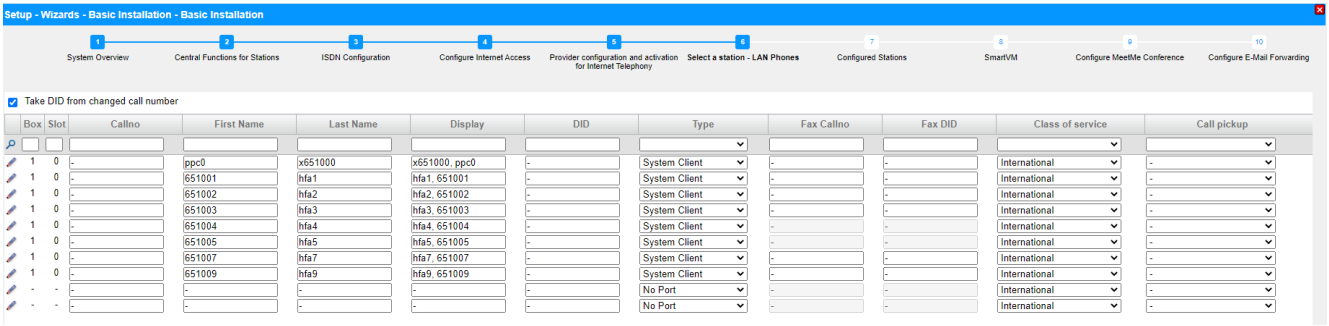
9) Click on **OK & Next**.

7.7.7.4 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.

---

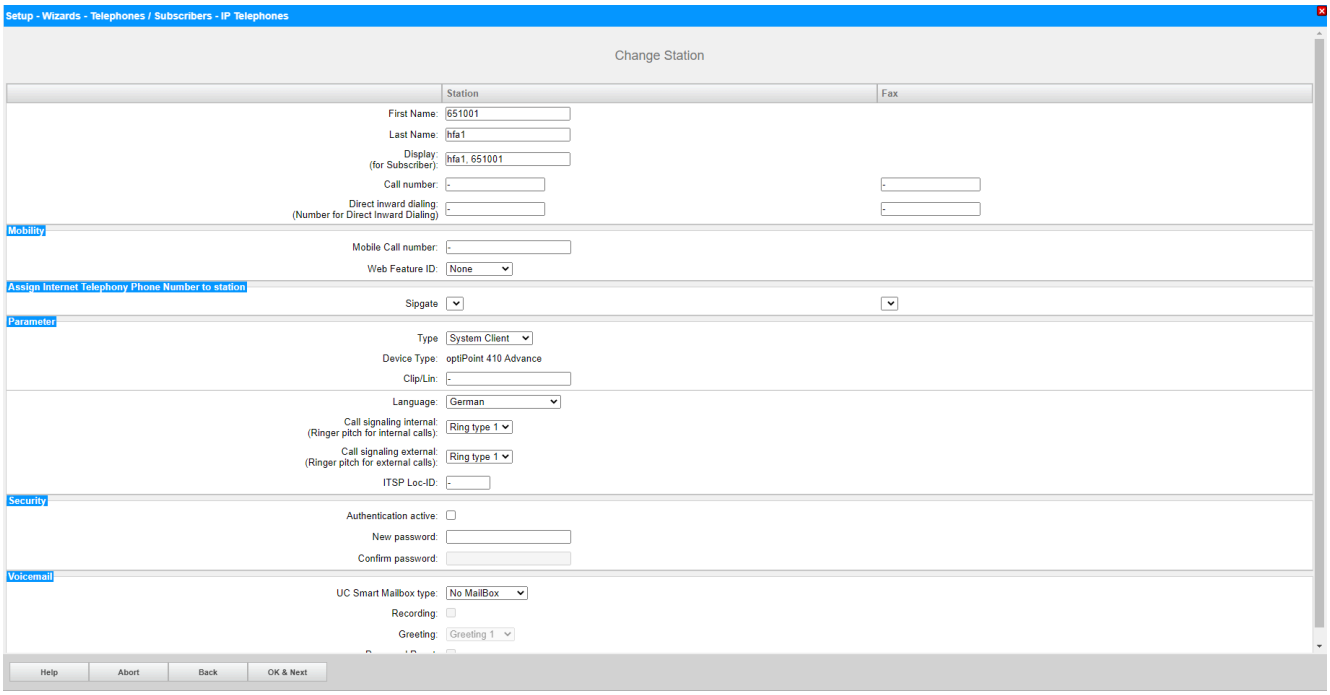
5) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

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.

