SWYXWARE

ADMINISTRATOR DOCUMENTATION

As of: April 2025

Legal information

Trademarks: Swyx, SwyxIt! and SwyxON are registered trademarks of Enreach GmbH.

All other trademarks, product names, company names, trademarks and service marks are the property of their respective owners.

The contents of this documentation are protected by copyright. Publication in the World Wide Web or in other services of the Internet does not constitute a declaration of consent for other use by third parties. Any use not permitted under German copyright law requires the prior written consent of Enreach GmbH.

The information in this documentation has been carefully checked for correctness, but may contain errors due to constant updating and changes.

Enreach GmbH assumes no responsibility for printing and writing errors.

Despite careful control of the content, Enreach GmbH accepts no liability for the content of external links and does not adopt it as its own. The operators of the linked sites are solely responsible for the content of their sites

Enreach GmbH

Robert-Bosch-Straße 1

D-44803 Bochum

office@enreach.de

enreach.com/en

NEW FUNCTIONS

Additional functions and increased flexibility and user-friendliness are typical features of every new version of SwyxWare, making SwyxWare one of the most advanced IP telephone systems on the market.

SwyxWare 14.20- New functions

See ReadMe file:

help.enreach.com/readme/14.00/web/Swyx/en-US/ReadMe.html

Function	Description
Updated Entra ID integration: (extended functionality, simplified configuration)	Contact synchronization Calendar synchronization Microsoft Teams synchronization See help.enreach.com/controlcenter/14.20/web/Swyx/en-US/#context/EntraID
Connection to virtual voice assistants (DialoX Bots)	You can create and manage virtual voice assistants (voice bots) on the DialoX social messaging platform. You can make these bots accessible by telephone via SwyxWare. See help.enreach.com/controlcenter/14.20/web/Swyx/en-US/#context/Botlinks-Overview Further information on DialoX - Social Messaging: help.enreach.com/dialox/1.00/social_messaging/Enreach/en-US/

SwyxWare 14.10 - New functions

Function	Description
Voice message transcription (SwyxON, Swyx Flex only)	Voice message transcription is the conversion of incoming voice messages for users and user groups into text. This function can be activated and configured in Swyx Control Center. See help.enreach.com/controlcenter/14.10/web/Swyx/en-US/#context/GeneralSettings-System-VoiceBox
Advanced configuration of the groups	You can now define the location and call authorization for a group. See *12.2.7 The "Properties..." Dialog The "Advanced" Tab*, Page 223

SwyxWare 14.00- New functions

Function	Description
64-bit	All SwyxServer services are now 64bit executable files. By default, the installation program stores the 64bit components under c:\Program Files\Swyx instead of c:\Program Files (x86)\Swyx. This applies to new installations and updates. If you update an existing supported SwyxWare to v14, the files are stored by default under c:\Program Files\Swyx.

Function	Description
New SwyxIt!	The new SwyxIt! has been introduced as a new Windows client application and offers a modern user interface for improved usability. The former SwyxIt! Client was changed to "SwyxIt! Classic" to differentiate between the new and the classic version of the client. **Default settings** For new SwyxWare installations, the client mode is set to "SwyxIt!" by default. For update installations, the default client mode is set to "SwyxIt! Classic" in order to maintain continuity for existing users. **Configuration** Administrators can configure the default client mode for all users via the Swyx Control Center and adjust this setting for individual users. Users with the appropriate function authorization can switch directly between SwyxIt! and "SwyxIt! Classic" wechseln.

SwyxWare 13.31- New functions

See ReadMe file:

help.enreach.com/readme/13.00/web/Swyx/en-US/ReadMe.html

Function	Description
Improved emergency call recognition and handling of emergency calls in Germany	As of version 13.30, the handling of emergency calls has changed, see *8.1 Emergency call detection*, Page 122
Configuration of the RemoteConnector for SwyxIt! Port forwarding	Access to Swyx VisualGroups or Swyx VisualContacts via RemoteConnector for SwyxIt! if these services are not installed on SwyxServer. See *6.8 Access VisualGroups and VisualContacts on a separate server via RemoteConnector*, Page 79.

Function	Description
RemoteConnector for Yealink	Yealink desk phones can be connected to SwyxON UC Tenants via the Internet, see help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/index.html#context/RemCon_Yealink

SwyxWare13.28

Function	Description
Complex passwords and password history	From version 13.28, the security standards for handling user passwords will be increased. The policy for complex passwords is being expanded. A check is made to ensure that none of the last three passwords used are used again, see *7.1.1 Complex passwords*, Page 81
Password reset service	The password reset service in Swyx Control Center offers the possibility to reset your own password or the password of a user, see *Reset password:*, Page 167

SwyxWare13.27

Function	Description
IMAP4 is no longer supported	As of version 13.27, voice messages are no longer managed via IMAP4 on a mail server, but within SwyxWare. Voice messages can be stored both in the database and in the file system. They can be listed, listened to and deleted with different client applications. This means that voice messages can still be delivered by e-mail, for example. The storage location is configured via the Swyx Control Center, see help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/index.html#context/DataStorage

Function	Description
Changes in the management of trunk recordings	As of version 13.27, trunk recordings can be managed by SwyxWare. They can be stored in the database, in the file system or in an S3 object store. The storage location is configured via the Swyx Control Center, see help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/index.html#context/DataStorage
Group voice messages	As of version 13.27, voice messages can be left on a group call. See *12.2.6 The "Properties..." Dialog The "Voice Box" Tab*, Page 222
Yealink T31G Support	enreach.de/en/products/complete-your-telephone-system/phones-more/desk-telephones.html
SwyxPhone L74 and L77 Support	enreach.de/en/products/complete-your-telephone-system/phones-more/desk-telephones.html

SwyxWare13.00

Function	Description
Swyx Connector for Microsoft Teams	With the Swyx Connector for Microsoft Teams you can useSwyxIt! functions directly on the Microsoft Teams Windows interface, see help.enreach.com/teamsconnector_install/1.00/web/Swyx/en-US/index.html
DCF functions for DECT 800 systems	DECT 800 systems can be provided quickly and easily via DCF. DCF also enables better integration of DECT systems in SwyxWare, see /help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/index.html#context/help/DectSystems

CONTENTS

INTRODUCTION

Enreach develops and markets powerful solutions for company telephony.

In contrast to the old telephone exchanges, the "SwyxWare" telephone system is a pure software solution, using the existing standard computer platform: telephony thus becomes a network application like your e-mail system, your ERP system for company data management, or your CRM system for management of your customer and prospects database.

What is SwyxWare?

Enreach is a software which turns your computer into a powerful and user friendly telephony system.

This telephone system can grow almost seamlessly from a few telephone subscribers to company sizes of around 1000 subscribers, simply by adding licenses and without cost-intensive hardware replacement.

SwyxWare offers a flexibility and capability for its telephone users, who can choose freely between a wide variety of telephone terminals.

You'll find details and advice on the efficient use of SwyxWare, interesting use cases and tips and tricks for the operation of more complex SwyxWare installations, not only in this manual but also on the Enreach Internet pages at:

enreach.com

About this Documentation

This documentation contains the information necessary for making the most effective use of the Swyx solution and the advantages it provides.

Who is this Documentation written for?

The SwyxWare documentation assumes that you, as system administrator, know the platforms used and their conventions.

Accordingly, a detailed description of Windows menu calls, for example, is not included in this documentation, and adequate basic knowledge of network administration is assumed.

Conventions for the Descriptions

Operating Steps

In this documentation, "click" always means: You click the left mouse button once.

Double-click: You quickly click twice with the left mouse button.

If the right mouse button is required for an operating step, it will be indicated explicitly in the text.

"Click with the right mouse button..."

Menu Operation

Instructions which refer to the selection of certain menu entries will be presented as follows:

Lists | Phonebook...

refers to the menu item "Phonebook...", which you will find in the "Lists" menu.

The context menu for an element opens when you click with the right mouse button on the element.

Special design elements

STOP This symbol indicates safety advice: ignoring the advice can lead to material damage or loss of data.

⚠ This represents an advice which should be observed in order to avoid possible license infringements, misunderstandings, malfunctions and delays in software operation.

This indicates information which should not be skipped.

This highlights handy tips, which could be helpful for running the software.

These are instructions,

...which prompt the user to perform an action that can also be performed in several steps (1., 2. etc.).

Online Help

To start the Help system, go to the menu bar and click on "Help | Help Topics...". Many dialogs contain a "Help" button. To receive help for the respective dialog, just click on "Help". Alternatively, press the function key "F1" to start the online help to the respective subject.

Further Information

- For current information on the products, please see our homepage: enreach.com
- Furthermore, in Swyx Help Center, you will find additional information regarding special installation scenarios as well as tips & tricks for the optimal implementation of your SwyxWare. service.swyx.net/hc/en-gb
- The latest documentation for all products can be found in the support area of the homepage: enreach.de/en/products/support/documentation.html

1 THE BASICS

Basic technical concepts of SwyxWare

SwyxWare are available in different variants: SwyxWare for installation in the customer network and the cloud-based variants SwyxWare for DataCenter and SwyxON which can be reached for the customer from the computer center.

> The descriptions in this manual concern in most cases the product variant "SwyxWare". Descriptions concerning SwyxWare for DataCenter and SwyxON are specially emphasized.

SwyxWare for DataCenter and SwyxON

SwyxWare for DataCenter and SwyxON are cloud-based variants of the SwyxWare telephony system and offer customers optimally scalable telephony services. The telephony servers remain with the provider for this purpose and are installed and configured according to the customer's wishes.

The customer installs only the telephony clients, either as on the employees' PCs or as stand-alone IP telephones, e.g. from the SwyxPhone family. These telephony clients then connect via IP to the telephony server managed at the provider. If the customer wishes, his system administrator can also be allowed to maintain his own telephony server. SwyxWare Offers the option of administration at various levels, see *9.3 Administration profiles*, Page 143. Each customer company has its own telephony server. All servers are screened from one another, so that a customer administrator can only configure his own server.

The telephony services are invoiced using a reporting system, which takes into account the functional range permitted for the individual users of SwyxWare. Each user's scope for use is defined by the provider or by the reseller, with the help of so-called features profiles (*9.2 Function profile*, Page 137).

For information on reporting, see *7.5.12 The "Usage Reports" Tab*, Page 102.

1.1 CONCEPT OF SWYXWARE

Several components are required for setting up SwyxWare, with SwyxServer representing the actual central system component.

Although SwyxServer performs an important central function, this does not mean a "central bottleneck". In contrast to conventional telephone systems and IP telephone systems with a central switching unit, SwyxServer is only minimally involved in setting up and controlling the call: SwyxServer essentially takes on elementary functions relating to a connection setup - such as determining the associated IP address for a number to be called - and establishes its availability, while the actual call with SwyxWare then takes place directly between the participating terminal devices. It is therefore easily reconstructed, so that SwyxServer satisfies even medium-sized firms and can initiate and control hundreds of calls in parallel without causing internal "busy" situations.

Due to the fact that not only connection control data but also voice, fax, or video data are transported as IP packets, SwyxWare retains complete control at all times over all existing connections. This allows SwyxWare to easily create, play, or record voice information, for example, during connection control and depending on the current data structures. In this way it can function as an automatic announcement system, as an answering machine, as voice messages, or play any music on hold with no additional hardware required.

On the subscriber side, SwyxServer recognizes "Users", who can use a telephone client with suitable handsets and headsets, or various IP desk telephones.

For SwyxWare a backup server is also available with the option pack, SwyxStandby which automatically takes over the tasks of the primary master SwyxServer if this fails.

Also of great importance for a SwyxWare installation is the link to the existing mail system. SwyxServer saves all voice messages and all fax messages as email attachments on the firm's email server, often but not necessarily a Microsoft Exchange server.

1.2 SOFTWARE COMPONENTS

SwyxServer

SwyxServer manages, controls and monitors all functions and services of the SwyxWare company telephony. Its configuration level in relation to the maximum number of subscribers and the optimal functions determines the capability of the overall system.

SwyxWare Administration

The SwyxWare Administration is handled with a supplementary module (snap-in) to the Microsoft Management Console (MMC) and enables easy setup and management of SwyxServer and all further SwyxWare components.

Number Mapping and locations

The concept of Number Mapping and the property "Location", both of users and of trunk groups, enable extensive flexible arrangement of the internal number scheme.

See *10 Numbers and Number Mappings*, Page 146.

Profiles

With the call permissions, you can define the options for users to make calls. Forwarding of calls via trunk groups can likewise be restricted with the help of the call permissions

Feature profiles define the usage of further SwyxWare functions. Administration profiles define different levels of administration options.

See *9 Profiles*, Page 128.

Trunk and Trunk Groups

"Trunk" denotes a connection to another network, e.g. the public telephone network. A connection to another network can be e.g. an "ISDN trunk", a connection to the Internet an "SIP trunk". Connections or trunks of the same type are combined to form groups. The trunks of a trunk group then have the same properties (such as the same connection protocol or the same rights parameters). The trunks of a trunk group are thus primarily "capacity expansions" from the user's point of view, with no further differences for their use. A trunk must always be a member of a trunk group.

Routing Table

Different trunk groups can be differently prioritized. The result is e.g. that calls are handled with preference given to a server-server connection. If this is not available, a lower-priority path is chosen, e.g. an ISDN trunk.

SwyxIt!

SwyxIt! is the high-performance telephone for your Windows PC. Due to its freely configurable user interface, SwyxIt! can easily be customized to meet your personal needs. The call takes place with a handset (usually with a USB cable attached to the PC) or a headset.

With SwyxIt! in CTI mode (CTI SwyxIt!), you can control phones from your computer. There are various functions available to users with SwyxCTI and SwyxCTI+. See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/#context/help/phone_control_CTI_$.

Call Routing Manager

Furthermore SwyxWare offers with the Call Routing Manager an appointment based call management to deliver incoming calls according to different criteria to a subscriber or a group of subscribers in different ways.

Software services

The SwyxWare installation further consists of a range of services, which are installed as separate processes together with the SwyxServer or on a separate server system, if this is desirable or advisable on capacity grounds. Such services are e.g.

- SwyxGate
  for the interface of the IP network to the public telephone network
- SwyxPhoneManager
  for controlling the SwyxPhone system telephone family
- SwyxConferenceManager
  for supplying telephone conferencing services
- SwyxLinkManager
  for operating coupled SwyxServers over a WAN connection and for linking SIP/ENUM connections

1.3 HARDWARE COMPONENTS

As well as the SwyxWare software components, SwyxWare also includes a range of (optional) hardware solutions.

In addition to Swyx's hardware products, you can also use SwyxWare to operate third-party devices, provided that these products comply with international standards. This applies especially to the wide range of SIP telephones and other SIP devices. Please note, though, that compliant devices almost always offer a functional scope inferior to comparable Enreach devices. Because of the broad variety of available devices Enreach cannot ensure the interoperability.

For information about devices from third party manufacturers, see the Enreach web pages

enreach.com/products/third-party-provider-products.html

SwyxPhone Family

SwyxPhone is a family of IP Desk Phones, which brings the full capability of a company telephone system via Ethernet to your workstation - independently or together with your PC.

SwyxPhone L6x

The SwyxPhone model series consists of several different models. All have a telephone display with two, four or more lines, and have other differing features. These relate to the number of function keys and speed dials, the handsfree facility, LAN switch integration and much more.

They all offer comfortable telephony via "Computer Telephony Integration (CTI)", in collaboration with software clients.

SwyxPhone D8xx

Both these telephones belong to the SwyxDECT 800 and allow cordless access directly to the SwyxWare installation. The users concerned can then be reached anywhere. The direct link to SwyxServers means that the phone functions such as Hold, Call Swap, and also voice messages are available to the users.

SwyxPhone D5xx

These phones are a part of the SwyxDECT 500 system.

They support HD audio. Maximum 40 base stations can be added in a network.

SwyxPhone D7xx

These phones belong to SwyxDECT 700.

See *App. K: Devices*, Page 453.

1.4 GDPR

For further information on EU GDPR (General Data Protection Regulation) and Enreach, please refer to the Enreach website.

2 ONLINE LICENSING

Enreach offers various licensing models that can be tailored to the needs of your business.

There are following technical ways to licence your software:

- *Licensing via license key*Licensing via license key where the purchased license key is checked once during the installation and
- Online Licensing, which requires a permanent Internet connection to the Swyx license server to check the validity of the license.

> The Online Licensing is not available for SwyxON and SwyxWare for Data-Center.

The Online Licensing is supported for new installations from SwyxWare Version 11.50

Ordering

Licenses are ordered via Swyx operator web portal by your service provider. The number of function profiles or additional functions ordered by you is licensed, see *2.2 Feature Profiles*, Page 21 and *2.3 Additional functions*, Page 24

Using activation key

You must enter the license key, which you received from your provider, in the configuration wizard during the SwyxWare installation. see *5.4.2 Configuring SwyxWare*, Page 54, step (8).

license server

The validity of the licenses is constantly checked by the Enreach license server. If, for example, the connection between SwyxServer and the Enreach license server is interrupted due to network problems, the technical supervisors are automatically informed. Since the licenses are stored locally on SwyxServer, SwyxWare can be operated for a few days without synchronization with the central Swyx license server.

2.1 SUBSCRIBE OR PURCHASE

Online Licensing allows you to chose between the following Variants:

- Swyx Purchasing
- Swyx Flex

Swyx Purchasing

You can purchase features for permanent use.

You can extend the ordered functions at any time, e.g. upgrade the basic function profile to professional.

> To obtain software updates outside the warranty, you must also close an update agreement with your service provider.
> The update agreement can also be closed subsequently. In this case, however, the full period of use from the delivery date will be invoiced.

Swyx Flex

You can subscribe to the required functions on a monthly basis and use them flexibly. You can order the corresponding license subscriptions via your service provider and adjust the scope at any time.

The included software updates keep SwyxWare up to date during the whole subscription period.

2.2 FEATURE PROFILES

The required SwyxWare functions are summarized in feature profiles.

The following function profiles are offered as standard:

- Basic
- Professional
- Premium

The feature profiles contain the following functions:

Functions	Feature Profiles:		
	Basic	Professional	Premium
Telephone system and UC functionality (incl. desktop clients for Windows and macOS)	✓	✓	✓
Connections: Voice and fax channels	✓	✓	✓
SwyxAdHocConference	✓	✓	✓
SwyxBCR (Basic Call Routing)	✓	✓	✓
SwyxECR (Extended call routing)	✓	✓	✓
Swyx Meeting 2	✓	✓	✓
Swyx Mobile		✓	✓
SwyxConference		✓	✓
SwyxRecord		✓	✓
SwyxFax		✓	✓
Voice Message Transcription		✓	✓
Federated Authentication		✓	✓
SwyxCTI+			✓
SwyxMonitor			✓
Swyx VisualContacts			✓

Functions in Detail: Performance features

Function	Explanation
SwyxAdHocConference	Dial-in conferences with 3 internal and/or external participants
SwyxBCR (Basic Call Routing)	Use of the Call Routing Manager. This is an additional component of SwyxIt! Classic, which allows the user to define simple call forwarding.
SwyxECR (Extended call routing)	This function contains the full usage of use of the Graphical Script Editor.. This is an additional component of the SwyxIt! Classic software, which offers the user a comfortable interface especially to clearly define and illustrate complex rules for call handling. Certain functions are supplied only by the Graphical Script Editor, such as the access to email directories, the creation of queues or the addition of your own scripts. It is a significant extension of the Call Routing Manager.
Swyx Meeting (Basic version)	WebRTC-based web conference service. Maximum 2 participants: 1 host + 1 guest
Swyx Mobile	Integration of mobile phones with "One Number" concept and telephony via data connections with apps for Android and iOS
SwyxConference	Dial-in conferences with any number of internal and external participants.
SwyxRecord	The recording function makes it possible to record, save and forward telephone calls with the Windows client. For users with other terminal devices, e.g. SwyxPhone, SIP phones or GSM phones (or with SwyxIt! Classic in CTI mode), the conversations can be recorded directly on the trunk connection.
SwyxFax	Use central, server-based fax services with the Windows client. Sending fax messages from any application with a print function.
SwyxCTI+	Makes any phone (e.g. DECT, SIP or analog) an extension for incoming and outgoing calls with the Windows client.
SwyxMonitor	Permanent call recording of incoming or outgoing external calls, silent connection to calls (Silent Call Intrusion).