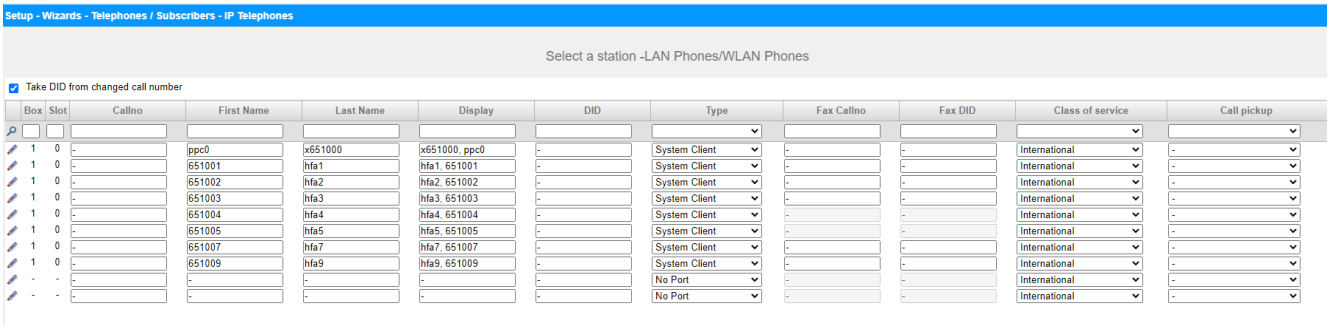
10) Click on **OK & Next**.

7.7.7.5 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.

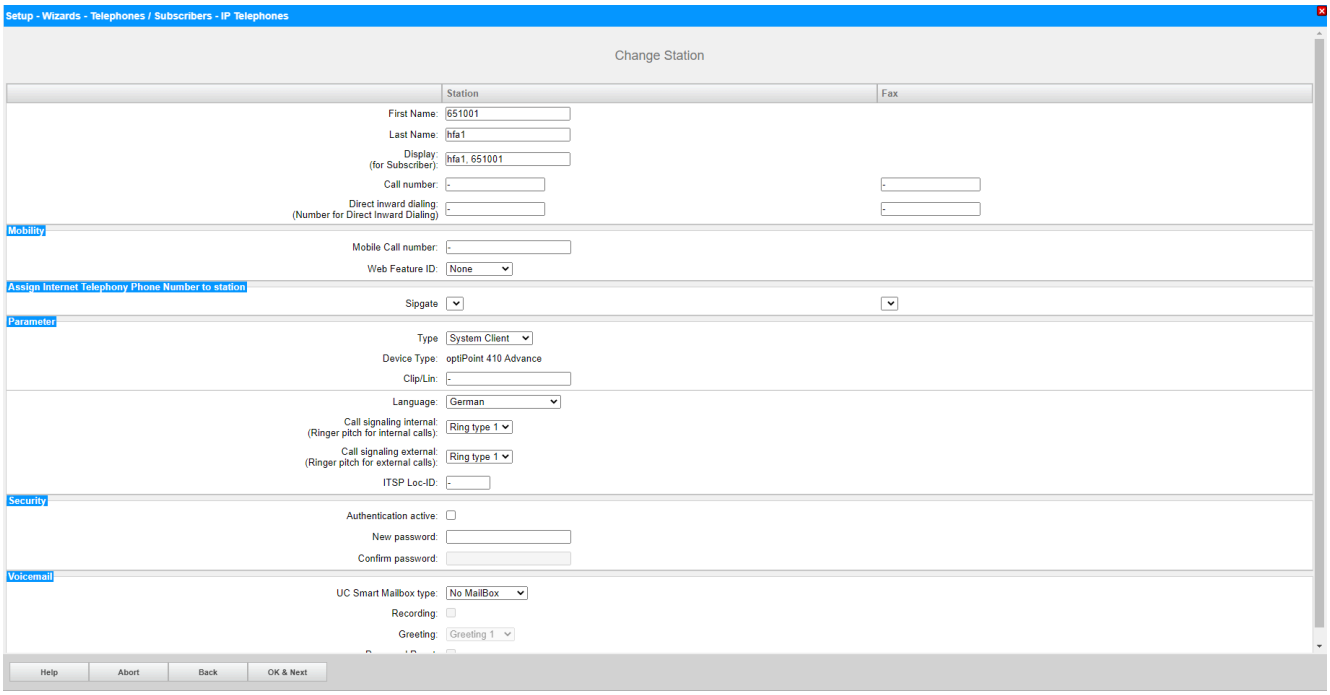
   b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.

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**.

7.7.8 Configuring UC Suite

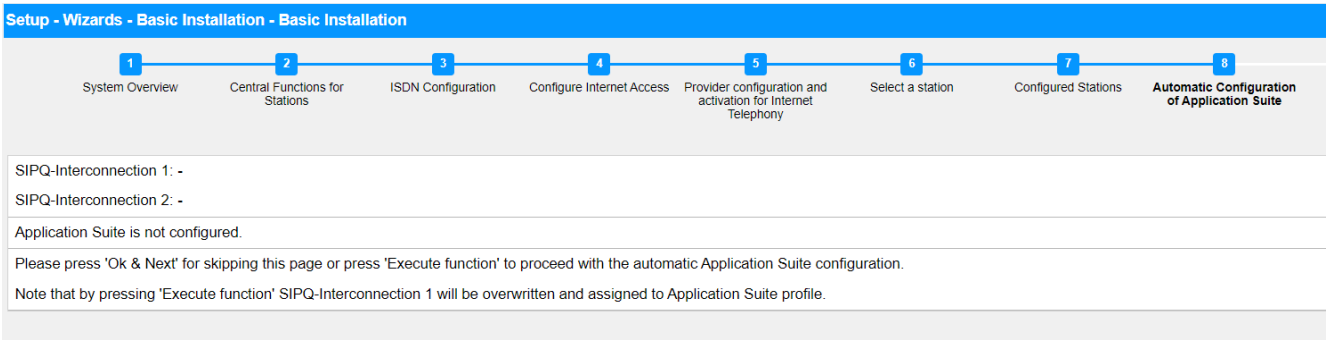
You can perform the automatic configuration of the UC solution UC Suite in the **Automatic Configuration of the Application Suite** window.

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

7.7.8.1 How to Configure the UC Suite

Prerequisites

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



Click **OK & Next**. The configuration will be skipped.

7.7.9 Configuring UC Smart Mailboxes

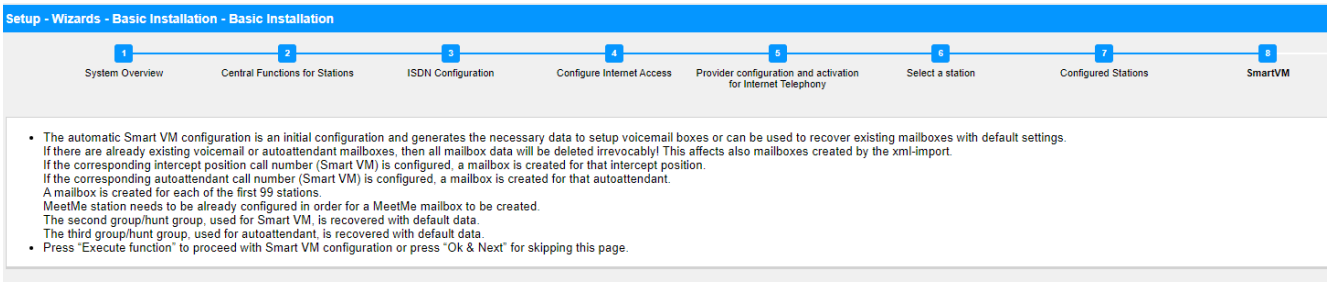
If you are using the UC solution UC Smart, you can perform the automatic configuration of the UC Smart voicemail boxes (Smart VM, Smart VoiceMail) in the **Automatic Configuration of Smart VM** window.

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

7.7.9.1 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.

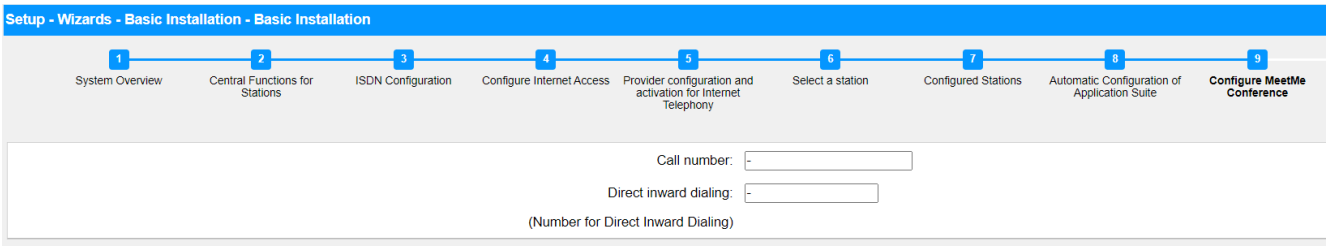
7.7.10 Conference Server Settings

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

7.7.10.1 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**.