Function	Explanation
Swyx VisualContacts	Integration of contact information stored in the various applications in the company (e.g. merchandise management, CRM or other databases). Fast phone number identification and contact search directly in the Windows client.
Voice Message Transcription (SwyxON, Swyx Flex only)	Automatic conversion of incoming voice messages into text for users. This technology uses speech recognition to analyze the content of the message and convert it into text.

You must consider the following information when ordering feature profiles:

Licenses for Clients

The number of telephony clients who can log in to SwyxServer is limited to four per user. This means that a user can e.g. log on simultaneously with a desktop client, a SwyxPhone at the workstation, a further SwyxPhone in the conference room and via the Swyx Mobile app.

SwyxConference

For using conferences you may have to appropriately extend the number of calls to a location, see *Conference and limitation of the calls to a location*, Page 124

Swyx VisualContacts

The technical prerequisite for this function is the installation of the ESTOS or C4B application. The corresponding server licenses are not part of the Swyxlicensing and must be purchased separately.

Group Voice Message Transcription

Automatic conversion of incoming voice messages for groups into text.

The number of "Group Voice Message Transcription" licenses determines how many groups this function can be activated for.

Voice and fax channels

The number of voice and fax channel licenses defines how many telephone calls or fax transmissions can be carried out in parallel on SwyxServer. Voice and fax channels are generally free of charge, but their maximum number is limited by the following rule:

- The number of voice channels must not exceed the number of ordered function profiles multiplied by two.

  Example:

  If you have ordered 50 function profiles, up to 100 voice channels can be used.

- The number of fax channels may not exceed the total number of ordered Professional and Premium Functional Profiles.

  Example:

  If you have ordered 20 Professional and 10 Premium Function Profiles, you may use up to 30 fax channels.

The number of internal calls, i.e. calls between users of the same SwyxServer, is unlimited.

SwyxMonitor

The SwyxMonitor function includes two options: permanent call recording, and intrusion on a conversation (Silent Call Intrusion).

- Permanent call recording
  On any trunk connection, the calls for selected internal numbers can be permanently recorded. It can be specified whether one or both sides of the conversation are recorded. This option is often used in call center scenarios for training purposes, or for calls in which important transactions are authorized.
- Silent Call Intrusion
  In a call center, the supervisor can useSwyxIt! Classic to intrude on an ongoing conversation and listen in, give directions to the speaking call center agent (e.g. advice on presenting the case) or even actively join in the call.

You are obliged to adhere to any legal requirements when using the Swyx-Monitor option pack.

SwyxMonitor-functions are only available when CTI is deactivated.

2.3 ADDITIONAL FUNCTIONS

In addition to the function profiles, you can order additional functions and assign them individually to the users who require such functions.

The number of voice channels must not exceed the number of ordered function profiles multiplied by two. Some additional functions may only be ordered with Professional or Premium function profiles.

Example:

You have ordered 50 Basic, 30 Professional and 20 Premium function profiles. You can additionally order up to 100 System Phones, only up to 50 VisualGroups (Professional + Premium) and only up to 20 Swyx Connector for DATEV (Premium) additional functions.

You may order the following additional functions depending on the function profiles you have already purchased:

Additional function	Purchased Feature Profiles:		
	Basic	Professional	Premium
System phone license	✓	✓	✓
Feature Pack for Certified SIP phones	✓	✓	✓
IBM Notes	✓	✓	✓
Swyx Meeting	✓	✓	✓
Swyx Analytics by aurenz	✓	✓	✓
Swyx Connector for Microsoft Teams	✓	✓	✓
Swyx VisualGroups Standard		✓	✓
Swyx VisualGroups Enhanced		✓	✓
Swyx Connector for DATEV			✓

You can assign an additional function to any user. This means that a user with the Basic function profile, may be assigned additional functions that require the corresponding number of purchased Professional or Premium function profiles.

Additional functions: Performance features

Function	Explanation
System Phone	Additional functions for system telephones (Unify), e.g. server-based call lists, telephone directories and extended CTI functions with the Windows client
Feature Pack for Certified SIP phones	Advanced SwyxWare features, such as CTI, global phonebook integration and various system phone features, with certified third-party SIP phones. The scope of functions depends on the provider and telephone model.
Swyx Connector for Notes	Integration with Lotus/IBM/HCL Notes, calendar-based call forwarding, dialling from any contact database, number identification
Swyx Meeting	WebRTC-based web conference service Maximum 25 participants: 1 host + 24 guests
Swyx Analytics by aurenz Swyx Analytics for Microsoft Teams by aurenz	Extension for the analysis of corporate communication on the basis of the generated call data

Function	Explanation
Swyx VisualGroups Standard	VisualGroups provides departments with a high call volume with an optimal queuing solution with seamless integration into the SwyxIt! Classic user interface.
Swyx VisualGroups Enhanced	Additionally, VisualGroups Enhanced offers a statistics function.
Swyx Connector for DATEV	Integration of Enreach telephony functions in DATEV applications
Swyx Connector for Microsoft Teams	Integration of client telephony functions in Microsoft Teams

You must consider the following information when ordering additional functions:

Licenses for desk phones

With SwyxWare you can use both, the telephony client and desk phones.

A separate license is required for each desk phone that is to be operated using SwyxWare. When telephones, e.g. SwyxPhones, are purchased within a SwyxWare installation, this individual license is included, i.e. SwyxServer will either recognize the SwyxPhone automatically (Whitelist), see *7.5.5 The "Licenses" Tab*, Page 91, or an individual license for the system phone is included in the package, see *Install and update Whitelist*, Page 331.

Desk Phone	License type
SwyxPhone	Whitelist
System Phone (Phones by Unify)	System phone license (already included)
Certified SIP phones	Feature Pack for Certified SIP phones

If a desk phone cannot log on due to a missing license and no licenses have been provided, please contact the supplier of this desk phone.

A desk phone license does not include a user license, it only serves to authorize the system phone to SwyxServer.

If a user is simultaneously logged in to SwyxServer with a SwyxIt! Classic and a desk phone, he will only need one user license but he will also need a license for the desk phone if it is not a SwyxPhone.

Swyx VisualGroups

The number of queues used in a customer instance is not limited. A user can be assigned to an unlimited number of queues with a user license. In the SwyxWare variant for the installation in the customer network, the user license is floating based, i.e. only as many user licenses are needed as users are logged into VisualGroups queues.

Statistics, reporting and wallboards are only included in the Enhanced version.

Function	Swyx VisualGroups	Swyx VisualGroups Enhanced
Queue	included	included
Statistics		included
Reporting		included
Administration missed calls		included
Wallboard		included

Swyx Connector for DATEV

The technical prerequisite for this function is the installation of the ESTOS or C4B application. The corresponding server licenses are not part of the SwyxFlex model and must be purchased separately.

Swyx Analytics by aurenz

Extension for the analysis of corporate communication on the basis of the generated call data

This option package must be ordered for the total number of users of your system.

Swyx Analytics by aurenz

Extension for the analysis of corporate communication on the basis of the generated call data

This function must be ordered for the total number of users of your system.

DialoX

Information on the licensing of DialoX applications can be found in the documentation for the respective application or in the license agreement.

2.4 EVALUATION INSTALLATION

This evaluation installation is limited to a period of 30 days. Up to five users can thus use SwyxWare at the same time.

The following licenses are included:

License	No. of
Feature Profile "Premium"	5
System Phone	5
Feature Pack for Certified SIP phones	5
IBM Notes	5
Swyx Connector for Microsoft Teams	5
Swyx Connector for DATEV	5
Swyx Analytics by aurenz	5
SwyxConference	2
Fax channels	2
Voice channels	10
Swyx VisualGroups Enhanced	5
Swyx Meeting (basic version)	5

2.5 BILLING

With the Swyx purchase model, the invoice is issued once on the delivery date. An update agreement is invoiced monthly.

The billing for Swyx Flex is carried out monthly according to the usage report.

You can assign the licensed function profiles to the required users. Only one function profile can be assigned to each user. Additionally, it is possible to assign each user an additional function or several different additional functions to each user. The number of ordered function profiles and additional functions will be invoiced.

Example:

You have ordered 20 Premium, 30 Professional and 50 Basic function profiles. The ordered profiles may be assigned to a total of 100 users. 100 function profiles are recorded accordingly in the usage report.

With online licensing, the ordered number of function profiles is always taken into account. If you assign the function profile "Deactivated" to a user, you only release the ordered capacity for another user, it will not influence the accounting.

You can configure additional users in advance, even if the number of function profiles ordered is exceeded. Assign the function profile "Deactivated" to the new users and order later if required.
See *11.4 Activate/deactivate or delete users*, Page 207 and *9.2 Function profile*, Page 137.

3 LICENSING VIA LICENSE KEY

Swyx offers various licensing models that can be tailored to the needs of your business.

There are following technical ways to licence your software:

- *Online Licensing*, which requires a permanent Internet connection to the Swyx license server.
- Licensing via license key where the purchased license key is checked once during the installation.

3.1 LICENSING PROCEDURE

During the first installation, you will be asked for the license keys. These license keys are limited to 30 days. The temporary license key is sent to you as a PDF. Within these 30 days it is possible to receive an unlimited (permanent) key for your SwyxWare installation by completing registration.

Permanent license keys can be requested using the SwyxWare Administration. In addition to customer data, the hardware information of the computer on which SwyxWare is installed is recorded in the form of checksums. The use of checksums ensures that Swyx does not acquire knowledge concerning your actual hardware information. This data is then sent to Swyx. Based on this data, Swyx derives an unlimited key for your SwyxWare installation which is then sent to you. The installation of SwyxWare onto another system (e.g. due to a failure of the previously used system) requires that you repeat the registration procedure.

> The file which is created when requesting a permanent license key, contains encrypted information concerning the hardware of the computer on which the product is installed. Please note that you must create the license key request on the system you want to use later.

When purchasing additional licenses, it is possible to simply add other license keys in order to expand an existing license. See *3.2.3 User license*, page 31.

Swyx will only use the recorded data for licensing purposes.

Please see the license conditions included in the package for further information.

Evaluation Installation

An evaluation installation is limited to 30 days. Up to five users can thus use SwyxWare at the same time. After purchasing SwyxWare you can enter a valid license key within this 30 day period using SwyxWare Administration and after that request a permanent license key via SwyxWare Administration.

Update Licenses (kb2876)

If you want to update an older version, you need update licenses. Together with existing licensing, an update license allows a newer software version to be installed.

> Before a new version is installed, you must have the necessary update license with the appropriate number of users. SwyxWare will not be available again until after input of the update license.

> If you want to update an older version, please contact your Swyx partner or Support.

Number of update licenses

You need update licenses for each of your SwyxWare users.

Example:

If you operate SwyxWare with 100 users, you will need an update license for 100 users.

Receipt of Update Licenses

An update license cannot be directly or separately purchased. You can purchase the Swyx Update Service (SUS) for a specific validity period. During this validity period you will receive the necessary update licenses directly from Swyx.

See also *3.1.1 Swyx Update Service (SUS)*, page 29.

> Please note that Swyx will not automatically send you the required update licenses based on an existing Swyx Update Service (SUS) license. Please request these by e-mail (license@Swyx.com)..

3.1.1 SWYX UPDATE SERVICE (SUS)

You need a Swyx Update Service license with the same scope for which you have licensed users. A Swyx Update Service license has a validity period of up to 3 years. During this validity period you will receive all necessary update licenses from Swyx with the scope of the existing Swyx Update Service licenses.

Example:

You have a SwyxWare version with 100 users. Therefore, you need 100 update licenses in order to upgrade to a later SwyxWare version. You buy a Swyx Update Service license for 100 users for a period of 3 years, and receive the required SwyxWare update licenses right away. The same naturally also applies for all other required update licenses within the coming 3 years.

The validity period of a Swyx Update Service license begins with the first permanent server key for your SwyxWare. This can be extended by the additional purchase of new Swyx Update Service Licenses.

To update from older versions you need an update key.

If you would like to upgrade an older version, you need an update license that has been specifically created for the desired new version. You cannot use it to update to any newer version of your choice.

> The number of users or voice channels will not be changed during the update.

For further information, please contact your specialist dealer.

3 LICENSING VIA LICENSE KEY

Swyx offers various licensing models that can be tailored to the needs of your business.

There are following technical ways to licence your software:

- *Online Licensing*, which requires a permanent Internet connection to the Swyx license server.
- Licensing via license key where the purchased license key is checked once during the installation.

3.2 LICENSING PROCEDURE

During the first installation, you will be asked for the license keys. These license keys are limited to 30 days. The temporary license key is sent to you as a PDF. Within these 30 days it is possible to receive an unlimited (permanent) key for your SwyxWare installation by completing registration.

Permanent license keys can be requested using the SwyxWare Administration. In addition to customer data, the hardware information of the computer on which SwyxWare is installed is recorded in the form of checksums. The use of checksums ensures that Swyx does not acquire knowledge concerning your actual hardware information. This data is then sent to Swyx. Based on this data, Swyx derives an unlimited key for your SwyxWare installation which is then sent to you. The installation of SwyxWare onto another system (e.g. due to a failure of the previously used system) requires that you repeat the registration procedure.

⚠ The file which is created when requesting a permanent license key, contains encrypted information concerning the hardware of the computer on which the product is installed. Please note that you must create the license key request on the system you want to use later.

When purchasing additional licenses, it is possible to simply add other license keys in order to expand an existing license. See *3.2.3 User license*, page 31.

Swyx will only use the recorded data for licensing purposes.

Please see the license conditions included in the package for further information.

Evaluation Installation

An evaluation installation is limited to 30 days. Up to five users can thus use SwyxWare at the same time. After purchasing SwyxWare you can enter a valid license key within this 30 day period using SwyxWare Administration and after that request a permanent license key via SwyxWare Administration.

Update Licenses (kb2876)

If you want to update an older version, you need update licenses. Together with existing licensing, an update license allows a newer software version to be installed.

ℹ Before a new version is installed, you must have the necessary update license with the appropriate number of users. SwyxWare will not be available again until after input of the update license.

ℹ If you want to update an older version, please contact your Swyx partner or Support.

Number of update licenses

You need update licenses for each of your SwyxWare users.

Example:

If you operate SwyxWare with 100 users, you will need an update license for 100 users.

Receipt of Update Licenses

An update license cannot be directly or separately purchased. You can purchase the Swyx Update Service (SUS) for a specific validity period. During this validity period you will receive the necessary update licenses directly from Swyx.

See also *3.1.1 Swyx Update Service (SUS)*, page 29.

⚠ Please note that Swyx will not automatically send you the required update licenses based on an existing Swyx Update Service (SUS) license. Please request these by e-mail (license@Swyx.com).

3.2.1 SWYX UPDATE SERVICE (SUS)

You need a Swyx Update Service license with the same scope for which you have licensed users. A Swyx Update Service license has a validity period of up to 3 years. During this validity period you will receive all necessary update licenses from Swyx with the scope of the existing Swyx Update Service licenses.

Example:

You have a SwyxWare version with 100 users. Therefore, you need 100 update licenses in order to upgrade to a later SwyxWare version. You buy a Swyx Update Service license for 100 users for a period of 3 years, and receive the required SwyxWare update licenses right away. The same naturally also applies for all other required update licenses within the coming 3 years.

The validity period of a Swyx Update Service license begins with the first permanent server key for your SwyxWare. This can be extended by the additional purchase of new Swyx Update Service Licenses.

To update from older versions you need an update key.

If you would like to upgrade an older version, you need an update license that has been specifically created for the desired new version. You cannot use it to update to any newer version of your choice.

⚠ The number of users or voice channels will not be changed during the update.

For further information, please contact your specialist dealer.

3.2.2 SWYXWARE FOR DATACENTER LICENSING PROCEDURE

A licensing server is licensed in the same way as SwyxWare is licensed . During installation a temporary license key is entered, which is made permanent in the procedure described. A customer installation is then licensed by a logon to the licensing server. The configured data is recorded daily, and summarized in monthly usage reports. These are sent to the service provider and Swyx. The invoicing can be based on these reports.

The backend server, which is used only for the license management and reporting, requires a special license.

3.2.3 USER LICENSE

According to the type, the license will be granted either per logged-on user (SwyxWare), per configured user (SwyxWare for DataCenter) or per ordered user (SwyxON).

⚠ After the installation of an option pack the entire number of user licenses is reduced to the number of option pack licenses.
Please make sure to acquire a sufficient amount of option pack licenses.

Example:

If you have set up a SwyxWare installation with 100 users, and add a license for an additional option pack with 80 users, only 80 users can simultaneously log on to SwyxServer.

Example:

If there are 100 user licenses and the customer purchases 150 option pack licenses, only 100 user licenses including option pack will be available after adding the keys.

If you find that you have too few users after you have installed an option pack, you can remove the license for the option pack. You will then have the original number of users. Please contact your dealer in order to receive an option pack with a sufficient user quantity.

Does not include an upgrade of the current software version , see *Update Licenses (kb2876)*, page 28.

In SwyxWare for DataCenter and SwyxON , the allocated functions per configured or ordered user are recorded in the usage report, even if this user is logged off or deactivated.

In SwyxWare for DataCenter, you can allocate the deactivated user the function profile "Deaktiviert" ("Deactivated") in order to avoid invoicing the user.

In SwyxON, the ordered number of users for a function profile is always invoiced. If you allocate a user the "Deactivated" profile, you only release the ordered capacity for a different user.

In SwyxON, you can configure further users in advance, even if this means exceeding the number ordered. Assign the "Deactivated" function profile to the new users and order later if necessary.

3.2.4 LICENSES FOR CLIENTS

The number of telephony clients who can log on to SwyxServer is limited to four per user. This means that a User can e.g. log on simultaneously with a desktop client, a SwyxPhone at the workstation, a further SwyxPhone in the conference room and via the Swyx Mobile app.

Licenses for desk phones

With SwyxWare you can use both, the telephony client and Desk Phones.

A separate license is required for each Desk Phone that is to be operated using SwyxWare. When telephones, e.g. SwyxPhones, are purchased within a SwyxWare installation, this individual license is included, i.e. SwyxServer will either recognize the SwyxPhone automatically (Whitelist) or an individual license for the system phone is included in the package.

Desk Phone	License type
SwyxPhone	Whitelist
System Phone (Phones by Unify)	System phone license
Certified SIP phones	Feature Pack for Certified SIP phones

If a Desk Phone cannot log on due to a missing license and no licenses have been provided, please contact the supplier of this Desk Phone.

A Desk Phone license does not include a user license, it only serves to authorize the system phone to SwyxServer.

> If a user is simultaneously logged on to SwyxServer with a SwyxIt! and a Desk Phone, he will only need one user license but he will also need a license for the Desk Phone if it is not a SwyxPhone.

Licenses for Swyx Mobile

The functions of SwyxWare can also be used by mobile devices while traveling. For this

- the administrator must make the Swyx Mobile option available for the User (in the user properties on the **Rights** tab)
- the User himself - or the administrator on his behalf - must activate the use of Swyx Mobile in the Forwardings on the **Mobile Extensions** tab

The Swyx Mobile licenses are individual licenses and are valid for the number of Users who have activated this option in their call forwarding.

> ! The Swyx Mobile license is an additional license for a User who is already configured and licensed.

> The special User MobileExtensionManager, who is created within SwyxWare for Swyx Mobile, does not need a separate user license.