7.7.11 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.

7.7.11.1 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.

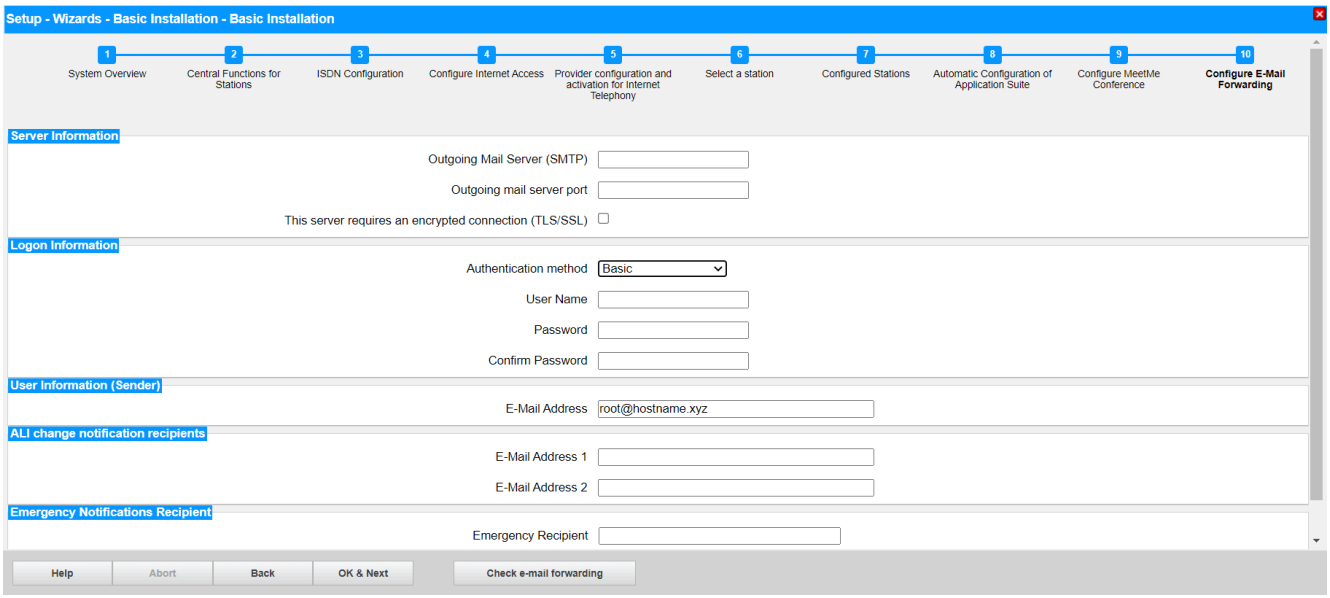


Figure 15: E-mail forwarding options when basic authentication method is selected

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 204 (**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.

7.8 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) 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.

7.8.1 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.