3.2.5 LICENSING OF DATA CHANNELS

Voice Channel Licenses

The number of voice channels is licensed. A voice channel is the connection from the own network, where SwyxServer is installed, to a device connected to another network. A distinction is made according to the type of voice channel:

- Voice channels via ISDN into the public telephone network or over SIPGateway trunks are licensed per configured voice channel
- Voice channels via IP to another location (SwyxLink or SIP trunk) are only charged when an active call exists over this connection

  Example:

  A SwyxWare installation has 8 ISDN channels. A branch is further linked in with a maximum of 4 channels (SwyxLink), and a SIP trunk is set up to a provider with a maximum of 10 channels. Altogether 22 channels are set up.

  In this case at least 9 channels should be licensed.

  If 16 channels are licensed, then 8 channels are recorded via the ISDN trunk, and a further 8 channels are available for simultaneous calls via the SwyxLink trunk and the SIP trunk. If e.g. all 4 SwyxLink connections and 4 SIP trunk connections are active, no further call can be initiated via the SwyxLink or SIP trunk.

The number of internal calls, i.e. calls between users of the same SwyxServer, is unlimited.

Fax Channel Licenses

The number of configured fax channels is licensed. No distinction is made between the fax channel types, e.g. ISDN to the public telephone network or IP to another site (SwyxLink).

3.2.6 OPTIONS AND OPTION PACKS

For certain use scenarios, supplementary modules are offered which significantly expand the functional scope of SwyxWare. These supplementary modules can either be added as option packs (e.g. Extended call routing for all users of a SwyxServer), or as options (single licenses for a certain number of SwyxFax users).

SwyxBCR (Basic Call Routing)

The option "SwyxBCR" for SwyxWare for DataCenter includes the use of the Call Routing Manager.

SwyxECR (Extended call routing)

This option pack contains the full usage of use of the Graphical Script Editor.. This is an additional component of the SwyxIt! software, which offers the user a comfortable interface especially to clearly define and illustrate complex rules for call handling.

Certain functions are supplied only by the the Graphical Script Editor, such as the access to email directories, the creation of queues or the addition of your own scripts. It is a significant extension of the Call Routing Manager.

SwyxConference

The option pack offers professional conference management. You can hold conferences with numerous participants (more than three), and virtual conference rooms can be set up into which the individual subscribers can dial independently of one another, both from the company network and from outside.

Please note that in order to use conferences you must appropriately extend the number of calls to a location.

SwyxAdHocConference

The option "SwyxAdHocConference" for SwyxWare for DataCenter enables the user to initiate conferences spontaneously with more than three users. See also *Scope of functions in SwyxWare for DataCenter and SwyxON*, page 36.

SwyxRecord

If the "SwyxRecord" option pack is installed, then during a call a user can independently record the conversation (or terminate this recording) with a click of the mouse. For users with other devices, e.g. SwyxPhone, SIP phones or GSM phones (or with SwyxIt! in CTI mode), the conversations can be recorded directly on the trunk connection.

SwyxProfessional

The option pack "SwyxProfessional" includes the option packs SwyxRecord, SwyxConference, SwyxECR, Swyx Mobile and SwyxFax available for all SwyxWare Users.

SwyxMonitor

This function is not available for SwyxON.

The SwyxMonitor option pack requires the SwyxRecord option pack.

The "SwyxMonitor" option pack includes two options: permanent call recording, and intrusion on a conversation (Silent Call Intrusion).

- Permanent call recording
  On any trunk connection, the calls for selected internal numbers can be permanently recorded. It can be specified whether one or both sides of the conversation are recorded. This option is often used in call center scenarios for training purposes, or for calls in which important transactions are authorized.
- Silent Call Intrusion
  In a call center, the supervisor can useSwyxIt! to intrude on an ongoing conversation and listen in, give directions to the speaking call center agent (e.g. advice on presenting the case) or even actively join in the call.

You are obliged to adhere to any legal requirements when using the SwyxMonitor option pack.

SwyxMonitor-functions are only available when CTI is deactivated.

Swyx Connector for Swyx Connector for Notes

The Swyx option pack for Swyx Connector for Notes offers the following functions:

- Direct dialing from Swyx Connector for Notes
- Display Swyx Connector for Notes contacts (for incoming call, from lists)
- The search function in the SwyxIt! input field and the phonebook also searches Swyx Connector for Notes contacts
- Name resolution from Swyx Connector for Notes for incoming calls and for list search
- Swyx Connector for Notes on the Speed Dial button

SwyxFax

SwyxFax Server is a component of SwyxServer. With this component you can send and receive fax documents. SwyxFax uses the same connection to the public network as SwyxServer, typically an ISDN trunk. SwyxFax Server can be installed on the same computer as the ISDN card of the ISDN trunk, but also on another permanently running computer, which is connected via an IP network to the ISDN trunk (SwyxWare uses the T.38 protocol for secure transmission).

Licenses for SwyxFax Users

The number of SwyxFax Client installations is unlimited. Licensed is the number of Users who have configured a fax number and configured at least one fax forwarding (to SwyxFax Client, to an e-mail address or a printer).

SwyxCTI+

This option allows you to control a third party phone with CTI SwyxIt! or link with an external phone via its phone number.

The number of Users with this option must be licensed.

Swyx VisualContacts

Swyx VisualContacts is an option which allows a SwyxIt! User to access various contact data bases via the ESTOS MetaDirectory.

All SwyxIt! Users, who want to use the Swyx VisualContacts upgrade, need a Swyx VisualContacts license. SwyxIt! retrieves this license during log on to the SwyxServer, if Swyx VisualContacts is installed.

Swyx Connector for DATEV

Swyx Connector for DATEV is an option that integrates the DATEV telephony function into SwyxIt!.

SwyxIt! Users who use the integration with DATEV need a Swyx Connector for DATEV license. SwyxIt! retrieves this license when registering at SwyxServer, if Swyx Connector for DATEV is installed. Users with a Swyx Connector for DATEV license do not need an additional Swyx VisualContacts license.

Swyx Connector for Microsoft Teams

With this option you can use SwyxIt! Use functions directly on the Microsoft Teams Windows interface.

Feature Pack for Certified SIP phones

Feature Pack for Certified SIP phones is not supported in the standby scenario (SwyxStandby).

This option offers the possibility to use extended SwyxWare functionalities, such as CTI, integration of the global phone book and various system phone functions, with certified third-party SIP phones. The scope of functions depends on the provider and telephone model.

Swyx VisualGroups

When licensing VisualGroups, the customer can choose one of the following options:

- Licensing per user
  The number of queues used in a customer instance is not limited. A user can be assigned to an unlimited number of queues with a user license. In the SwyxWare variant for the installation in the customer network, the user license is floating based, i.e. only as many user licenses are needed as users are logged into VisualGroups queues. In SwyxWare for DataCenter configured users and in SwyxON ordered users are considered.

> If licenses for the Enhanced version are active, standard licenses become invalid.
> For example, 1 Enhanced-licensed user and 6 standard users will result in only one Enhanced license.

Statistics, reporting and wallboards are only included in the Enhanced version.

Function	Swyx VisualGroups	Swyx VisualGroups Enhanced
Queue	included	included
Statistics		included
Reporting		included
Administration missed calls		included
Wallboard		included

- Licensing per number of queues
  The number of queues used in a customer instance is not limited.

The documentation for VisualGroups from version 1.1 can be found on the Swyx website.

Swyx Analytics by aurenz

Extension for analyzing corporate communication based on the call data generated by SwyxIt!

This Option Pack must be ordered for the total number of users of your system.

Swyx Analytics by aurenz for Microsoft Teams

Extension for analyzing corporate communication based on the call data generated by Swyx Connector for Microsoft Teams

This function must be ordered for the total number of users of your system.

Swyx Meeting (basic version)

WebRTC-based web conference service
Maximum 2 participants: 1 host, 1 guest

Swyx Meeting

WebRTC-based web conference service
Maximum 25 participants: 1 host, 24 guests

Scope of functions in SwyxWare for DataCenter and SwyxON

The options offered by the various option packs are reflected in the feature profiles, which are assigned to the individual users. If you use another option, a different feature profile is assigned to the user. This profile contains the relevant feature and makes it available to the user.

Reporting daily records the functions or cloud profiles used and the number of users to whom these functions are assigned, along with the number of installed voice and fax channels and the conference rooms that have been set up. The cumulative data is sent monthly from the licensing server both to Swyx and to the provider.

3.2.7 SWYXWARE OPTION PACKS AT A GLANCE

The following option packs are available:

Option Pack	SwyxWare Variant	Explanation
SwyxProfessional	● SwyxWare	Includes the option packs SwyxRecord, SwyxConference, SwyxECR, Swyx Mobile and SwyxFax
SwyxRecord	● SwyxWare ● SwyxWare for DataCenter ● SwyxON	If the "SwyxRecord" option pack is installed, then during a call a user can independently record the conversation (or terminate this recording) with a click of the mouse (not in CTI mode!). For users with other devices, e.g. SwyxPhone, SIP phones or GSM phones (or with SwyxIt! in CTI mode), the conversations can be recorded directly on the trunk connection.
SwyxConference	SwyxWare	The option pack "SwyxConference" for SwyxWare offers professional conference management.
SwyxAdHocConference	● SwyxWare for DataCenter ● SwyxON	The option pack "SwyxAdHocConference" offers users the opportunity to initiate 'ad hoc' conferences with three or more participants during a call. In SwyxWare, this basic function is included for three participants of a conference.
SwyxBCR	● SwyxWare for DataCenter ● SwyxON	This package contains the full usage of Call Routing Manager. This is an additional component of the SwyxIt! software, which enables complex rule-based call handling for the user. This option pack is already included in SwyxWare.
SwyxECR	● SwyxWare ● SwyxWare for DataCenter ● SwyxON	This package contains the full usage of the Graphical Script Editor. This is an additional component of the SwyxIt! software, which offers the user a comfortable interface especially to clearly define and illustrate complex rules for call handling.
SwyxMonitor	● SwyxWare ● SwyxWare for DataCenter	The "SwyxMonitor" option pack includes two additional options: permanent call recording, and intrusion on a conversation (Silent Call Intrusion).
Swyx Meeting	● SwyxWare ● SwyxWare for DataCenter ● SwyxON	WebRTC-based web conference service
Swyx Analytics by aurenz	● SwyxWare ● SwyxWare for DataCenter ● SwyxON	Extension for the analysis of corporate communication on the basis of the generated call data
SwyxStandby	SwyxWare	The option pack SwyxStandby offers enhanced availability of the SwyxWare PBX through the use of a second redundant SwyxServer installed on a further Windows server, which acts as a standby server.

Cloud Services in SwyxON

System Functions	Description
Basis system	Telephone system functionality and Unified Communications
Fax channel	T.38 support for sending fax messages
Conference Room	Participation in conferences with any number of internal and external participants

User functions	Description
Basic user	Basic functionality for users including desktop clients for Windows and macOS, Call Routing Manager, presence information, messaging, Outlook integration, CTI, Voicemail, adhoc conference feature

User functions	Description
System Phone	Enables comfortable additional functions for system telephones such as server based call lists, telephone books and extended CTI functions for example SwyxIt!
Mobility	Integration with applications for Android and iOS.
Extended call routing basic	Use of company-wide call routing, e. g. as central call pickup and distribution or the creation of speech dialog systems (ACD/IVR)
Extended call routing User	Creation and execution of complex call diversions with the Graphical Script Editor individually for each User
VisualContacts	Integration of contact information which are saved in the company's various applications (e.g. logistics, CRM and further databases). Fast number identification and contact search directly in SwyxIt!
CTI+	Makes a telephone (DECT, SIP or analog telephones) an extension for incoming and outgoing calls with SwyxIt!
Recording	The recording function enables the recording, saving and forwarding of telephone calls with SwyxIt!
Fax	Use of central, server-based fax services with SwyxIt!. Transmission of fax messages from all applications with a print function
Swyx Connector for DATEV	Enables direct phone calls from DATEV applications
Swyx Connector for Notes	Integration in Lotus/IBM/HCL Notes, dialing from any contact databases, number identification
Swyx Connector for Microsoft Teams	Integration in Microsoft Teams user interface
Swyx Meeting	WebRTC-based web conference service
Swyx VisualGroups	With Swyx VisualGroups, departments with a high caller volume receive an optimal queue solution with seamless integration into the SwyxIt! user interface.

3.2.8 LICENSING OF THE SWYXWARE VARIANTS AT A GLANCE

	Evaluation Installation	SwyxWare	SwyxWare for DataCenter/ SwyxON
SwyxServer	1 license	1 license	unlimited
Users	5 licenses	Scope of supply	-
SwyxBCR	included	included	pro User
SwyxECR	5 licenses	Option Pack	per user
SwyxFax	5 licenses	Option	per user
SwyxPhone	2 licenses	Option per phone	pro User
SwyxRecord	5 licenses	Option Pack	per user
SwyxConference	5 licenses	Option Pack	-
SwyxMonitor	5 licenses	Option Pack	-
SwyxStandby	included	Option Pack	-
SwyxAdHocConference	included	included	pro User
Swyx Option Pack for Swyx Connector for Notes	5 licenses	Option Pack	per user
Conference Rooms (requires SwyxConference)	any number	any number	per room set up
Voice channels	4 channels	Scope of supply	per channel
Fax channels	2 fax channels	Scope of supply	per channel
Swyx VisualContacts	5 licenses	Option	pro User

	Evaluation Installation	SwyxWare	SwyxWare for DataCenter/ SwyxON
Swyx Connector for Microsoft Teams	5 licenses	Option	per user
Swyx Connector for DATEV	5 licenses	Option	pro User
Feature Pack for Certified SIP phones	5 licenses	Option	per user
Swyx Visual-Groups Enhanced	1 queue or 5 licenses	Option	-
SwyxVoicemail	included	included	pro User
SwyxCTI	included	included	per user
SwyxCTI+	5 licenses	Option	per user

Explanation:

Option pack-- All users must be licensed

Option-- License per logged-on user

included-- License is included in the basic version

per user-- License per configured user

per channel-- License per configured channel

Scope of supply-- Number is fixed with the order

pro phone-- License per phone which was not purchased from Swyx

4 SYSTEM REQUIREMENTS

Hardware, software, and network requirements, in addition to the license conditions

> Please make certain that the most up-to-date Service Pack from Microsoft is installed when using the Windows system. Install the security updates provided by Microsoft on a regular basis.

> Please note that the following hardware requirements apply only to a SwyxWare installation. If you want to run other processes on this computer, such as a file server application, the hardware requirements are different.

Under certain conditions, SwyxWare may be operated on a virtual machine hardware.

> Special requirements apply to the SwyxON components. For more information, please contact your provider.

You can obtain more information on this subject from your Enreach partner or support.

4.1 HARDWARE REQUIREMENTS

No special hardware equipment is necessary for the operation of a SwyxServer or SwyxGate. The software can be run on all standard PCs, which also support Windows Server. The hardware requirements correspond essentially to those recommended by Microsoft for the use of these operating systems.

Detailed information regarding the computer equipment can be found in the Knowledgebase on the Enreach Homepage.

service.swyx.net/hc/en/articles/4404114457618

> Please note that SwyxWare only works with the ISDN cards of the SX2 family.

> Please note that you may need further memory on SwyxServer, especially for recording conversations, creating own Skins or for defining user rules.

Hard Drive Memory and File System

A complete SwyxWare installation requires approx. 1 GB of hard disk space. Plus storage space for data generated during operation, e.g. announcements, voice messages, etc.

Network card(s)

The system requires a network card, which is connected to the network (LAN, Local Area Network). If there is more than one network card in the system or if several IP addresses are assigned to one network card, you must define which IP address SwyxWare should work with. There is a registry key for this purpose:

```
Location:
HKLM\Software\Swyx\General\CurrentVersion\Options
Type: REG_SZ
Name: LocalIpAddress
Value: <IP address in the local LAN>
```

Restart the computer after setting this registry key.

For current information on this topic, see the knowledge base article.

service.swyx.net/hc

4.2 SOFTWARE REQUIREMENTS

Please make certain that the most up-to-date Service Pack from Microsoft is installed when using the Windows system. Install the security updates provided by Microsoft on a regular basis.

Special requirements apply to the SwyxWare for DataCenter server components.

(A list of supported operating systems can be found in the knowledgebase article:

Supported operating systems (overview)
service.swyx.net/hc/en/articles/4405218845330

You can obtain more information on this subject from your Enreach partner or support.

Microsoft .NET Framework

Microsoft .NET Framework **4.7.2** is a prerequisite for SwyxServer and all other SwyxWare components. It can also be downloaded subsequently via the Windows update feature, or from the SwyxWare DVD.

SQL Database for the user data

SwyxServer needs a Microsoft SQL database for storing the user and configuration data. You can choose from a variety of options:

- Microsoft SQL Server Express 2019, 2022
  Microsoft SQL Express can be downloaded directly from the SwyxWare DVD.
- Microsoft SQL Server Standard Edition 2019, 2022
  For larger installations, e. g. a installation, please use at least Microsoft SQL Server Standard Edition.

The database server must be set up before the installation of SwyxWare.

The existing SQL server is not updated in a SwyxWare update.

Mail server

To send welcome and password reset e-mails and voice messages, you need a SMTP mail server that can be reached from SwyxServer.

SMTP authentication (user name and password) is supported.

Microsoft Exchange Server for Call Management

This function is not available for SwyxON.

With the SwyxWare, Call Routing Manager further offers calendar-based call management. If you want to use this, you need a Microsoft Exchange Server or Exchange Web Services to be accessible. In order to ensure this, we recommend the installation of a Microsoft Outlook Client on the SwyxServer.

See: *5.3.3 Installation for Calendar-Based Call Management*, Page 51.

Lotus/IVM/HCL Domino Server for Call Management

If you have a Lotus/IBM/HCL environment, you can also carry out an integration for calendar based call management.

See: *App. F: IBM Notes integration*, Page 434

Virus Scanner

If you operate a virus scanner on the computer on which SwyxServer is installed, you should exclude the database files from the scan process.

4.3 NETWORK REQUIREMENTS

The IP network, in its function as a transport medium, has a significant influence on the voice quality of the telephone connections. Therefore, special attention must be paid to the configuration of the network.

All common network topologies are supported (Ethernet 1000BaseT etc.). TCP/IPv4 must be available as a transfer protocol. Other network protocols such as IPv6, IPX or ATM are NOT supported by SwyxWare.

Various QoS (Quality of Service) mechanisms are supported in order to guarantee interference-free transmission of voice data in the network. These include:

- On TCP/IP protocol level, DiffServ (RFC 2474) is supported.
- Prioritization of the voice data using IEEE802.1p
  In order to take advantage of this feature, it is necessary to use network cards which support this standard.

Bandwidth Requirement

In idle mode, packets are exchanged between the clients and the SwyxServer, e.g. to update the status signaling.Create a suitable network environment for SwyxServer

In order for the SwyxWare telephone system to operate smoothly, the existing network infrastructure is a deciding factor in addition to the basic software and hardware requirements described above. The following provides a description of an environment that offers optimal conditions for the functioning of SwyxServer.

It is assumed that we are dealing with a network which is based on a Windows Active Directory.

General

To create optimal conditions for SwyxServer, the following should be set up:

- The computer on which the SwyxWare is installed will be configured exclusively as the telephony server. Other network services, such as email server, DHCP or DNS server, should not be provided on this computer.
- SwyxServer contains a permanent IP address.

Infrastructure of the Network

SwyxWare uses the Internet Protocol (IP) to transfer voice and control data. Each client and SwyxServer computer requires a unique IP address in the network.

A complete layer2 switched network guarantees an optimal transmission of the voice and control data, even in case of a large number of SwyxWare telephone calls or in a network with increased data traffic (e.g. file transfer, HTTP, FTP), however, this is not obligatory.

The SwyxServer computer or the SwyxGate which has been installed on a separate computer must be connected to a switch. This will ensure that there is sufficient bandwidth available for the data traffic between the telephony clients (SwyxIt! Classic or SwyxPhone) and SwyxServer.

Quality of Service

In order to improve the voice quality, the use of Quality of Service in the network is advantageous.