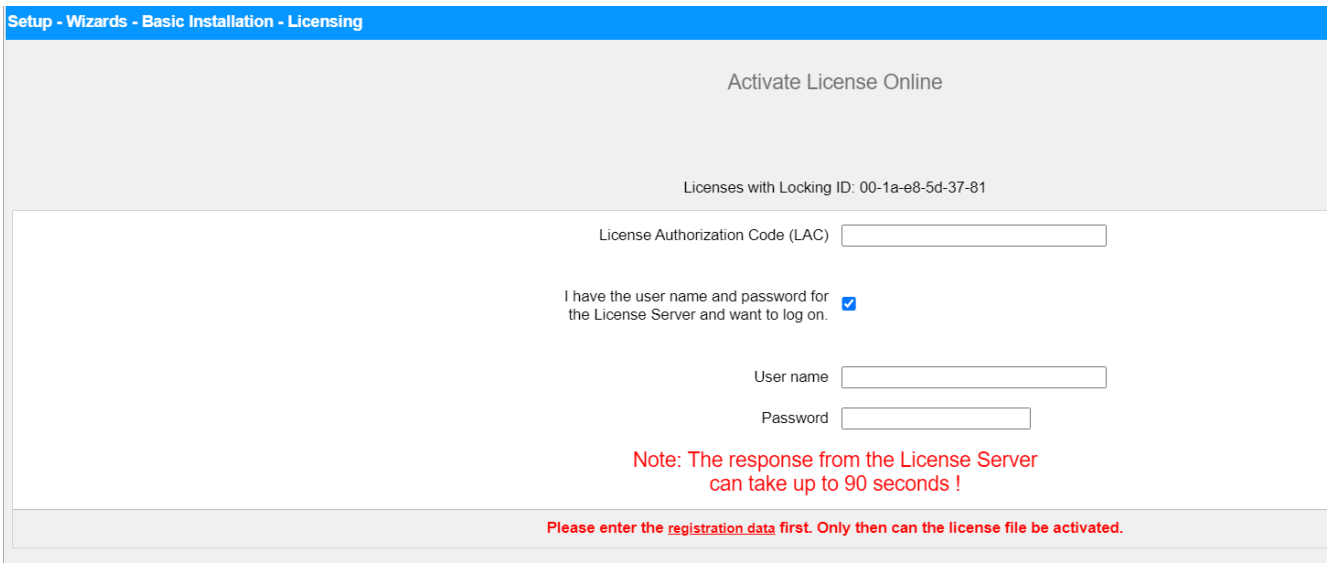
Step by Step

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.

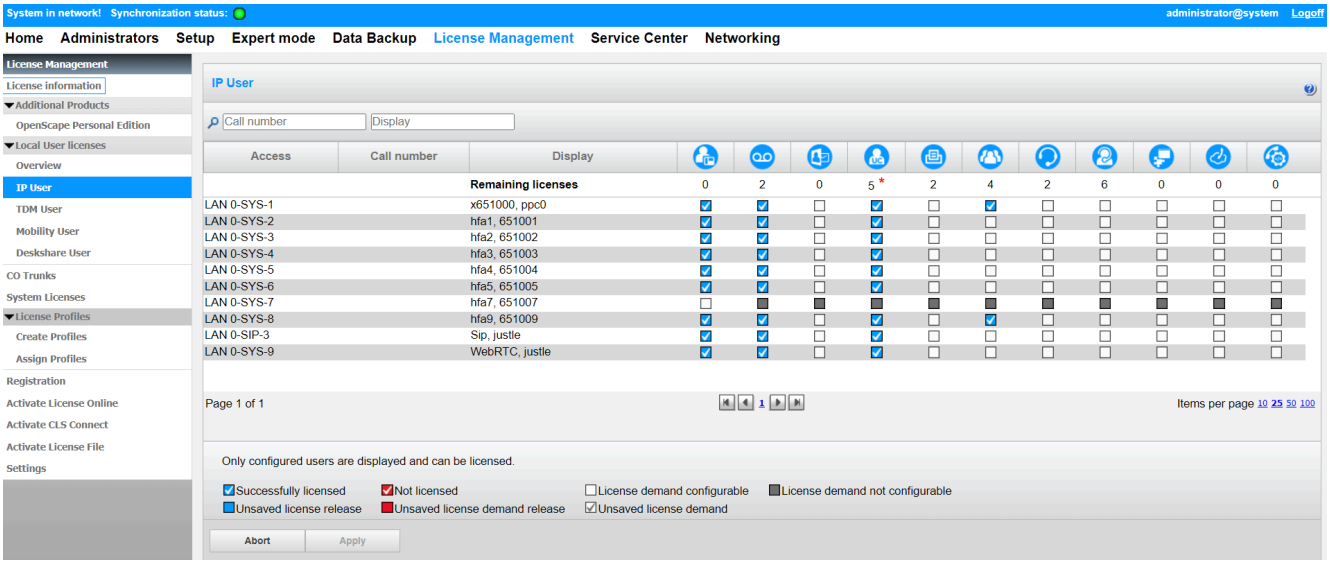
g) Click on **OK & Next**. The connection to the license server is established, and the licenses are released.

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.

7.8.2 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
```

7.8.3 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
   ```

7.8.4 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*).

7.9 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.

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.

7.9.1 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.

7.9.2 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.

8 Discontinued components

This section contains information that is relevant to discontinued components, and are included here only for reference.

8.1 Main Distribution Frame MDFU (Optional)

Telephones, CO trunks, etc., can either be connected directly to the boards of the OpenScape Business X3W and OpenScape Business X5W communication systems or via an external main distribution frame MDFU.

The main distribution frame MDFU (Main Distribution Frame Universal) provides nine slots for splitting and jumper strips.