For further information see

Support of QoS (Quality of Service)
service.swyx.net/hc/en-gb/articles/360000007840-Support-QoS-Quality-of-Service- (You may need to be logged in to view the content)

Firewall

Detailed and actual information about the ports used by SwyxWare see

INFO: Which Ports are used by SwyxWare v11
https://service.swyx.net/hc/en-gb/articles/360000566005-Which-Ports-are-used-by-SwyxWare-v11 (You may need to be logged in to view the content)

DHCP (Dynamic Host Configuration Protocol)

The use of a DHCP server for the distribution of the IP addresses to the telephony clients offers the following advantages:

- Unique assignment of IP addresses in the network

- Automatic transmission of the SwyxServer IP address to the clients

To find out how to install a DHCP server and how to configure it for the use of telephony clients see *20.1.1 DHCP-Server (Dynamic Host Configuration Protocol)*, Page 332.

DNS (Domain Name Service)

An Active Directory requires a DNS Server located in the network. The Active Directory uses DNS as a locator service, which helps to assign the names of the client's FQDN (Fully Qualified Domain Name), domains, locations and services in the Active Directory of an IP address.

If the WINS resolution for DNS is activated on the DNS server, the WINS server will be queried if the name of the client cannot be resolved by the DNS server.

See *20.1.3 DNS (Domain Name Service)*, Page 333.

Reserve ports for SwyxWare

Enreach recommends not using SwyxWare on systems which are simultaneously DomainController or DNS Server. If you do run SwyxWare on a Windows DNS Server, Microsoft Security Fixes (patches KB951748 and KB951746) can cause the Microsoft DNS Server to occupy all IP ports so that SwyxWare is unable to allocate any more. To avoid such conflicts, a static range of ports can be reserved, excluding these for random port requests from applications/services.

For further information, please contact you specialist dealer.

Portforwarding for SwyxRemoteConnector

If SwyxRemoteConnector is used, the company router (NAT gateway) has to be configured accordingly.

See *Port forwarding via router*, Page 386.

WINS (Windows Internet Name Service)

The service WINS resolves NetBios names into IP addresses and is therefore an elementary component of a Windows network. Given this fact, this service should already be installed on the Windows Server located in the network.

See *20.1.2 WINS (Windows Internet Name Service)*, Page 333.

If the above mentioned components are correctly configured, SwyxWare will be provided with an optimal environment.

4.3.1 OPERATING SYSTEM

The purchase of SwyxWare does not include the operating system software necessary for installation and operation. As SwyxWare is based on Microsoft Windows operating systems, you must be in possession of such licenses for the computers on which you wish to install SwyxWare components. Appropriate licenses are needed in order to use a telephony Client.

In addition to the operating system licenses, so-called "Client Access Licenses" (CALs) from Microsoft for Windows server systems may be required.

For further information on the current licensing conditions for Microsoft WindowsServers, and access to services provided by such a server, please see the license agreements for these products and the Microsoft publications.

4.4 EXAMPLE SCENARIOS

In considering the operation scenarios for SwyxWare, you can distinguish in principle between two groups - stand-alone installations and migration scenarios.

4.4.1 STAND-ALONE INSTALLATION

In this case, SwyxWare provides the complete telephony functionality, i.e. a conventional telecommunication system is no longer necessary. The user is provided with either a desktop client or a SwyxPhone.

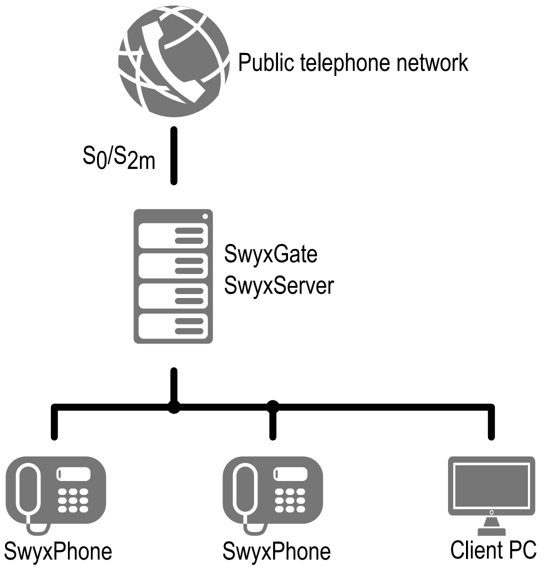


Fig. 4-1: SwyxGate connected to PSTN

The minimum amount of equipment corresponding to a traditional telecommunication system consists of SwyxServer as the central element, one or more s or SwyxPhones and SwyxGate as an interface to the PSTN.

Stand-alone installation with SIP extension

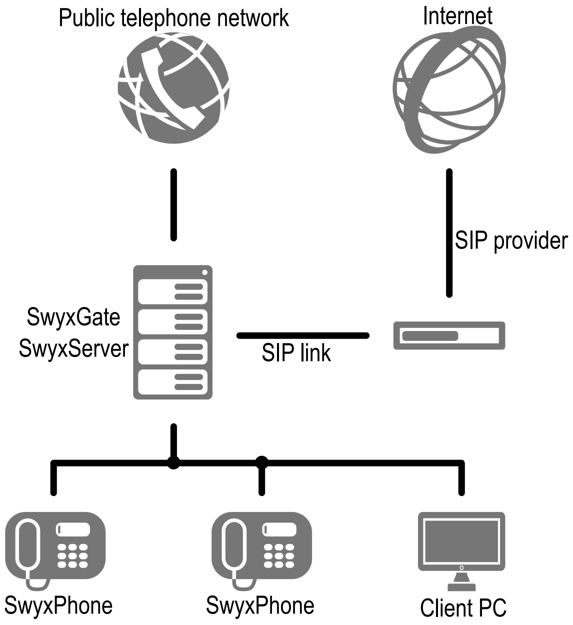


Fig. 4-2: SwyxServer connected via SwyxGate to PSTN and SIP link to the Internet

The simple installation is expanded here with a link-up to the Internet, e.g. via an SIP provider. In this case an SIP link can be used for telephoning an external SIP client. See *16 SIP Links*, Page 278.

4.4.2 MIGRATION SCENARIOS

Here we have an existing telecommunication system which is used together with SwyxWare.

The aim is to assign telephone numbers of the same length from within a possible range of numbers to all internal subscribers, regardless of whether they are connected to a traditional private branch exchange (PBX) or they use SwyxWare to place telephone calls. Moreover, all users should be able to dial an external line using the same procedure (e.g. "0" for public line access, followed by the destination number in the public network). For more details on the configuration of the Swyx-

Gate settings mentioned below and on the configuration of its lines, please read *The "ISDN Ports" Tab*, Page 274.

Example 1:SwyxWare as sub-telecommunication system

SwyxGate is connected to the traditional private branch exchange (PBX) using one line. Calls to A and B will be put through directly by the PBX. Calls from the public telephone network to C, D and E are forwarded to SwyxServer by the PBX and delivered from there. Calls from the SwyxWare users C, D and E into the public network are first forwarded to the PBX. The PBX then forwards these calls to the public network. Internal calls between A or B and C, D or E stay within the company.

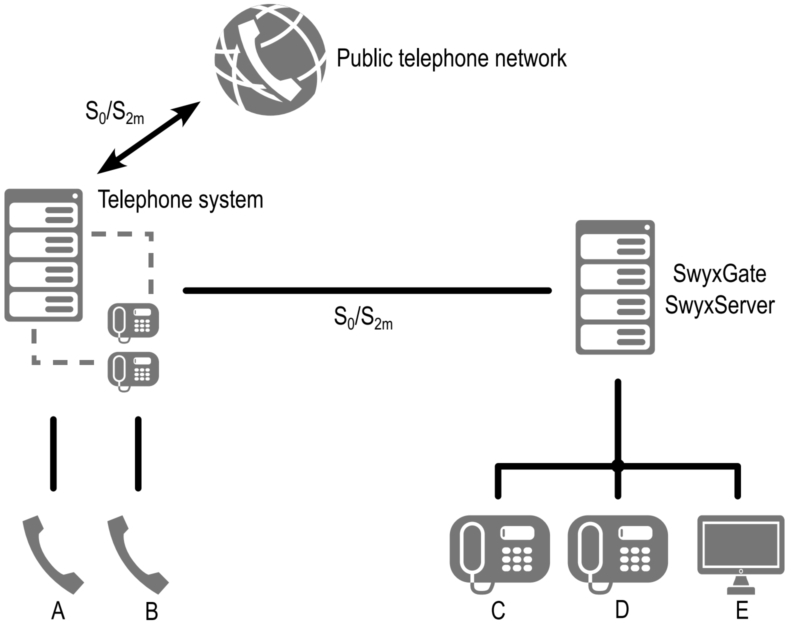


Fig. 4-3: SwyxGate connected to PBX

Example 2:SwyxWare in addition to a telecommunications system

SwyxGate is connected via one line to the traditional private branch exchange (PBX) and to the public network with a second line.

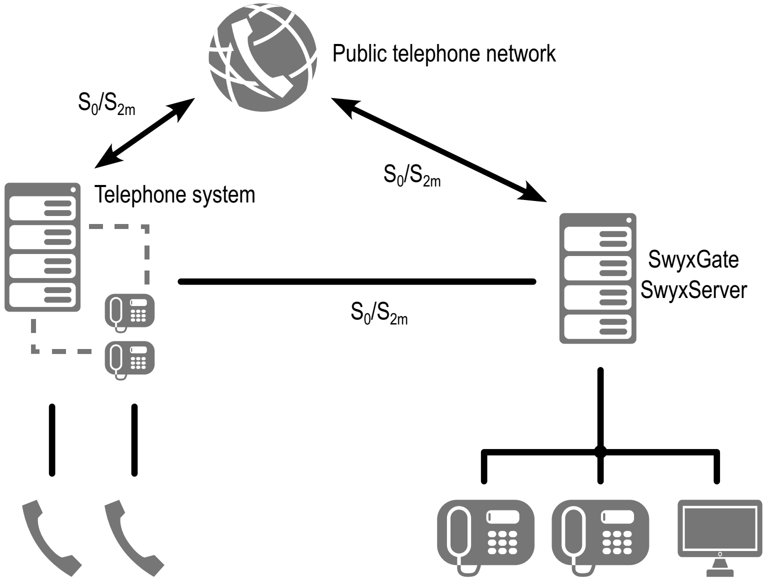


Fig. 4-4: SwyxGate to PBX and PSTN

This scenario is useful when you are migrating an old PBX over to SwyxWare in order to improve the availability of external lines for SwyxWare users without having to add more modules to the existing PBX.

Example 3: SwyxWare with a sub-telecommunication system

A SwyxGate is installed between the public network (PSTN) and the private branch exchange (PBX):

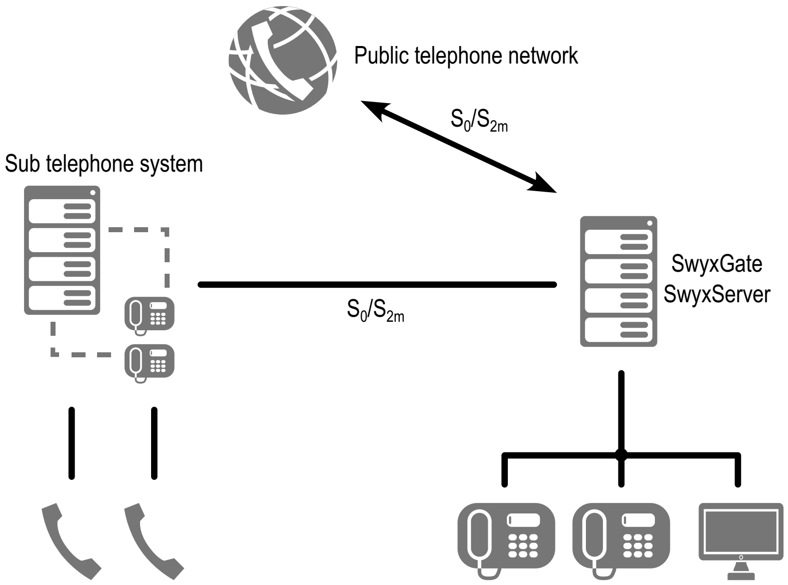


Fig. 4-5: SwyxGate connected between PBX and PSTN

Detailed information concerning the configuration of SwyxServer can be found in ***App. D: Internal connections (BRI/PRI)***, Page 417. For information on the configuration of ISDN cards for an internal S0 connection, please refer to ***D.1.2 SX2 in NT Mode***, Page 418.

5 SWYXWARE INSTALLATION

Installation or update of SwyxWare

The standard installation procedure for SwyxWare is described in this chapter.

In SwyxON, SwyxWare is provided by the service provider and requires no installation and initial configuration by the customer.

If you are updating a currently installed SwyxWare version, please continue reading in ***5.6 SwyxWare Update***, Page 65.

Summary of the SwyxServer Installation

Which services belong to SwyxServer

Preparation for Installation

Installation of SwyxServer

Installation of the SwyxWare Administration

SwyxWare Update

Separated Services

5.1 SUMMARY OF THE SWYXSERVER INSTALLATION

The following actions must be carried out in order to successfully install SwyxWare in your company. You will find references to the detailed step-by-step instructions for every step.

Preparation		
1	Hardware	Make certain that the necessary hardware conditions have been fulfilled See *4.1 Hardware Requirements*, Page 40.
2	Software	Check whether you have the necessary software, e.g. Windows Server, Firewall or virus scanners. See *4.2 Software requirements*, Page 41.
3	Network	Check your network in order to guarantee interference-free transmission. See *4.3 Network requirements*, Page 42.
4	Installation of the ISDN Cards	For access to the public ISDN (SwyxGate), install the necessary ISDN cards. See *15.2 Installation of the ISDN Cards*, Page 246. You will find the necessary test programs in *App. E: Tools & Traces*, Page 424.
5	Voice Box	For the Voice Box functionality, you need an optional SMTP-capable mail server. SwyxServer Sends the voice messages via this to the users. When installing SwyxWare you will need the name of the mail server, e.g. mail.company.com. See *Mail server*, Page 41.

After the installation of SwyxServer (step 7) the configuration wizard starts automatically.
Go through all the steps of the Configuration Wizard.

Software Installation		
6	Database	Install the database for user administration, along with the necessary software .Net Framework. See *5.3.4 Install Microsoft SQL Database*, Page 52.

Software Installation		
7	Installation of Swyx-Server	You must license SwyxWare. For licensing with a license key, have the license certificate ready that you received as a PDF file. See *3 Licensing via license key*, Page 30. For information on Online Licensing, see *2 Online Licensing*, Page 21.
8	Installation of the Swyx-Ware Administration	Then install SwyxWare Administration to configure SwyxServer. See *5.5 Installation of the SwyxWare Administration*, Page 64. You can also install the SwyxWare Administration on another computer, see *5.7.1 Installation of a SwyxWare component on an additional computer*, Page 67.
9	Installation of Swyx Control Center	Then install Swyx Control Center to configure SwyxServer. See *5.4.3 Install Swyx Control Center*, Page 59
10	Installation of Swyx Visual Groups	Then install Swyx Visual Groups. The current documentation for SwyxVisualGroups can be found at: help.enreach.com/docs/manuals/english/VisualGroups.pdf

Configuration		
11	Licensing	You must license SwyxWare. For licensing with a license key, have the license certificate ready that you received as a PDF file. See *3 Licensing via license key*, Page 30. For online licensing, make sure that an SwyxWare instance has been created in the operator. For information on Online Licensing, see *2 Online Licensing*, Page 21.
12	Number plan	Plan the topology of SwyxWare before installation, and design a number plan (e.g. for company headquarters and branches). See *10 Numbers and Number Mappings*, Page 146.
13	Configuration of Swyx-Server	For details of how to change SwyxServer settings after installation, please refer to *7 Configuration of SwyxServer*, Page 80.

Configuration		
14	Create users and groups	For details of how to set up new users and groups after installation, please refer to *7.5 Configuring SwyxServer settings*, Page 86.
15	Scripts	When carrying out the first configuration, adapt the scripts to the conditions in the company. See *22 Scripts*, Page 347.
16	Setting up connections	Creating External Connections ● ISDN Set up the access to the public telephone network (PSTN). See *15 ISDN connections*, Page 245. ● SIP Trunk You need to have the access data for the relevant SIP provider. See *16 SIP Links*, Page 278. ● Further connection options: *17 SwyxLink (Server-Server Connection)*, Page 292 *18 ENUM Links*, Page 309 *19 SIP Gateway Links*, Page 321

Installation of Clients		
17	Install a Desktop Client and SwyxPhone	Install the telephony client or telephones of the SwyxPhone family on the workstation computers. See *20 Connection of SwyxPhone and SwyxIt!*, Page 331 and the SwyxIt! Classic documentation.

⚠ Do not under any circumstances change the name of the server computer after installing SwyxWare.

Extensions

Subsystem configuration	You can now ● integrate a sub-telecommunication system. See *D.1.4 Connecting a Sub-telecommunication System (Sub-PBX) to SwyxWare*, Page 419 ● operate SwyxWare as a sub-telecommunication system. See *D.2 Connection of SwyxWare as Sub-telecommunication System on a Main Telecommunication System*, Page 420.
SwyxDECT 500	Integrate a DECT system SwyxDECT 500. See SwyxDECT 500.
SwyxDECT 800	Integrate a DECT system SwyxDECT 800. See SwyxDECT 800.

General information

Update the operating system and save the database at regular intervals.

Backup copy	We recommend making backup copies on a regular basis. See *7.10 Backing up the SwyxWare Database*, Page 120
Updating	You will find information on the updating of SwyxWare via the link on the start page of the SwyxWare Administration, or on the website: enreach.com/products/support/support-downloads.html
Updates from Microsoft	Install on a regular basis the security updates recommended by Microsoft:
Knowledge base	Further information on special installation scenarios as well as tips & tricks for the optimal use of your SwyxWare can be found in the support database (Help Center). service.swyx.net/hc/en-gb

5.2 WHICH SERVICES BELONG TO SWYXSERVER

SwyxServer

In the Windows Server Service Manager you will find the SwyxServer service under the name "SwyxServer". It manages the users and assigns the calls. The Call Routing Manager scripts and use of the Graphical Script Editor. scripts are also run here.

SwyxConfigDataStore

The "SwyxConfigDataStore" service controls the access to the database for SwyxServer. All server parameters are stored in the database, such as user data, trunk parameters, trunk groups, announcements and scripts.

SwyxPhoneManager

The "SwyxPhoneManager" service is included in SwyxPhone support. It is responsible for the connection of the SwyxPhone Lxxx. SwyxPhone cannot be used unless this service is running.

SwyxQueueManager

This service is required for managing queues via Graphical Script Editor.

SwyxLinkManager

The SwyxLinkManager manages all connections that are not made via the public network, but rather via IP-WAN connections, e.g.SwyxLink, SIP or ENUM connections.

SwyxGate

SwyxGate is responsible for the communication with the public telephone network (PSTN). It manages ISDN connections according to installation via BRI or PRI connection.

SwyxRemoteConnector

This service facilitates connections from authorized subscribers to SwyxWare outside the local (LAN) or virtual private network (VPN).

SwyxConferenceManager

As Conference Manager, this service manages all initiated conferences and conference rooms. If this service is not active, no conference can be initiated from this location.

SwyxCTI+

The "SwyxCTI+" is licensed with the SwyxCTI+ option. This option allows you to control a telephony device with CTI SwyxIt! or to link CTI SwyxIt! with an external phone via its phone number.

SwyxFax Server and SwyxFax Printer Gateway

These two services belong to the SwyxServer and are licensed with the SwyxFax option pack. They are used both for receiving and sending fax documents, and for outputting these documents on a printer.

Swyx Utility Program

The "Swyx Utility Program" service monitors the current processes of SwyxWare. Each SwyxWare component automatically registers itself with Swyx Utility Program each time it is started. The Swyx Utility Program then checks these components regularly and terminates them if there is a malfunction. If automatic restart has been configured under "Restore" in the options of the service, (this is automatically done by the SwyxWare installation program), WindowsServer will restart these components. If the component is terminated manually, it removes the registration with Swyx Utility Program automatically and no restart will occur.

SwyxReporting

The service "SwyxReporting" is always installed, but is only activated in SwyxWare for DataCenter and SwyxON . On the back end server this service ensures that the usage reports are sent, see *7.5.12 The "Usage Reports" Tab*, Page 102.

SwyxUaCSTA

This service enables the control of certified SIP telephones via SwyxCTI.

Swyx Management Service

This service provides a REST API that is used by the Swyx Control Center to configure the SwyxWare.

SwyxMSTeamsPresenceSync

This service integrates the user status of Microsoft Teams into SwyxWare. The display of status information ("Logged out", "Reachable", "Speaking", "Do not disturb", "Away") is synchronized with the data from MS Teams.

The service is installed by default and is in an inactive state. To use the corresponding functions you have to activate the service via Swyx Control Center, see

help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/index.html#context/help/MSTeams_synch_$

MS Teams Mode

This service supports the integration of SwyxIt! Classic functionality into Microsoft Teams via SwyxIt! Classic Connector for Microsoft Teams App.

5.3 PREPARATION FOR INSTALLATION

Before you can execute the actual installation of SwyxServer, you must first take several preparatory steps as system administrator.

5.3.1 USER ACCOUNT FOR THE SWYXWARE COMPONENTS

The SwyxWare-Components are Windows Server services and should be **own** Domain user account or a local Windows user account through which they have access to system resources. When doing this, please do **not** use the predefined, local administrator account, **nor** another user account with administrator rights.

SwyxWare is installed and updated by a user with local administrator rights. The user account for the installation must be allowed to add domain user accounts to groups.

The configuration or administration of SwyxWare can be executed by a user who has been assigned corresponding administrator rights in the SwyxWare Administration. See *9.3 Administration profiles*, Page 143. He does not need to have any local administrator rights.

How to prepare for installation

1 Create a new domain user, e.g. called ‘swyxpbx’.
A domain user account is mandatory if
- SwyxWare components such as, SwyxServer, SwyxGate and SwyxPhone support are to be installed on more than one computer,
- Fax documents are to be output to a network printer. In this case, the user under which the "SwyxFax Printer Gateway" service is running requires access rights to the network printer, or
- the Calendar-Based Call Management (access to e.g. a Microsoft Exchange server) is to be used. In this case please execute also step (2).

2 If you want to use Calendar-Based Call Management within the Call Routing Manager, you must, before installing SwyxWare, install the Outlook profile for the SwyxServer user account (‘swyx pbx’), see *5.3.3 Installation for Calendar-Based Call Management*, Page 51.

5.3.2 INSTALLATION OF THE ISDN CARDS

If SwyxServer and SwyxGate are to be run together on one computer, then you must now install the ISDN cards.

Install and configure the ISDN cards and drivers as described in *15.2 Installation of the ISDN Cards*, Page 246.

You will find information on the test programs for the ISDN connection in *App. E: Tools & Traces*, Page 424.

5.3.3 INSTALLATION FOR CALENDAR-BASED CALL MANAGEMENT

The following provides a description of the integration of SwyxWare in an environment with Microsoft Outlook and a Microsoft Exchange Server.

In order for SwyxWare users to be able to use Calendar-Based Call Management, the exchange mailbox of the corresponding user must be entered in the SwyxServer user configuration.

How to configure the Calendar-Based Call Management

1 Start SwyxWare Administration.

2 Move to the "Users" directory.

3 Please select a user and click with the right mouse button on the list entry.

4 In the context menu, select "Properties".
The "Properties of..." window of the user will appear.

5 Click on "Administration..." on the "Preferences" tab.

6 Select the "Advanced" tab.

7 In the field "Mailbox", enter the corresponding Exchange user (*Calendar Access*, Page 173).

Please note that according to the default settings, Microsoft Exchange Server or Outlook changes which users make in their Outlook Calendars will be updated only every 15 minutes and made public for a six-month period. If this interval is too long or you would like to publish appointments for a period longer than 6 months, you must modify the local Outlook settings for the appropriate user as described in the following.

How to reduce the update interval

1. Start MS Outlook by using the Windows user account of the user to be configured.
2. In the main menu, under "File | Options | Calendar" click on the "Free/Busy Options..." button.
3. In the "Authorizations" tab, click on "Free/Busy options".
4. Within the dialog "Free/Busy Options" you can now enter the interval length for the update and the time period of the appointments to be published.
5. Then confirm all open dialogs by clicking on "OK".

5.3.3.1 MICROSOFT EXCHANGE SERVER

If Exchange Server is used, additional requirements apply.

You must create a user in the Exchange Server who uses the same Windows user account ('swyxpbx') under which the SwyxWareservices also run. See *5.3 Preparation for Installation*, Page 50

After this action, SwyxServer can access the Exchange server via the MAPI interface and the appointment-based call management is available to SwyxWareusers.

5.3.4 INSTALL MICROSOFT SQL DATABASE

A database is required for the administration of the user data. You can choose from various options:

- Microsoft SQL Server Express
  Microsoft SQL Servers Express can be downloaded directly from the SwyxWare DVD.
  See *5.3.4.1 Microsoft SQL Server Express installation*, Page 52.
- Microsoft SQL Server Standard Edition
  For larger installations, e. g. an installation, please use a Microsoft SQL Server (e. g. Standard Edition).

The database server must be set up before the installation of SwyxWare.

Please refer to the Microsoft documentation to find out which database is suitable for your scenario:

learn.microsoft.com/en-en/sql/sql-server/editions-and-components-of-sql-server-2022?view=sql-server-ver16

5.3.4.1 MICROSOFT SQL SERVER EXPRESS INSTALLATION

The installation of a Microsoft SQL Server Express is briefly described below. For further information please refer to the associated Microsoft documentation.

Microsoft SQL Server Express is installed using the software contained on the SwyxWareDVD.

> Before starting the software, please confirm that there is no SQL Server installed on the target computer, as this will not be checked by the installation program.

How to install an MS SQL Server

1. Start the installation of the MS SQL Server.
2. Click on "New Installation or Addition of Functions to an Existing Installation".
3. Accept the license agreement and click on "Next>".
4. Accept the installation of the product update and click on "Continue>".
5. Install the Setup support files by clicking on "Next>".
6. Function selection:
   Various function parameters can then be configured.
   Click on "Next>".
7. Instance name:

You can create an instance name here, if you want to install multiple database instances on one SQL Server.
It is recommended to keep the default values.
Click on "Next>".

8 Service accounts:
Keep the standard parameters and click "Next>".

9 Account Provisioning:
Choose "Mixed mode" and give the password for the SQL Server System administrator account. Confirm the password.

10 Click on "Add..." to allow the members of the local administrator group to access the SQL Server. Click on "Next>".

11 Click on "Install" to start the installation.

The installation wizard now installs the SQL Server with the given parameters.

If you change the name of the server computer after the installation, please follow the instructions contained in the following Technet article:
technet.microsoft.com/en-US/library/ms143799.aspx

Make sure that most recent service pack is installed for your SQL Server, and check regularly, e.g. on the Microsoft Security Website (www.microsoft.com/security), if other security-relevant updates for this Microsoft software exist; and if so, install them.

5.4 INSTALLATION OF SWYXSERVER

The installation program makes SwyxWare installation very easy. If you have already installed SwyxWare components, such as SwyxServer, PhoneManager or SwyxGate, then you can modify the selection of installed components. In this way you can remove or add components from/to the installation.

You can start the configuration of SwyxWare for DataCenter via command line with the following command:
"msiexec.exe /i setup.msi HOSTED=1"
See *5.4.4 SwyxServer installation via command line*, Page 60.

5.4.1 SWYXWARE - RUN SETUP

The installation of SwyxServer is carried out by a Microsoft Windows Installer file.

How to perform installation with the help of SwyxWare Setup

1 Close all Windows applications.

2 Mount the ISO image or unpack the SwyxWare DVD zip file.
In case the setup does not start, double-click on the file autorun.exe, which is located on the SwyxWare DVD.

3 The SwyxWare Setup start page will appear.

4 Select "Install SwyxServer".
The system checks whether the necessary requirements have been installed.
If they are not, you can install them directly from the DVD, by clicking on the relevant link.
Please follow the instructions and click on "SwyxServer".
The SwyxWare installation will open.

5 Accept the license agreement.

6 Use the Installation Wizard to define the components you wish to install.
- SwyxServer
handles user administration, and contains as an additional component the AutoAttendant. You can individually select the components during the installation.
- Auto Attendant
Auto Attendant with support and sales groups
- SwyxConferenceManager
manages all conferences and conference rooms
- SwyxPhoneManager

manages the connection of the telephones (SwyxPhone)

- SwyxGate
  for the connection to the public telephone network
- SwyxLinkManager
  supplies WAN connections (IP) to another SwyxServer or to a SIP provider or ENUM
- SwyxMobileExtensionManager
  manages the connection of mobile phones
- SwyxCTI+
  allows the control of phone devices and external phones via the phone number
- SwyxRemoteConnector
  Facilitates connections to SwyxServer outside a local and/or virtual private network
- SwyxUaCSTA
  enables the control of certified SIP telephones via SwyxCTI.
- SwyxFax Server
  enables transmission and receipt of fax documents.
- SwyxFax Printer Gateway
  enables automatic printing of received fax documents.
- Swyx Trace Tool
  manages SwyxWare protocol files and enables the transfer of these files to the support, see *E.5.1 Swyx Trace Tool*, Page 428
- Push Notification Service
  sends push messages to the mobile apps

The field next to the component selection contains a description of the selected component, the installation status and the required memory.

All components listed are installed in the default setting.

If you would prefer not to have a component installed on this computer (or later, separately), select "Unavailable" from the drop-down list. If you would like to install the individual components separately, deactivate the other components in the corresponding drop-down list.

Memory

With "Memory" you can display the current storage space allocation of the available disks.

7 Start installation:

- Click on "Next>". By clicking on "Install" in the "Start installation" dialog, the installation process starts. During this process the required files will be copied and the registration database entries will be made.

Complete the installation using the Configuration Wizard.

See *5.4.2 Configuring SwyxWare*, Page 54.

5.4.2 CONFIGURING SWYXWARE

After the installation the Configuration Wizard starts. Use this Wizard to define the configuration parameters for the installed components.

The Configurations Wizard can also be started again later in an existing installation, e.g. in order to make changes to the SwyxWare configuration.

For online licensing, have the activation key that you received from your service provider ready.

Please note that the SwyxWare suspends all SwyxWare services. Even active calls are interrupted. It is not possible to telephone during configuration with the configuration wizard! If the configuration wizard is interrupted, all services remain suspended. If you quit the configuration wizard, all services will be started again.

This is how you configure SwyxWare

Under "Start | Programs | SwyxWare | SwyxWareConfigurations Wizard " you can start the Configurations Wizard.

1 Connect to SQL Server
Enter here the SQL Server instance on which you want to set up the database for SwyxWare.

- Windows authentication (Standard)
  Select this form of authentication if the user currently logged in has administrative rights on the SQL Server.

- SQL Server authentication

  Alternatively, select authentication with the name and the associated password of an SQL Server user.

> The Windows user account specified here must have administrator rights on the SQLServer instance to create a new database. If an existing database is to be updated, administrator rights to this database ('db_owner') are required.

2 Database installation type:
You can choose whether you

- create a database

  This is only possible if an SQL Server is installed **locally**. The standard settings are used in this case and the SwyxWare database schema is installed.
  Enter a name for the new SwyxWare database and a user name with password. The user account under which the Configurations Wizard now accesses the SQL Server needs the rights of an SQL Server administrator ('sysadmin') in order to create the SwyxWare database.
- use an existing SwyxWare database

  Select an existing database from the drop-down list. For this, the user account specified in step (1) needs at least the rights of a database owner ('db_owner').

3 Select database account
SwyxServer needs only restricted rights for database access. If you have selected an existing database, specify here the user name and password with which the SwyxServer should access the database.

For the rest of the installation the Configurations Wizard grants the necessary rights (db_datawriter; db_datareader; IpPbxUser) to the user account specified here.

4 SwyxServer Database:

- Create... or Update...

  Click on "Create..." to create a new local database.
  If an existing database was selected, the database schema can be updated here.
- Restore**

  You can also use "Restore" here to restore an existing local database, e.g. from an older SwyxWare installation.
- Backup*

  You can create a backup copy of your database later, see *7.10 Backing up the SwyxWare Database*, Page 120.

> Please note that when using an existing database the update of the database is irreversible. The Configurations Wizard automatically updates the existing database of an older SwyxWare installation. In addition, a backup copy is made before the update of a local database. You can find this backup copy in the SwyxWare program directory under "C:\ProgramData\Swyx\Backup".

Only local databases can be restored or backed up here. A database that is installed on another computer cannot be backed up or restored by the Configuration Wizard. Use the mechanisms provided by Microsoft for this.

5 Service account:
Here you set the user account which should be used to start the SwyxWare system services (for example ’ippbx’).
A domain user account is required, if

- different components are installed on different computers (e.g. a separate gateway)
- SwyxFax Printer Gateway will send printing jobs to a network printer
- The calendar-based call management will be used

The user name should be selected by using the "Browse" button. You then only enter the password. The validity of your entries will be checked by the Setup program. This check may take several seconds. If there is an error in the entries an error message will appear and you can repeat the procedure.
If SwyxServer does not need a domain user account, you can let the Configuration Wizards create a local user account.
The service account will also be added to a locally created group called ’SwyxWare Services’. This group is used exclusively for the SwyxWare services.

6 Service Account Information
The Configuration Wizard gives an overview of the user account used, and the created group.

7 Licensing (not for SwyxWare for DataCenter)

If you have selected the standard installation in step (5), you can choose between the following licensing types:

> The selected Licensing type, Online Licensing or Licensing via License Key, cannot be changed afterwards. If you want to select a different type of licensing after a licensing process has been completed, you must uninstall and reinstall SwyxWare and the SwyxWare database, see also chapter "Configuration of SwyxServer", section "Uninstalling".

- Online Licensing
  The Swyx license server sends requests to check the licence presence. For this purpose, there must be a permanent Internet connection between the license server and your SwyxServer, for which you can specify a proxy server in one of the following steps or later, see step (8). Additionally you have to create an instance for your system in the Swyx Operator Portal.
- Use the Licensing via license key, see *3 Licensing via license key*, Page 30
- Test installation (limited license key)
  Use the Licensing via license key, see *Evaluation Installation*, Page 28

The following steps only apply to the "Online Licensing" type of licensing:

8 Connect SwyxServer to the Swyx License Server
- Call Transfer
  Click on the button to test the connection to the Swyx license server.

9 Enter the activation key you received from your service provider.

10 You can also use a proxy server for the connection, which you can define in this step or later via Swyx Control Center, see also the Swyx Control Center documentation, section "Defining proxy servers".
- Outbound HTTP Proxy
  Enter the IP address or DNS name of the proxy server.
- Encryption mandatory
  Select the check box if authentication is required to connect to the proxy server.
  Enter the user name and password for authentication.

11 When you have defined a proxy server, a step for re-testing the connection to the Swyx license server appears.

12 If you have activated the programme via Swyx License Server, a step to activation via SwyxServer will appear. Click on "Activate".

13 If the activation has failed, a step to re-check the Internet connection appears.
Click on "Activate" and/or repeat the activation in Swyx Operator.

> You can also enter the license key later via Swyx Control Center, see also the Swyx Control Center documentation for users, chapter "Editing General Settings", section "Entering License Activation Keys".

The following steps apply only to SwyxWare for DataCenter:

14 License Server
- Use this system as licensing server
  The current system (back end server) is configured as licensing server. The SwyxWare for DataCenter license is read in on this system. All other SwyxWare for DataCenter installations (front end servers) contact this installation to license themselves in turn. The reporting service must be activated on this server.
- Connect to a SwyxWare for DataCenter licensing server
  Enter here the name of the licensing server. The configured system then contacts the licensing server regularly to confirm the license validation.

15 Connect to SQL Server reporting database (for SwyxWare for DataCenter backend servers only)
Specify the SQL Server instance on which a reporting database was set up. Specify whether the Configurations Wizard should log in there with the current user account or with user name and password. For updating an existing reporting database, administrator rights ('db_owner') on this database are needed in any case.

16 Reporting database (for SwyxWare for DataCenter backend servers only)
Select a previously created reporting database. The user account specified in (15) must be 'db_owner' in this database.

17 Account for reporting database

The reporting service, which regularly records the license data of all servers, accesses the reporting database with restricted rights. Specify the user name and password for this access.

The following steps only apply to the licensing type "Licensing via license key":

18 SwyxWare licenses

If you want to insert license keys, click on "Add License...". Another window, "Add SwyxWare License Key" will now open. Indicate whether you will enter a limited or a permanent license from your license certificate (PDF). The limited license key is sent to you as a PDF.

Enter the limited license key or the name of the file containing the permanent license key.

Use this step to add all license keys for the options you want to install.

If you are licensing a SwyxWare for DataCenter licensing server, you need only one license key.

The license key (PDF) supplied is limited to a period of 30 days and includes the number of users and channels you have ordered. After the key is entered, the corresponding licenses will be shown.

Install SwyxWare with these limited keys and request permanent keys after installation. You then insert this permanent license key into the SwyxServer configuration at this point by activating the option "File with permanent license keys", see *7.4 Pre-Configured Users and Groups*, Page 85.

If you chose a standard installation, continue with step (19), see *19 Mail server:*, Page 57.

The following steps apply to all types of licensing:

19 Mail server:

SwyxServer requires an e-mail server to send voice messages, fax mails and usage reports (for SwyxWare for DataCenter) .

Enter the name of the mail server to be used for email delivery in the field "Name of the SMTP Mail Server".

Every Email which is sent by the SwyxServer contains the Email address entered in the field "Voice Box originating address" as the sender. Enter here the email address of the SwyxWare administrator, for example.

20 SwyxServer location:

- Time zone

  From the selection list, choose the time zone that is applicable for the default location of this SwyxServer.
- Own country code

  Here you define your country code. For the United Kingdom, it is '44’.
- Own area code

  Enter your area code here without the preceding '0', for example, '20' for London or '161' for Manchester.
- Prefix for international calls

  The code for international calls is entered in this field. In Germany, this code is '00'.
- Prefix for long distance calls

  Here you enter the digit(s) which must be dialed in order to make a long distance call. In Germany, the digit required for long distance calls is always '0'.
- Public Line Access

  This is the number that SwyxWare users must first dial in order to make external calls. Default value: ‘0’.

21 Create an administrator account to log in to Swyx Control Center.

22 Swyx Messenger

From SwyxWare version 12.10 onwards, a new Messenger with a wide range of functions is available.

For further configuration steps see the Swyx Control Center documentation, section "Connection to Cloud Services".

By default, SwyxIt! Classic accepts connections from Swyx Messenger on port 5000. This port can be used by another program and Swyx Messenger will not work.
In this case you can change the address port, see *20.3.4 SwyxIt! Installation from the Command Line*, Page 338

> For the provision of the Swyx Messenger / Swyx Meeting service, user-related data will be transmitted to and processed by our order processor, Voiceworks B.V. (also part of the Enreach Group) on the basis of a corresponding order processing contract. These products require the transmission of various data such as IP address, login data, chat messages, names of communication partners, dial-in numbers (Swyx Meeting), files sent and screenshare content (Swyx Meeting) each time they are used. Please note your duty to inform your users according to Art. 13/14 GDPR.

23 Active Directory extension
You can integrate the SwyxWare user administration into a Windows Active Directory environment.
If the log-in user account doesn't have the according rights, please enter under "Register" a user account (name and password) which has the authorization to change the Active Directory configuration, e.g. a domain administrator account.

24 SwyxPhone Firmware Update

> This function is not available for SwyxWare for DataCenter.

You can automatically update the SwyxPhone software from the FTP server at Enreach.
If you would like to set up your own FTP server, you can enter the required data in the SwyxWare Administration.