Dimensions:

- Height = 367.0 mm (3.36 in)
- Width = 328.8 mm
- Depth = 125.4 mm

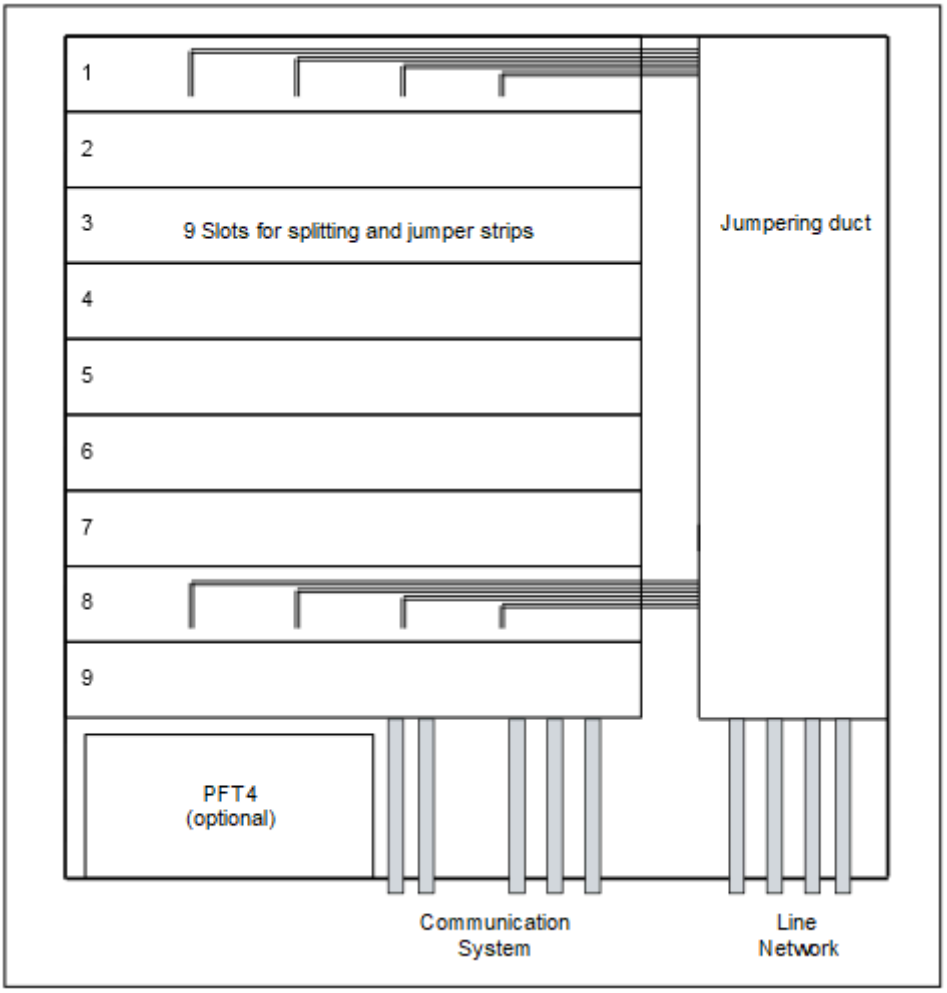


Figure 16: Main Distribution Frame MDFU

NOTICE: If you use a main distribution frame from a third-party vendor rather than the MDFU, you must observe the manufacturer's instructions for installation and protective grounding.

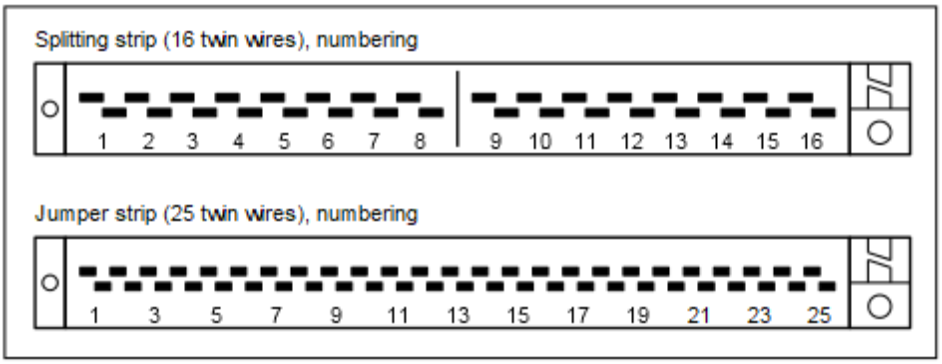


Figure 17: Splitting and Jumper Strip - Numbering of Connectors

8.1.1 How to Mount the Main Distribution Frame MDFU to a Wall

Prerequisites

A strong wall with enough space for the installation of the main distribution frame MDFU is available.