25 Conference:
Define the user under which the ConferenceManager will later log in to the SwyxServer (default name: Conference).
The user "Conference" is always created. For SwyxWare Conference rooms and conferences with more than three participants are only possible if you install the option pack "SwyxConference".
In a SwyxWare for DataCenter area, conferences become possible with the "SwyxAdHocConference" option.

26 After installation, set up ISDN trunks in the SwyxWare Administration. The link to SwyxGate is made via the name of the computer on which the service was installed.
See *This is how you create an ISDN Trunk*, Page 267.

27 The SwyxWare-database is configured with the parameters entered.

28 SwyxFax Server Properties
Enter here the Fax Station ID of SwyxFax Server.

29 SwyxFax Server configuration overview
The parameters for the SwyxFax- configuration are displayed.

30 Configuring the fax settings (Not available for SwyxWare for DataCenter)
The displayed SwyxFax configuration takes place. As many fax channels are created as licenses are present. The configured Fax Station ID is configured on all fax channels, and can be changed later in the properties of the individual fax channels.

31 Automatic updating of the system phone whitelist
You should determine a Windows task for the automatic daily updating of the system phone whitelist.
Activate the "Create scheduled task" checkbox. A new task "PhoneWhitelistUpdate" is created in the Windows task schedule and executed once. I. e. the whitelist is updated immediately. See *Install and update Whitelist*, Page 331.

> If you do not activate the "Create scheduled task" checkbox any exisisting tasks for the automatic update of the whitelist will be removed.

32 If Internet connections with Swyx Clients should be supported, activate the SwyxRemoteConnector. As of V13.20, RemoteConnector is no longer configured in the configuration wizard. The required settings can be defined in the Swyx Connectivity Setup Tool (SCST), see *6 Swyx Connectivity Setup Tool*, Page 68

33 Close the configuration wizard afterwards with "Finish".

All services (SwyxServer, SwyxConfigDataStore, SwyxGate, PhoneManager, Swyx Utility Program, Conference Manager) will be started automatically during the configuration and are ready for operation after the configuration.

> If you change the name of the server computer after the installation, please follow the instructions contained in the following Technet article:
> technet.microsoft.com/en-US/library/ms143799.aspx

You will find information on how to install SwyxWare Administration in *5.5 Installation of the SwyxWare Administration*, Page 64.

The Configurations Wizard creates a trace file ConfigWiz-<time in format yyyy.mmdd-hhmmss>.log. You will find this, like all other trace files, in the directory <common_app_data>\Swyx\Traces. Here, <common_app_data> is the standard application directory of Windows, e.g. C:\ProgramData

See also *E.5 Traces of the SwyxWare Services*, Page 428.

5.4.3 INSTALL SWYX CONTROL CENTER

The installation is carried out by a Microsoft Windows Installer file. Swyx Management Service provides a REST API that is used by Swyx Control Center.

> If you want to use SwyxWare with third-party products, you need to install the "Swyx Management Service" component.

How to install Swyx Control Center

1. Close all Windows applications.
2. Start SwyxControlCenter.msi.
   The installation assistant for Swyx Control Center appears.
3. Accept the license agreement and click on "Next>".
4. Specify the components you want to install:
   - Swyx Control Center

   SwyxWare Web-Administration
   - Swyx Management Service

   Provides a REST API that is used by Swyx Control Center.
   The field next to the component selection contains a description of the selected component, the installation status and the required memory.
   All components listed are installed in the default setting.
   If you would prefer not to have a component installed on this computer (or later, separately), select "Unavailable" from the drop-down list.
   "Not available". If you would like to install the individual components separately, deactivate the other components in the corresponding drop-down list.
   Memory
   With "Memory" you can display the current storage space allocation of the available disks.

> To install Swyx Management Service later, start SwyxControlCenter.msi again and select the option "Change".

5. If necessary, specify the desired installation path and port to identify the corresponding network service.
6. Activate the checkbox if you want the shortcut to be stored on the desktop and click on "Next>".
7. If you have selected the Swyx Management Service component, enter the IP address of the Config Data Store.

> By default, the IP address of the Config Data Store is 127.0.0.1. If the service is installed on another computer, enter the address of that computer.

8. Click on "Install".

After successful installation you can access Swyx Control Center via the Windows Start menu or via the URL in a web browser. By default, the URL for local access is https://localhost:9443/swyxcontrolcenter, see *5.4.5 Installing Swyx Control Center via command line*, Page 61.

> If you want to access Swyx Control Centerfrom a computer other than the installation computer, replace "localhost" in the URL with the IP address and port of the installation computer.
> See also *5.4.6 Swyx Control Center use with your own SSL certificates*, Page 61.

5.4.4 SWYXSERVER INSTALLATION VIA COMMAND LINE

You can also start the installation of SwyxServer by opening it via the command line. For this type of installation it is always advisable to create a log file (msiexec /l or /l*v for a detailed log). Start the installation with the command "msiexec /i". You can control the scope and the progress of the installation with certain parameters.

You want to install SwyxServer with all available functions, without further user inputs ("silent"):

```
msiexec /qn /i Setup.msi
```

You can use the following parameters

Parameter	Explanation
msiexec /i	Start of installation
Server.msi	Name of installation file Please check that the name of the MSI installation file is correct.
/qn	Silent installation The installation of SwyxServer does not require any user entries. If you don't use this parameter, the installation wizard is started as for the normal installation. Each separate step must then be confirmed with the "Next" button, and the predefined options can be changed.
ADDLOCAL	Definition of the functions You will find the available features and components in the following table.
/l*v <Name of the log file>	Generation of a detailed log file during the installation A log file (*.log) enables you to detect errors during the installation. The directory to which the log file will be written must already exist.
INSTALLDIR	Specification of the installation directory This option allows you to set the directory in which SwyxServer is to be installed.
/help	Help function This option displays further parameters of the Windows Installer, which you may be able to use.

The following table contains the functions valid for ADDLOCAL:

Parameter	Component name
All	All available options are installed.
IpPbxSrv	SwyxServer, this option MUST be specified, unless you use the parameter "All".
AutoAttendant	Installation of an AutoAttendant including creation of "Support" and "Sales" groups
ConferenceMgr	SwyxConference Manages telephone conferences (virtual conference rooms)
FaxPrinterGateway	SwyxFax Printer Gateway Enables automatic printing of received fax documents
FaxSrv	SwyxFax Server Provides fax functionality
IpPbxGate	SwyxGate Connects IP telephony with classic telephony
LinkMgr	SwyxLinkManager Connects SwyxServers to each other or handles the connection of SIP providers
MobileExtensionMgr	SwyxMobileExtensionManager Connects mobile phones to the telephone system
PhoneMgr	SwyxPhoneManager Connects telephone terminal devices to the telephone system
IpPbxUaCSTASrv	This service enables the control of certified SIP telephones via SwyxCTI.
IpPbxConnectSrv	SwyxRemoteConnector Facilitates connections to SwyxServer outside a local and/or virtual private network

Parameter	Component name
TraceTool	Swyx Trace Tool Logs activities of the SwyxWare services
IpPbx3pcc	With SwyxCTI+, a phone device or an external phone can be controlled via its phone number
IpPbxMgmt	Swyx Management Service Provides a REST API that is used by the Swyx Control Center to configure SwyxWare.
FeaturePresenceSyncMsTeams	MS Teams user status information this service integrates the user status of Microsoft Teams into .
FeaturePNS	Push Notification Service sends push messages to the mobile apps

5.4.5 INSTALLING SWYX CONTROL CENTER VIA COMMAND LINE

You can also start the installation of Swyx Control Center by opening it via the command line. Start the installation with the command "msiexec /i". You can control the scope and the progress of the installation with certain parameters, e. g.:

```
msiexec /i "SwyxControlCenter.msi" /passive /l*v
MyLogFile.txt WEBSITEFOLDER= "C:\Program Files\Swyx"
INSTALLPORT=9443 INSTALLSHORTCUT=1
```

You can use the following parameters:

Parameter	Explanation
msiexec /i	Start of installation
SwyxControlCenter.msi	Name of installation file Please check that the name of the MSI installation file is correct.
/passive	Use this parameter to display the installation progress bar. No prompts or error messages are displayed. The installation cannot be aborted.
/l*v <FileName>.txt	Use this parameter to record the installation process in a log file.
WEBSITEFOLDER	This option allows you to set the directory in which the IIS-Website is to be installed. Standard value: /swyxcontrolcenter
INSTALLPORT	This option allows you to set the port for the IIS web site, (from 1 to 65535) default value: 9443.
INSTALLSHORTCUT	You can use this option to specify whether a desktop shortcut is to be stored for the call. (=0:no, Default value: =1:yes).

5.4.6 SWYX CONTROL CENTER USE WITH YOUR OWN SSL CERTIFICATES

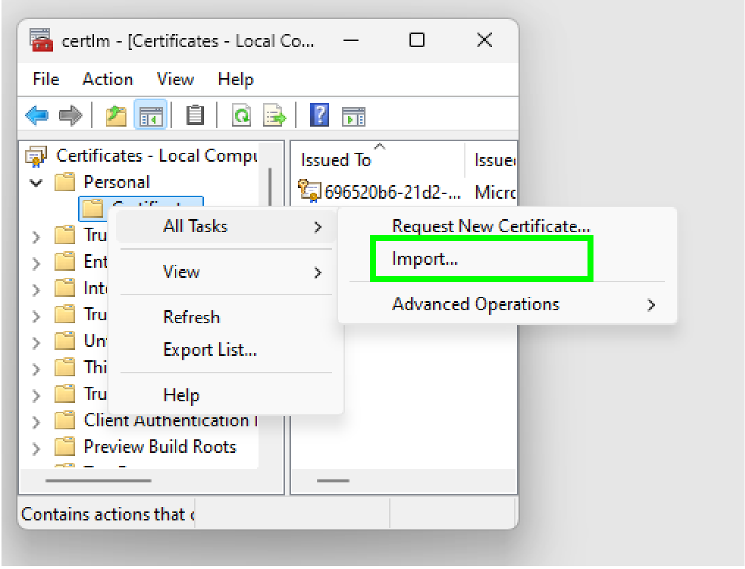
SSL certificates are automatically configured during the installation of the Swyx Control Center. You can also use your own certificate.

How to import your own SSL certificate for Swyx Control Center

1 Search for "Manage computer certificates" in the Windows search bar and open the certificate manager.

2 Open Certificates - Local Computer | Personal | Certificates.

3 Open Certificates | All tasks | Import... in the context menu.



4 Click on Next.

5 Select the certificate file from the directory and click Next.

6 Leave the "Personal" area as the storage destination and click Next.

7 Click on Finish.
✓ Your certificate is imported and appears in the Certificates - Local computer | Personal | Certificates list.

To assign the SSL certificate to the Swyx Control Center port (default: 9443)

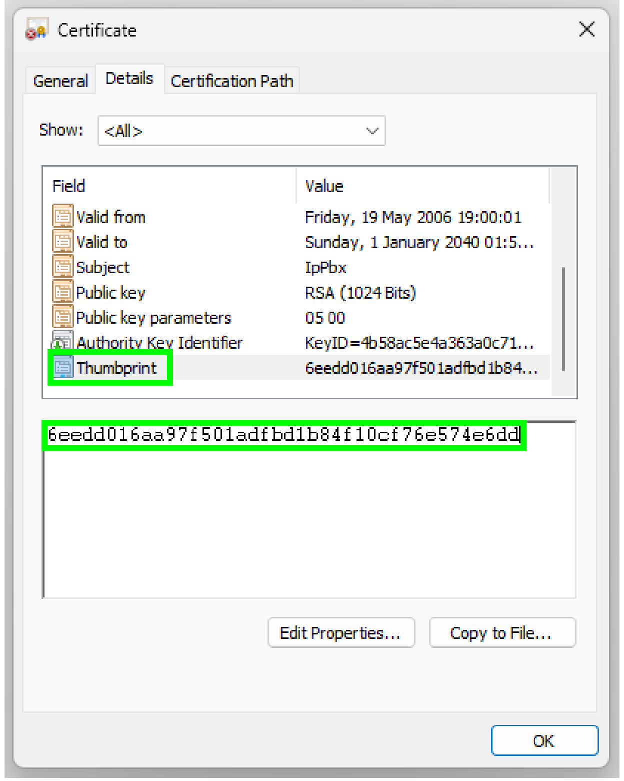
You have imported your own SSL certificate.

1 Search for "Manage computer certificates" in the Windows search bar and open the certificate manager.

2 Open Certificates - Local Computer | Personal | Certificates.

3 Double-click on the imported certificate.

4 Select the Details tab and click on the Thumbprint field.



Field	Value
Valid from	Friday, 19 May 2006 19:00:01
Valid to	Sunday, 1 January 2040 01:5...
Subject	IpPbx
Public key	RSA (1024 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=4b58ac5e4a363a0c71...
Thumbprint	6eedd016aa97f501adfbd1b84...

6eedd016aa97f501adfbd1b84f10cf76e574e6dd

5 Copy the thumbprint into a text file.

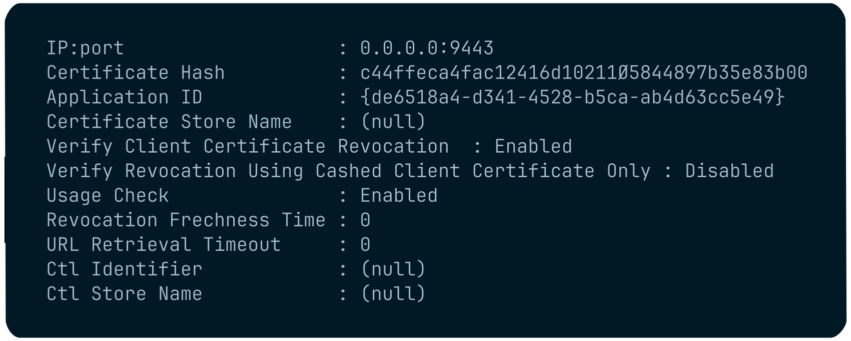
6 Make sure that the copied thumbprint does not contain any trace characters.

7 Start Windows PowerShell as an administrator.

8 Make sure that no SSL certificate is assigned to port 9443, e.g. with the following command:

```
netsh http show sslcert | Select-String ":9443" -
Context 0,10
```

9 If an SSL certificate is assigned to the target port, check the corresponding details:
Here is an example:



```
IP:port                      : 0.0.0.0:9443
Certificate Hash             : c44ffeca4fac12416d1021105844897b35e83b00
Application ID               : {de6518a4-d341-4528-b5ca-ab4d63cc5e49}
Certificate Store Name       : (null)
Verify Client Certificate Revocation  : Enabled
Verify Revocation Using Cashed Client Certificate Only : Disabled
Usage Check                  : Enabled
Revocation Frechness Time : 0
URL Retrieval Timeout        : 0
Ctl Identifier               : (null)
Ctl Store Name               : (null)
```

10 You can cancel the assignment of the existing certificate with the following command:

```
netsh http delete sslcert ipport=0.0.0.0:9443
```

11 Assign your own SSL certificate to port 9443:

```
netsh http add sslcert ipport=0.0.0.0:9443
certhash=<Thumbprint> appid="<GUID>"
```

Parameter	Explanation
<Thumbprint>	Thumbprint of the certificate, see steps 4,5,6
<GUID>	Application GUID, which you can define yourself, or it is best to use the following {de6518a4-d341-4528-b5ca-ab4d63cc5e49}

5.4.7 UNATTENDED CONFIGURATION

In unattended setup, the SwyxWare configuration is run without the need for inputs in the configuration wizard.

Instead, the configuration settings are stored in the file "Unattended.xml". You will find this file on the SwyxWare DVD in the "SwyxWare" directory.

There is extensive comment in the file to assist with the input of the parameters.

The "mode" attribute, which you set at the beginning of the file "Unattended.xml", controls how the configuration will be executed - unattended, or with the help of the graphic configuration wizard:

Attribute, Mode	Explanation
off	The graphic configuration wizard starts automatically after the SwyxServer installation has run. Unattended configuration is deactivated.
automatic	The configuration takes place unattended with the help of the stored parameters. The graphic configuration wizard is deactivated.
manual	Neither the unattended configuration nor the graphic configuration wizard will start. This mode can be used to start the configuration with the help of a script.

This is how you execute the SwyxWare configuration using the file "Unattended.xml"

1 Copy the directory "SwyxWare", which is on the DVD under "DVD Files | Swyx", locally on your computer.

2 Open the file "Unattended.xml" (also in this directory) with an editor. It is advantageous to use an XML editor.

Before the installation is executed, the file "Unattended.xml" must be in the same directory as the file "Setup.msi". This is the only way to ensure a successful call of the file.

3 Set the execution mode within the file, and store the configuration parameters of your choice.
Save the changes.

4 Close all Windows applications.

5 Make sure that

- Microsoft .NET Framework 4.7.2 and
- Microsoft Visual C++ Redistributables (x86 and x64) are installed.

is installed. If they are not, you can install them directly from the DVD, by clicking on the relevant link. Follow these instructions. You will find further information on the unattended setup of Microsoft .NET Framework in the Microsoft documentation.

6. Execute the installation of SwyxServer from the command line. See *5.4.4 SwyxServer installation via command line*, Page 60.
7. If you have set the execution mode in the file "Unattended.xml" to "automatic", the configuration of SwyxWare then takes place automatically after the installation, unattended in background. Another command line window opens. When the configuration is complete, the window closes automatically.

During the installation, your configured file "Unattended.xml" is copied into the SwyxWare installation directory. If you want to start the graphic configuration wizard once again later, you must first set the execution mode within the file to "Off", before calling the wizard. Otherwise the call of the graphic configuration wizard will remain suppressed, and the unattended configuration will be run once again.

5.5 INSTALLATION OF THE SWYXWARE ADMINISTRATION

The administration of a SwyxWare installation is done using a snap in module for the Microsoft Management Console, the SwyxWare Administration.

Start the installation of the SwyxWare Administration after the SwyxWare installation. You can additionally install the SwyxWare Administration on further computers in the network and administer SwyxWare remotely.

Prerequisites for the SwyxWare Administration

The following prerequisites apply for the installation of the SwyxWare Administration:

- Operating system: Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022 or Windows Server 2025.
- Microsoft .NET 4.7.2 Framework
- Mirosoft Visual C++ Redistributalbes (x86 and x64)
- 180MB of free disk space

How to install the SwyxWare Administration on a Windows computer

1. Verify that all prerequisites are fulfilled, see *Prerequisites for the SwyxWare Administration*, Page 64.
2. Mount the ISO image or unpack the SwyxWare DVD zip file.
   The Setup program will start automatically.
   In case the setup does not start, double-click on the file autorun.exe, which is located on the SwyxWare DVD.
   The SwyxWare Setup start page will appear.
3. If the necessary preconditions are satisfied, click on "Install SwyxWare Administration".
   Depending on the current system, the 32bit or 64bit variant is installed.
4. The installation start page for SwyxWare Administration will appear.
   Click on "Next>".
5. Accept the license agreement.
   Click on "Next>".
6. Read the latest information.
   Click on "Next>".
7. Select the components to be installed, here "SwyxWare Administration":
   - SwyxWare Administration
     Is used for the configuration of SwyxServer. Additional components you will find here are Call Routing Manager and Graphical Script Editor, which are used for creating scripts.
     - Desktop link
     Please specify whether you would like to create a desktop shortcut.

- PowerShell support
  Installs the PowerShell expansion for SwyxWare.
  See *E.1 PowerShell support*, Page 424.
  - Script execution rule
  Sets the script execution rule for Windows PowerShell to "All-Signed". Only scripts generated by a trustworthy author can be executed. This option is necessary for SwyxWare PowerShell support and must be activated.
- AD Integration
  Installs the interface for the SwyxWare Active Directory integration. See *11.6 Configure users in the Windows user administration*, Page 209.

You can view the hard disk memory usage here, and specify the installation directory for the SwyxWare Administration.

8 Start the installation.
The installation will be performed automatically. The SwyxWare Administration is then available to you.

Installation of the Active Directory extension

The component "Active Directory Extension" is a native 64bit module, therefore it requires the 64bit version of the SwyxWare Administration.

If Windows Server is installed as domain controller, the associated tools (Domain Services tools) are installed by default and links are created under "Control Panel | Administrative Tools".

If the Windows Server computer is not installed as domain controller, these tools may be installed subsequently.

5.6 SWYXWARE UPDATE

This chapter describes how to update SwyxWare.

In order to update SwyxWare, you must have installed a released version of SwyxWare.

It is **not** possible to upgrade an installation of SwyxWare to a SwyxWare for DataCenter or vice versa.

The server components of SwyxWare should be updated first, then the clients.

Please perform a complete data backup before upgrading SwyxWare.

5.6.1 CHANGES BETWEEN THE VERSIONS

Before updating, please back up the database, see *7.10 Backing up the SwyxWare Database*, Page 120, and, if necessary, the directories in which the fax documents are saved (default setting: "C:\ProgramData\Swyx\IpBbxServer\Data").

Before you update an existing SwyxWare installation, please note especially the latest information in the ReadMe:

help.enreach.com/readme/latest.version/web/Swyx/en-US/ReadMe.html#SwyxServer

5.6.2 PREPARATION

Local administrator rights on your Windows Server are mandatory for updating the software.

When you update SwyxWare for DataCenter you must update the Reporting Server before you update the Frontend Server.

As already described in *5 SwyxWare Installation*, Page 47, the SwyxWare server services may run on a local user account, if no SwyxWare services are operated on other computers and use the local server. Nevertheless it is recommended to run the services on a domain user account. In this case name and password of the domain user account are required for an update.

An existing installation can be simply updated by starting the SwyxWare setup. If a SwyxServer is also running on SwyxGate it is necessary, for preparing upgrade of your ISDN card drivers, to stop the SwyxGate service and all utilities that access the ISDN card (e.g. Saphir Monitor or D channel monitor).

5.6.3 UPDATING THE ISDN CARD DRIVERS

SwyxWare also supplies updated drivers for your ISDN cards.

Please update the ISDN card drivers as described in the following.

How to update the drivers for SX2 cards

1. Start the device manager on the "Hardware" tab under "Start | Settings | Control Panel | System".
2. Under "Network adapter" choose the menu item "Update Driver..." in the context menu of the SX2 card.
   The Hardware Update Wizard is started.
3. Direct the launched wizard to the drivers on the download pages: https://www.enreach.de/produkte/support/support-downloads.html#cat_6
   The drivers are then updated. All settings remain unchanged.
4. If further ISDN cards are installed, please repeat steps 1 to 3 for each card.

Please also check whether the WAN Miniport driver has also been updated, see *Expert configuration - WAN parameters:*, Page 472.

5.6.4 EXECUTING THE SWYXWARE UPDATE

The update of your SwyxWare installation or the reinstallation of SwyxWare with takeover of the existing database is executed with the help of Microsoft Windows Installer.

You may need an update license key for the update. After the update, please request a permanent license key again in the SwyxWare Administration, see *7.5.5 The "Licenses" Tab*, Page 91.

With online licensing (Purchasing), the permission for an update is automatically checked.

It is not possible to update a SwyxWare to a SwyxWare for DataCenter.

How to update your SwyxWare installation using SwyxWare setup

1. Mount the ISO image or unpack the SwyxWare DVD zip file.
   In case the setup does not start, double-click on the file autorun.exe, which is located on the SwyxWare DVD.
2. Select "Install SwyxServer".
3. Please follow the instructions and click on "SwyxServer".
4. Follow the instructions provided by the Installation Wizard.
5. You can select the components to be installed.
   After a successful installation of the new software the Configurations Wizard will be started automatically.
   For further information on the Configuration Wizards, see *5.4.2 Configuring SwyxWare*, Page 54.
6. Following configuration of the SwyxWare, update the SwyxWare Administration by inserting the SwyxWare DVD, and starting autorun.exe if necessary.

5.7 SEPARATED SERVICES

Individual parts of SwyxWare can also be installed on a computer other than the SwyxServer, e.g. in order to distribute the computer work load. The following components can be installed separately from the SwyxServer:

- SwyxWare Administration
  Is used for the configuration of SwyxServer. The SwyxWare Administration can exist more than once in a network and it is configured using an independent installation program.
  See *5.5 Installation of the SwyxWare Administration*, Page 64.

- SwyxGate
  Represents the connection to the public telephone network. The ISDN card must also be installed on this PC.
  See *15.6 Installation of separated Gateways (SwyxGate)*, Page 275.
- SwyxPhone Support
  Is for the connection of the telephones to SwyxServer (SwyxPhoneManager). SwyxPhone support can exist more than once in a network.
  See *5.7.1 Installation of a SwyxWare component on an additional computer*, Page 67.
- SwyxRemoteConnectorServer
  Facilitates connections to SwyxServer outside a local and/or virtual private network. See *26.1 Internet connection via RemoteConnector*, Page 385.
- SwyxLinkManager
  Used for the link-up of a SIP, ENUM or SIP gateway trunk, or the connection to another SwyxServer via a WAN route.
  See *5.7.1 Installation of a SwyxWare component on an additional computer*, Page 67.
- SwyxConferenceManager
  This helps to manage conferences and conference rooms. SwyxConferenceManager can exist more than once in a network.
  See *5.7.1 Installation of a SwyxWare component on an additional computer*, Page 67.
- SwyxFax Server
  Enables fax documents to be sent and received. The licensing and administration of SwyxFax Server is handled centrally by the SwyxWare Administration. For communication, SwyxFax Server uses the ISDN cards in SwyxGate, which are also necessary for telephony.
  See *24.4 Install SwyxFax Server*, Page 362.

Only one SwyxFax Server can be set up on a SwyxServer.

- Database
  A separated database is supported, i.e. the database can also be installed on a separate computer.
  This component can be installed on a separate computer. See *E.5.1 Swyx Trace Tool*, Page 428

5.7.1 INSTALLATION OF A SWYXWARE COMPONENT ON AN ADDITIONAL COMPUTER

To install an additional SwyxWare component, please proceed as in the case of the installation of SwyxServer, whereby you only select the component you would like to install. See *5.4.1 SwyxWare - Run Setup*, Page 53.

Please note that Microsoft .NET Framework and Microsoft Visual C++ redistributables must also be installed for a remote SwyxWarecomponent.

In the case of a reduced installation, use the same domain user account under which SwyxServer was also installed.

After the installation and configuration, the corresponding services are started on this computer.

Please note that in the case of a separated installation, the corresponding service must be started on this computer. Otherwise, this functionality will not be available.

The administration of the SwyxWare components takes place via the SwyxWare Administration.

See *7 Configuration of SwyxServer*, Page 80.

6 SWYX CONNECTIVITY SETUP TOOL

SwyxWare is equipped with an automatically generated (SelfSigned) TLS certificate by default. The Swyx Connectivity Setup Tool (SCST) allows you to equip SwyxWare with an official trusted TLS certificate and optionally with a unique public server name (Fully qualified Domain Name, FQDN).

The TLS server certificate allows SwyxWare services and clients to ensure that you are communicating with the correct server in encrypted form. Swyx Control Center and the SwyxConfigDataStore service also use this TLS certificate on the provisioning interface for certified SIP phones, SwyxDECT 800 and the REST interface for client connections.

Currently, SCST does not support SwyxWare services installed on a machine other than SwyxServer.

RemoteConnector

You can define the settings for the RemoteConnector for SwyxIt! in the SCST.

The RemoteConnector for SwyxIt! is a SwyxWare service that enables and manages the connection of SwyxWare clients to SwyxServer from the Internet, see *26.1 Internet connection via RemoteConnector*, Page 385

settings of the RemoteConnector for SwyxIt! have no influence on the RemoteConnector for Yealink.

Connections to SwyxRemoteConnector are protected not only with a server certificate, but also with user-specific client certificates. This is why SwyxRemoteConnector uses its own X.509 root, server and client certificates. The RemoteConnector for SwyxIt! Certificates are independent of the TLS server certificate of the other SwyxWare services.

You can have RemoteConnector certificates (root and server certificate) generated and installed via SCST. You can generate client certificates manually for desired users or have them generated automatically for all users.

Split DNS in the internal network

The clients reaching SwyxServer on the internal network must also use the unique FQDN for which the TLS server certificate is issued.

It is not recommended that network traffic from clients on the internal network flow through their network's public IP and Internet router, rather than directly to SwyxWare. DNS queries for the IP address of the FDQN must be answered in your local network with the internal IP address of the SwyxServer.

Client type	Target SwyxServer Address	DNS configuration
External Clients	FQDN	External IP address
Internal clients	FQDN	Internal IP address of the SwyxServer

For this purpose, you need to set up a DNS service or server in your local network.

See *6.7 Configure Split DNS*, Page 78

Swyx Connectivity Setup Tool can only be started after the SwyxWare installation and its initial configuration in the SwyxWare configuration wizard has been done.

On the SwyxDECT 800 base station (Ascom) you have to install the TLS root certificate yourself, see *6.5 Install TLS root certificate on DECT 800 base station*, Page 76

If you equip SwyxWare with a trusted TLS certificate, you must ensure that SwyxServer and all clients that connect to SwyxWare receive the correct date and time. See also service.swyx.net/hc/en/articles/360000014639-SwyxPhones-need-correct-time-for-connections-to-the-SwyxServer-

If you are running a Windows domain on your internal network, the date and time on the Windows server and clients are already correctly synchronized.

See *Application scenarios of SCST:*

Application scenarios of SCST:

You can use SCST for the following purposes:

1) Obtain TLS certificate from Let's Encrypt (automatic certificate mode)

In this case SCST determines the currently used public IP address of SwyxServer and registers an FQDN within the SwyxON DNS service. SCST requests for this FQDN a TLS server certificate free of charge from the service provider **Let's Encrypt (letsencypt.org)** and installs the certificate in the SwyxWare, see *6.1 Use TLS certificate from Let's Encrypt*, Page 69

The prerequisite for this is that online licensing is used, see *2 Online Licensing*, Page 21

Certified SIP phones (Yealink) support the TLS certificate from Let's Encrypt and do not require additional TLS configuration.

2) Use your own TLS certificate (manual certificate mode)

If you prefer to use your own TLS certificate or one purchased from a commercial certificate authority (CA), SCST will help you to install it, see *6.2 Use own TLS certificate*, Page 72

When selecting this option, note that you must be in charge of your own DNS zone and the public IP address of your network must be resolved by a unique registered FQDN.

Certified SIP phones (Yealink) support TLS certificates from recognized certificate authorities (CA): https://support.yealink.com/en/portal/docDetail?documentCode=90ef402d65392bc5
If you use a certificate from the listed certificate authority, no additional TLS configuration is required on Yealink devices.

If your TLS certificate is not supported by Yealink, you need to install the corresponding root certificate on each SIP phone, see *6.6 Install TLS root certificate on Certified SIP phones*, Page 77

3) Configure SwyxRemoteConnector only

If you want to continue using the SelfSigned certificate, or if you already have a TLS certificate installed, you can also use SCST to set only the RemoteConnector parameters.

See *6.3 RemoteConnector Configuring*, Page 74

6.1 USE TLS CERTIFICATE FROM LET'S ENCRYPT

If your SwyxWare is licensed online, you have the possibility to get a unique server name (FQDN) from the SwyxON DNS service. SCST requests for this FQDN a TLS server certificate from the Let's Encrypt service and installs it in SwyxWare.

See also Let's Encrypt/how-it-works

SCST handles the communication to the SwyxON DNS service and Let's Encrypt service and completes the certification in a few steps.

The TLS certificate is automatically updated by SCST before the expiration date. For this purpose, a scheduled process is registered in Windows that regularly checks in the background whether the TLS certificate is about to expire.

FQDN validation

In order for SCST to request the TLS certificate from Let's Encrypt and update it regularly, the following requirements must be met:

- The SwyxServer machine must have a working DNS configuration, i.e. DNS queries for the FQDN and all its domains must succeed. If the DNS configured in Windows does not work, SCST tries to reach the following DNS servers: 8.8.8.8, 1.1.1.1, 8.8.4.4.
- The SwyxServer machine and your local network must allow outgoing connections via HTTPS. Connections to Let's Encrypt, registration with SwyxON DNS and Swyx online licensing each require the HTTPS protocol.

To use a TLS certificate from Let's Encrypt

1 Start Swyx Connectivity Setup Tool under "Start | Programs | SwyxWare | Swyx Connectivity Setup Tool".

2 Click on NEXT.
✓ The following page appears Server name.

3 Select the option Get name from SwyxON DNS to request a FQDN for the public IP address.

4 Click on NEXT.
✓ The following page appears Get name from SwyxON DNS.

5 If necessary, enter the public IP address of your network if SwyxWare has a static public IP address and you do not want to use automatic detection.

6 Click on Request.
✓ At Provided FQDN appears the randomly generated FQDN and the detected public IP address.

Be sure to use the corresponding data in the Split DNS configuration.

7 Click on NEXT.
✓ The following page appears Automatic certificate mode.

Name	Explanation
E-mail address	Enter an email address to receive notifications from Let's Encrypt.
Request and Install	Click the button to request a TLS certificate from Let's Encrypt. If the request was successful, the certificate information will appear, see the next table.

8 Click on "Request and Install".
The request may take a few minutes.
✓ The TLS certificate is being installed.
✓ The certified SIP phones will be provisioned again.

The following information will then appear:

Name	Explanation
Certificate	Name Certificate name is defined by Let's Encrypt and usually contains the FQDN and the creation date for information. Expiration date The date on which the validity of the certificate expires. The new certificate will be updated automatically by Let's Encrypt, you will receive a notification by e-mail.
Certificate installation state	Installed Status of the certificate installation in the SwyxWare services.

9 Click on NEXT.
✓ The following page appears RemoteConnector access.

Name	Explanation
Enable Remote access	Enable this option if client connections via Internet to SwyxServer should be allowed.
Authentication server (FQDN)	The public endpoint (as FQDN) of the company network, via which the authentication service can be reached, is assigned automatically. The default port for the authentication service is 9101. If you use a different standard port and not 9101, it has to be explicitly stated in the Client settings.
RemoteConnector server (FQDN)	The public endpoint (as FQDN) of the company network, via which the RemoteConnector can be reached, is automatically assigned. The default port for the RemoteConnector is 16203.

10 Click on NEXT.

✓ The following page appears **RemoteConnector certificate**.

Name	Explanation
Automatic password management	Enable this option if you want the root certificate password to be generated automatically.
Generate client certificates	Enable this option if you want a RemoteConnector client certificate to be automatically generated for each user.
Manual password management	Enable this option if you want to assign the password for the root certificate yourself. In this case SwyxWare cannot automatically generate client certificates. You must do this for each user individually, entering the password assigned here in each case, see *11.2.1.3 The "RemoteConnector" Tab*, Page 168
Password Authentication	Enter a password if necessary.
Generate certificates	Click the button to have the root and server certificates generated. The corresponding certificate thumbprints then appear.

11 Click on NEXT.

✓ The following page appears **Summary** with the overview of your configuration.

Name	Explanation
Server configuration	**Public IP address** This IP address has been determined by the SwyxON DNS service as the public IP address of your network. **Server name** This FQDN was randomly generated by the SwyxON DNS service and assigned to the public IP address. Clients must use this server name to communicate with the SwyxServer.
TLS configuration	**TLS certificate mode** Automatic: TLS certificate is provided by Let's Encrypt. **TLS certificate valid until** The date on which the validity of the certificate expires. The certificate is automatically updated by SCST. You will receive a notification from Let's Encrypt via email. **TLS certificate name** Certificate name is defined by Let's Encrypt and usually contains the FQDN and the creation date for information.
Certificate installation state	**Installed** Status of the certificate installation in the SwyxWare services.

Name	Explanation
RemoteConnector configuration	RemoteConnector access Enabled: Client connection via Internet to SwyxServer is allowed. Autom. password management Enabled: The password for the RemoteConnector root certificate was automatically generated and is used by SwyxWare. or Manual password management Enabled: The password for the RemoteConnector root certificate has been set by the administrator and must be entered each time when generating a RemoteConnector client certificate. Generate client certificates Enabled: Client certificates for all users are generated automatically. or Deactivated: The administrator must have a client certificate generated for each desired user.

12 Click on EXIT to close SCST.

> If necessary, resend a welcome email to the corresponding SwyxWare users with the new RemoteConnector credentials.

6.2 USE OWN TLS CERTIFICATE

You can also install an existing TLS certificate. In this case you must generate a TLS certificate yourself or purchase it from a certificate authority.

How to install an existing TLS certificate

You have placed the corresponding .pfx file, which contains the server certificate and the private key, in a directory on the SwyxServer machine.

1 Start Swyx Connectivity Setup Tool under "Start | Programs | SwyxWare | Swyx Connectivity Setup Tool".

2 Click on NEXT.
✓ The following page appears Server name.

3 Select the option Use your own Fully Qualified Domain Name (FQDN).

4 Click on NEXT.
✓ The following page appears Use your own FQDN.

5 Enter the registered FQDN of your network.

6 Click on Test to verify that the FQDN resolves to the correct IP address.

> If a Split DNS is configured in the network, the FQDN is resolved to the local IP address of the SwyxServer via the DNS service.

Name	Explanation
Test result	FQDN FQDN of your network. Resolved IP Address The public IP address associated with the FQDN.

7 Click on NEXT.
✓ The following page appears Manual certificate mode.

8 Click on NEXT.

9 Select the prepared .pfx file from the appropriate directory.

10 Enter the password with which the certificate was protected and click on OK.
✓ The following information will appear:

Name	Explanation
Certificate	**Name** Certificate name as defined when the certificate was generated. **Expiration date** The date until which the certificate is still valid. You must re-run SCST and install a new certificate before expiration.

11 Click on Install.
The request may take a few minutes.
- ✓ The TLS certificate is being installed.
- ✓ The certified SIP phones will be provisioned again.
- ✓ The following information will then appear:

Name	Explanation
Certificate installation state	**Installed** The certificate is installed for the listed services.

12 Click on NEXT.
- ✓ The following page appears RemoteConnector access.

Name	Explanation
Enable Remote access	Enable this option if client connections via Internet to SwyxServer should be allowed.
Authentication server (FQDN)	The public endpoint (as FQDN) of the company network, via which the authentication service can be reached, is assigned automatically. The default port for the authentication service is 9101. If you use a different standard port and not 9101, it has to be explicitly stated in the Client settings.
RemoteConnector server (FQDN)	The public endpoint (as FQDN) of the company network, via which the RemoteConnector can be reached, is assigned automatically. The default port for the RemoteConnector is 16203.

13 Click on NEXT.
- ✓ The page RemoteConnector certificate.

Name	Explanation
Automatic password management	Enable this option if you want the root certificate password to be generated automatically.
Generate client certificates	Enable this option if you want a RemoteConnector client certificate to be automatically generated for each user.
Manual password management	Enable this option if you want to assign the password for the root certificate yourself. In this case SwyxWare cannot automatically generate client certificates. You must do this for each user individually, entering the password assigned here in each case, see *11.2.1.3 The "RemoteConnector" Tab*, Page 168
Password Authentication	Enter a password if necessary.
Generate certificates	Click the button to have the root and server certificates generated. The corresponding certificate thumbprints then appear.

14 Click on NEXT.
- ✓ The page Summary with the overview of your configuration.

Name	Explanation
Server configuration	**Public IP address** The public IP address of your network. **Server name** The registered FQDN of your network.
TLS configuration	**TLS certificate mode** Manual: You use your own certificate. **TLS certificate valid until** The date on which the validity of the certificate expires. You must update the certificate before the expiration date. **TLS certificate name** Certificate designation, consisting among other things of the FQDN to which the certificate is assigned.