Step by Step

1) Attach the enclosed drilling template at the desired location.
2) Drill the holes.
3) Insert the wall anchors into the drill holes and screw in the screws, leaving approx. 5 mm projecting.
4) Remove the housing cover of the MDFU.
5) Hang the MDFU on the mounting brackets and align it.
6) Tighten the screws.

8.2 Connection Cable to External Main Distribution Frame (Optional)

Telephones, CO trunks, etc., can be connected to OpenScape Business X3W and OpenScape Business X5W either via the main distribution frame MDFU or via another external main distribution frame. A number of different options are available for connecting the communication system with a main distribution frame.

CABLU S30269-Z41-A30

CABLU (24 DA) with

- six Wieland screw clamps for connecting directly to the edge connectors on the boards of the OpenScape Business X3W and OpenScape Business X5W communication systems

- Jumper strip for installation in the MDFU

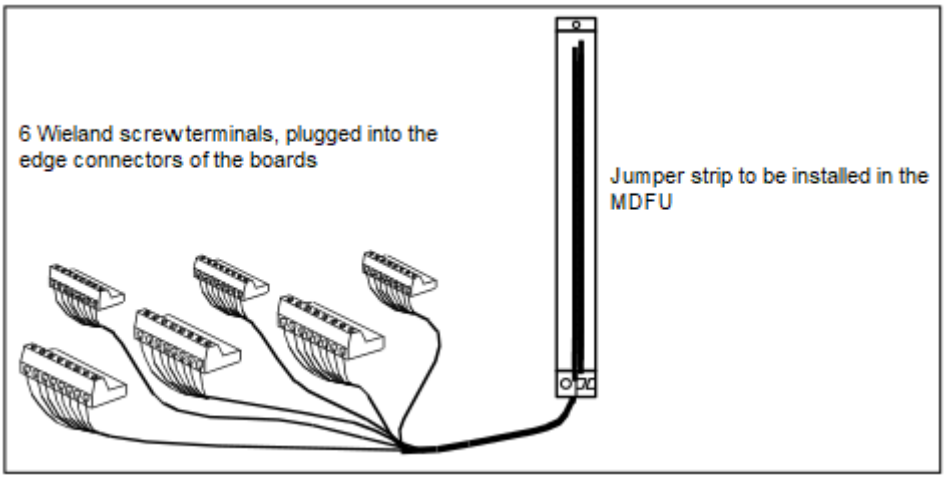


Figure 18: CABLU S30269-Z41-A30

Open-end cable S30267-Z322-Axxx

Open-end cable (24 DA) with six Wieland screw clamps for connecting directly to the edge connectors on the boards of the OpenScape Business X3W and OpenScape Business X5W communication systems. The cable must be connected manually to a splitting/jumper strip in the MDFU or any other external main distribution frame.

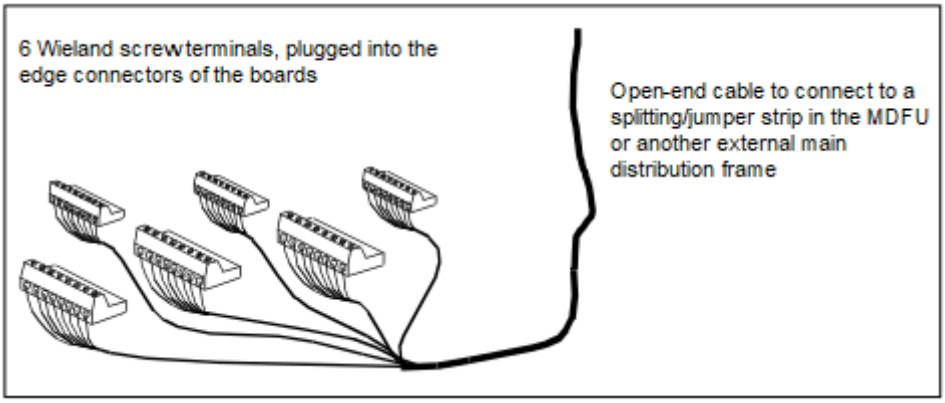


Figure 19: Open-end cable S30267-Z322-Axxx

CABLU S30269-Z100-A11/-A21

CABLU (16 DA) with

- one SIPAC 1 SU jack for connection to the backplane connector X8 of the OpenScape Business X5W communication system
- Splitting strip for installation in the MDFU

CABLU S30269-Z100-A14/-A24

CABLU (24 DA) with

- two SIPAC 1 SU jacks for connection to the backplane connectors X8 and X9 of the OpenScape Business X5W communication system
- Jumper strip for installation in the MDFU

CABLU S30267-Z346-A30

CABLU with

- one SIPAC 1 SU jack for connection to the backplane connector X8 of the OpenScape Business X5W communication system
- CHAMP connector for connecting an external main distribution frame

8.2.1 How to Connect a Connection Cable to the External Main Distribution Frame (Optional)

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.

The housing cover of the communication system is not mounted.

Step by Step

1) Select the appropriate connection cable based on the communication system and the board.

If		Then
Communication system	**Board**	**Connection cable**
OpenScape Business X3W	All peripheral boards and the OCCM, OCCMA and OCCMB mainboard	Connection to the external MDF: CABLU with six Wieland screw clamps (for direct connection to the edge connectors of the boards) and jumper strip for 24 DA: • S30269-Z41-A30: 3 m length Connection to the MDFU or to another external main distribution frame: Open-end cable (24 DA) with six Wieland screw clamps (for direct connection to the edge connectors of the boards): • S30267-Z322-A100: 10 m length

If		Then
Communication system	Board	Connection cable
OpenScape Business X5W	All peripheral boards (except for peripheral boards in SIPAC format) and the mainboard OCCM, OCCMA and OCCMB	Connection to the MDFU: CABLU with six Wieland screw clamps (for direct connection to the edge connectors of the boards) and jumper strip for 24 DA: • S30269-Z41-A30: 3 m length Connection to the MDFU or to another external main distribution frame: Open-end cable (24 DA) with six Wieland screw clamps (for direct connection to the edge connectors of the boards): • S30267-Z322-A100: 10 m length

2) Select one of the following connectivity options for the communication system:
   - If you are using a CABLU with six Wieland screw clamps, attach the screw clamps to the desired edge connectors of the desired boards.
   - If you are using a CABLU with one SIPAC 1 SU jack, connect the cable to the backplane connector X8.
3) Attach the connection cable to the communication system using cable ties.
4) Select one of the following options to connect to the MDFU or any other external main distribution frame:
   - If you use the MDFU and a CABLU with a splitting strip or a jumper strip, install the strip in the MDFU.

     For information on the main characteristics of the MDFU and on the numbering of the splitting and jumper strips see Main Distribution Frame MDFU (Optional).
   - If you use the MDFU and an open-end cable, connect the cable to the desired splitting/jumper strip in the MDFU.

     Procedure:

     Strip the cable wires.

     Strip the cable shield of the cable over a length of about 3 cm. Cut the drain wire to about 2.5 cm and fix it on the cable shield by wrapping it with tape (at least 1.5 times around).

     Use a standard wiring tool for laying the cable wires.

     Table 8: Color Codes for the Open-End Cable

Color Group	Pair	A-wire	B-wire
1	1	white/blue	
			blue/white
	2	white/orange	
			orange/white
	3	white/green	

Color Group	Pair	A-wire	B-wire
			green/white
	4	white/brown	
			brown/white
	5	white/gray	
			gray/white
2	6	red/blue	
			blue/red
	7	red/orange	
			orange/red
	8	red/green	
			green/red
	9	red/brown	
			brown/red
	10	red/gray	
			gray/red
3	11	black/blue	
			blue/black
	12	black/orange	
			orange/black
	13	black/green	
			green/black
	14	black/brown	
			brown/black
	15	black/gray	
			gray/black
4	16	yellow/blue	
			blue/yellow
	17	yellow/orange	
			orange/yellow
	18	yellow/green	
			green/yellow
	19	yellow/brown	
			brown/yellow
	20	yellow/gray	
			gray/yellow
5	21	purple/blue	

Color Group	Pair	A-wire	B-wire
			blue/purple
	22	purple/orange	
			orange/purple
	23	purple/green	
			green/purple
	24	purple/brown	
			brown/purple

For information on the main characteristics of the MDFU and on the numbering of the splitting and jumper strips see Main Distribution Frame MDFU (Optional).

- If you use an external main distribution frame with CHAMP connectors and a CHAMP cable, insert the connector into the desired CHAMP jack of the external main distribution frame.
- If you use another external main distribution frame and an open-end cable, connect the cable to the desired splitting/jumper strip in the external main distribution frame.

5) Attach the connection cable to the MDFU or to the external main distribution frame using cable ties.

Index

P

R

S

T

U

W