Name	Explanation
Certificate installation state	Installed The certificate is installed for the listed services.
RemoteConnector configuration	RemoteConnector access Enabled: Client connection via Internet to SwyxServer is allowed. Autom. password management Enabled: The password for the RemoteConnector root certificate was automatically generated and is used by SwyxWare. or Manual password management Enabled: The password for the RemoteConnector root certificate has been set by the administrator and must be entered each time when generating a RemoteConnector client certificate. Generate client certificates Enabled: Client certificates for all users are generated automatically. or Deactivated: The administrator must have a client certificate generated for each desired user.

15 Click on EXIT to close SCST.

If necessary, resend a welcome email to the corresponding SwyxWare users with the new RemoteConnector credentials.

6.3 REMOTECONNECTOR CONFIGURING

The public endpoints must be entered in the connection settings of the client, see help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/specify_connection_settings_$

You can set or adjust the following parameters:

- The public address for the authentication service (only for a Self-Signed certificate) and the port,
- the public address and port for the RemoteConnector,
- Generating of RemoteConnector root and server certificates
- Generating and assignment of client certificates to users,
- Password management when creating RemoteConnector client certificates.

To configure the RemoteConnector

1 Start Swyx Connectivity Setup Tool under "Start | Programs | SwyxWare | Swyx Connectivity Setup Tool".

2 Click on Configure only RemoteConnector.
✓ The following page appears RemoteConnector access.

Name	Explanation
Enable Remote access	Enable this option if client connections via Internet to SwyxServer should be allowed.
Authentication server (FQDN)	Enter the public endpoint (as FQDN or IP address) of the corporate network through which the authentication service can be reached. The default port for the authentication service is 9101. (If you have a TLS certificate installed, this address is fixed). If you use a different standard port and not 9101, it has to be explicitly stated in the Client settings.
RemoteConnector server (FQDN)	Enter the public endpoint (as FQDN or IP address) of the company network through which the RemoteConnector can be reached. (If you have installed a TLS certificate, this address is fixed). The default port for the RemoteConnector is 16203.

3 Click on NEXT.
✓ The following page appears RemoteConnector certificate.

Name	Explanation
Automatic password management	Enable this option if you want the root certificate password to be generated automatically.
Generate client certificates	Enable this option if you want a RemoteConnector client certificate to be automatically generated for each user.

Name	Explanation
Manual password management	Enable this option if you want to assign the password for the root certificate yourself. In this case SwyxWare cannot automatically generate client certificates. You must do this for each user individually, entering the password assigned here in each case, see *11.2.1.3 The "RemoteConnector" Tab*, Page 168
Password Authentication	Enter a password if necessary.
Generate certificates	Click the button to have the root and server certificates generated. The corresponding certificate thumbprints then appear.

4 Click on NEXT.

✓ The page **Summary** appeares with the overview of your configuration.

Table 1 (A TLS certificate from Let's Encrypt or your own is already installed)

Name	Explanation
Server configuration	**Public IP address** The public IP address of your network. **Server name** The registered FQDN of your network.
TLS configuration	**TLS certificate mode** Manual: You use your own certificate. or Automatic: TLS certificate was obtained from Let's Encrypt. **TLS certificate valid until** The date on which the validity of the certificate expires. You must update the certificate before the expiration date. **TLS certificate name** Certificate designation, consisting among other things of the FQDN to which the certificate is assigned.
Certificate installation state	**Installed** The certificate is installed for the listed services.
RemoteConnector configuration	**RemoteConnector access** Enabled: Client connection via Internet to SwyxServer is allowed. **Autom. password management** Enabled: The password for the RemoteConnector root certificate was automatically generated and is used by SwyxWare. or **Manual password management** Enabled: The password for the RemoteConnector root certificate has been set by the administrator and must be entered each time when generating a RemoteConnector client certificate. **Generate client certificates** Enabled: Client certificates for all users are generated automatically. or Deactivated: The administrator must have a client certificate generated for each desired user.

Table 2 (A SelfSigned certificate is used)

Name	Explanation
TLS certificate mode	Type of TLS certificate used: **SelfSigned** A TLS certificate automatically generated by SwyxWare is used.
RemoteConnector access	Allow client connections via Internet to SwyxServer: **Enabled/Disabled**
Autom. password management or Manual password management	**Enabled:** The password for creating client certificates is generated automatically. or must be entered manually by the administrator.

Name	Explanation
Generate client certificates	Generate client certificates for users automatically: Enabled: Client certificates for all users are generated automatically. or Deactivated: The administrator must have a client certificate generated for each desired user.

5 Click on EXIT to close SCST.

ⓘ If necessary, resend a welcome email to the corresponding users with the new RemoteConnector credentials.

6.4 RESET SCST CONFIGURATION

For example, if you need to reset the settings specified by SCST for technical reasons, you can run the following command in the command line interface as an administrator:

```
scst.cli.exe reset
```

- All TLS certificates installed by SCST are removed,
- certified SIP phones are re-provisioned and reset to HTTP protocol,
- the scheduled tasks created by SCST which update the Let's Encrypt certificate and SwyxON FQDN registration are removed.

Afterwards you can also remove the FQDN registered in SwyxON DNS with the following command:

```
scst.cli.exe unregister
```

ⓘ If you do not execute the unregister command, the FQDN remains registered in SwyxON DNS for some time. However, the DNS record is no longer updated when the public IP address changes. Therefore, you should stop using the FQDN in any case.

6.5 INSTALL TLS ROOT CERTIFICATE ON DECT 800 BASE STATION

For a secure provisioning of SwyxDECT 800 end devices you have to install your own TLS root certificate or the TLS root certificate of Let's Encrypt yourself:

To install the root certificate during a new provisioning

You have installed your own TLS server certificate or a TLS server certificate from Let's Encrypt via SCST.

1 Have your own root certificate ready,

Or

1 download a root certificate from Let's Encrypt (ISRG Root X1): letsencrypt.org/certificates/

2 Go through the steps for provisioning the DECT end devices (as described in the chapter help.enreach.com/controlcenter/latest.version/web/Swyx/en-EN/index.html#context/help/DECT800_provisioning_$).
In step 6, you must upload the corresponding root certificate, see help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/index.html#context/help/TLS_Rootcertificate_$

⚠ If you use your own certificate, make sure that you upload a valid trusted root certificate.

✓ The DECT 800 base station uses HTTPS provisioning to connect to SwyxWare.

To install the root certificate on already provisioned devices

1 Have your own root certificate ready,

Or

1 download the root certificate from Let's Encrypt (ISRG Root X1): https://letsencrypt.org/certificates/

2 Update SwyxWare .
3 Open the configuration wizard of the base station on the web interface.
4 Upload the root certificate at **General | Certificates |Trust List | Upload** upload.

> If you use your own certificate, make sure that you upload a valid trusted root certificate.

5 Perform the configuration in SCST to install the TLS server certificate.
6 Click on **Finish**.
✓ The base station is restarted The DECT 800 base station uses HTTPS provisioning to connect to SwyxWare. DECT 800 telephones are provisioned again.

6.6 INSTALL TLS ROOT CERTIFICATE ON CERTIFIED SIP PHONES

If your TLS certificate is not supported by Yealink, you need to install the corresponding root certificate on each SIP phone, see

You can distribute the root certificate in the provisioning network, see help.enreach.com/controlcenter/latest.version/web/Swyx/en-EN/index.html#context/help/provisioning_network_$

> The exact parameters you need to use for provisioning your own root certificate can be found in the common.cfg file in the provisioning template for your Yealink phone type.

or

You can upload the root certificate manually on the Yealink web interface.

Yealink models	Menu path
T4x	**Trusted Certificates** | Tab **Custom CA | Import Trusted Certificates**
T5x	**Trusted Certificates** | Tab **Custom CA | Import Trusted Certificates**

> If the provisioning of phones cannot be performed via multicast due to the network infrastructure, you can also distribute the provisioning URL (e.g. https://172.20.1.1:9200/ippbx/client/v1.0/device/provision/) via DHCP option 66.
> In this case, your DHCP server must support HTTPS protocol.

To install the root certificate during a new provisioning

You have installed your own TLS server certificate or a TLS server certificate from Let's Encrypt via SCST.

1 Distribute the root certificate in the provisioning network or upload the root certificate on each corresponding SIP phone.

> If you use your own certificate, make sure that you upload a valid trusted root certificate.

2 Connect the corresponding SIP phones to the productive network.
✓ The SIP phones are being provisioned.

To install the root certificate on already provisioned devices

1 Set up a provisional provisioning network to distribute your own TLS root certificate to all your certified SIP phones, see help.enreach.com/controlcenter/latest.version/web/Swyx/en-EN/index.html#context/help/provisioning_network_$

If you use your own certificate, make sure that you upload a valid trusted root certificate.

2 Connect the corresponding SIP phones to the productive network.

3 Update SwyxWare .

4 Perform the configuration in SCST to install the TLS server certificate, see *6.2 Use own TLS certificate*, Page 72
✓ The SIP phones will be provisioned again.

6.7 CONFIGURE SPLIT DNS

The following describes a DNS configuration using Windows Server 2019 as an example.

If not already present, install the DNS service.

Then you can create a new DNS zone with a corresponding host entry: FQDN > Internal IP address of the SwyxServer.

The DNS zone name must match the FQDN specified in the TLS certificate.

To install the DNS Manager, if necessary

1 Open the Server Manager.

2 Select in the menu Manage | Add Roles and Features.

3 In the step Installation Type select Role-based or feature-based installation and click Next.

4 Select the desired destination server and click on Next.

5 As Server Role select DNS Server and click on Next.

6 Click Add Features.

7 Confirm the further steps of the installation with Next (Continue) and Install.

8 Click Close.

To create a new DNS zone

1 Open the DNS manager: Win+R | dnsmgmt.msc

2 In the server list, select the desired server.

3 In the context menu of Forward Lookup Zone select New Zone...

4 Click Next, Primary Zone, Next.

5 Enter the name of the zone.

Z. E.g. my.fqdn_name.net

6 Click Next.

7 Keep the standard parameters and click Next.

8 Click on Finish.

To create a host entry

1 In the context menu of the DNS zone select New Host (A or AAA...).

2 Enter under IP address enter the internal IP address of the SwyxServer.

3 Click Add Host.
✓ The new entry was added. You can test your configuration.

To test your DNS configuration

1 Open the command line on a client computer in the local network.

2 Enter the command "nslookup <FQDN of your network>":

E.g.: nslookup my fqdn_name.net

✓ The internal IP address of the SwyxServer is displayed.

6.8 ACCESS VISUALGROUPS AND VISUALCONTACTS ON A SEPARATE SERVER VIA REMOTECONNECTOR

You have Swyx VisualGroups or Swyx VisualContacts **not** installed on SwyxServer and would like to access the services via RemoteConnector.

- For SwyxWare versions prior to 13.30, the configuration is done via registry key. This is described here: https://service.swyx.net/hc/en-gb/articles/360017729619-Access-VisualGroups-and-VisualContacts-which-are-installed-on-a-seperate-server-via-Remote-Connector
- For SwyxWare versions from 13.30, the configuration is carried out via a configuration file. This is described below.

To add a RemoteConnector access via configuration file

1 Open the SwyxWare Administration.

2 Choose your Server and click on Properties....

3 Select Files | Edit....

4 Click on the column heading Category column heading to switch the sorting.

5 Under the category RemoteConnector configuration file category, select the file CPE_ippbx_cpe_rcconfig file.

6 Select Save as... | [Select save path] | Save.

7 Open the file (with Notepad++) and navigate to the section VisualContacts or VisualGroups.

8 In the desired area, enter the following in the line DestinationSocket(...) for 0.0.0.0 enter the desired destination address.

Example:
You want to access VisualGroups via RemoteConnector using your server with the address 255.12.345.6.

```
<!-- VisualGroups -->
</TCPConfig>
  <ClientOS>Windows</ClientOS>
  <ClientListenSocket>0.0.0.0:9980</ClientListenSocket>
  <DestinationSocket>255.12.345.6:80</DestinationSocket>
</TCPConfig>
```

9 Save the file.

10 Upload the file in the Files window, see step (3): Add... | [...] | [Select file].

11 Choose from Category: RemoteConnector configuration file and confirm with OK.

✓ The new configuration file is uploaded and used.

> The previous system default file cannot be removed. The newly uploaded file is used because the Global area has a higher priority than System Default.

7 CONFIGURATION OF SWYXSERVER

Administration of SwyxServer, Configuration of server properties

The SwyxWare Administration is a so-called Snap In module for the Microsoft Management Console (MMC). Therefore, you can use the same user interface which you are already familiar with from most of the management tools found in Windows Systems, without having to become acquainted with a new user interface. Please consult the appropriate Windows Online Help for information on using the MMC.

With the help of SwyxWare Administration, you can, for example,

- define global SwyxServer settings, see *7.5 Configuring SwyxServer settings*, Page 86
- Configure users, see *11 User Configuration*, Page 160,
- configure a fax connection, see *11.7 Export User List*, Page 212,
- Create and modify groups, see *12 Configuration of Groups*, Page 215,
- Define secretariat relationships between users, see *12.3 Secretariate*, Page 224,
- Map internal to external numbers, see *7.5.4 The "Internal Numbers" Tab*, Page 91
- Define locations and thus prefixes and time zones, and assign these to users or trunk groups, see *8 Locations*, Page 122
- Set up routings to determine the connections individual calls can be routed by, see *14 Routing*, Page 239,
- Define profiles, which define calling rights, determine the usage of certain components and assign administration rights, see *9 Profiles*, Page 128
- Display a log of parameter changes for SwyxServer, see *7.7 Change log*, Page 117,
- manage the Global Phonebook, see *7.6 Global Phonebook*, Page 114,
- Add or remove trunks and trunk groups, see *Setting up trunks and trunk groups*, Page 227 and
- Obtain information concerning individual connections, see *7.8 Active Calls*, Page 119.

7.1 REGISTRATION ON SWYXWARE ADMINISTRATION

For information on installing the SwyxWare Administration, please see *5.5 Installation of the SwyxWare Administration*, Page 64. You can additionally install the SwyxWare Administration on further computers on the network and administer SwyxWare remotely, see *5.7 Separated Services*, Page 66.

Complex passwords

Limited number of log-in attempts

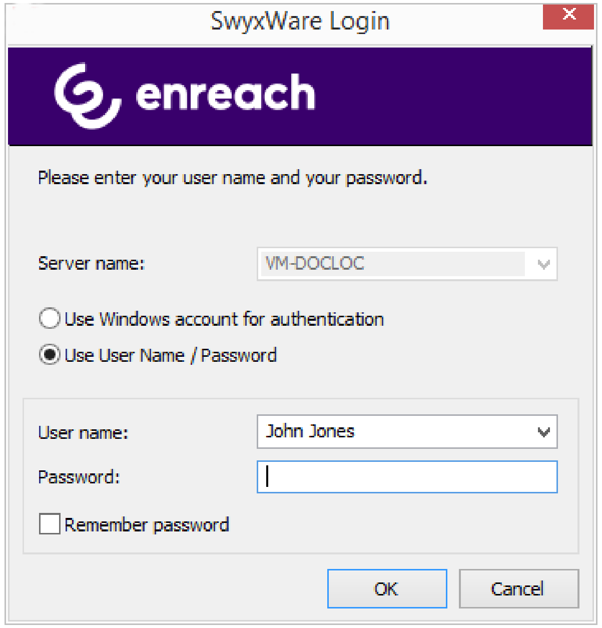
When saving and processing personal data, observe the respective applicable legal data protection regulations.

Personal data cannot be deleted automatically. In order to meet the valid data protection regulations, it may be necessary to delete the entries manually.

Note that you also need the corresponding rights for the administration of SwyxWare. See *9.3 Administration profiles*, Page 143.

How to log in SwyxWare Administration to

1 Double-click on the appropriate symbol on the Windows Desktop or select the Start Menu entry.
The "SwyxWare Login" window will appear.



Please enter your user name and your password.

Server name: VM-DOCLOC

○ Use Windows account for authentication

● Use User Name / Password

User name: John Jones

Password:

□ Remember password

2 You can choose between

- Login with Windows account (In SwyxWare for DataCenter and SwyxON not possible)
  You authenticate yourself with the Windows user account with which you have just logged in.
- Login with User Name / Password
  You can also log in with a SwyxWare user name and a password. The access information can be stored on the computer currently being used in the user profile of the Windows user logged in. This information will then no longer be queried in further logins.
- Login with authentication token (**only in** SwyxON)
  Administrators at the platform and partner level can log on to SwyxWare Administrationa UC Tenant via an authentication token for a limited time

7.1.1 COMPLEX PASSWORDS

If a complex password has been forced as a rule in server and/or user configuration, then you'll have to set up a complex password for every password change.

If the "Force complex user password" option is enabled for the user, the last passwords of the user will be taken into account during the change. The user cannot reuse the last three passwords.

Regardless of the password settings, an attempt to re-enter the current password during password change will be checked by the system and will not be permitted.

In SwyxON, the policy for complex passwords is enforced by default and cannot be overridden by any administrator.

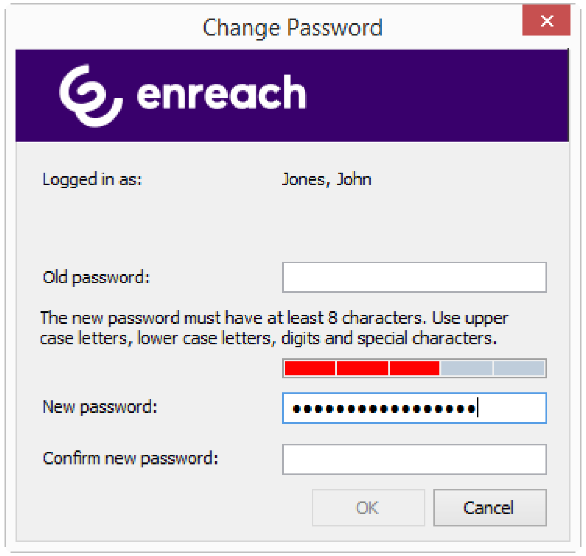
Complex passwords for SwyxServer must at least meet the following requirements:

- The passwords consists at least of eight characters.
- The password consists of any characters meeting at least the four following character categories:
  - upper-case letters such as: [A-Z]
  - lower-case letters such as: [a-z]
  - Numbers [0-9]
  - Non-alphanumeric characters (special characters), such as: Dot, comma, brackets, space, double cross (#), question mark (?), percent sign (%), ampersand (&).

Alphabetic characters (such as: ß, ü, ä, è, ô) and non-Latin characters (such as: φ, π, β) are no special characters and are regarded as letters.

See also *7.5.18 The "Security" tab*, Page 109.

The log-in dialog shows the password status bar while setting a new password, which indicates whether it meets requirements and will be accepted.


Change Password

Logged in as: Jones, John

Old password:

The new password must have at least 8 characters. Use upper case letters, lower case letters, digits and special characters.

New password: ••••••••••••••••

Confirm new password:

Password status bar

The bar consists of five sections. Each section verifies, if the following password requirements have been met:

- At least eight characters
- At least one upper-case letter
- At least one lower-case letter
- At least one digit
- At least one special character

The bar gets longer, the more password requirements have been met.

The color of the bar changes accordingly. It also indicates, if the password is being accepted by the system.

Password status bar	Password requirements	Accepted
🟥🟥🟥⬜⬜	3 password requirements fulfilled	Password not accepted
🟨🟨🟨🟨⬜	4 password requirements fulfilled	Password accepted
🟩🟩🟩🟩🟩	5 password requirements fulfilled.	Password accepted.

Enter your new password in the field "New Password". If the minimum requirements are met, you can repeat your entry in the field "Retype Password".

> ⚠ It is impossible to use the previous password again.

Once you are logged in, you can also change your complex password yourself at any time if you possess the requisite rights for doing so. See *11.2.1.2 The "Authentication" Tab*, Page 165.

7.1.2 LIMITED NUMBER OF LOG-IN ATTEMPTS

The number of attempts to log in to SwyxWare Administration may be limited.

If the maximum number of failed login attempts is reached, the following error message appears: "The user account is locked. Please contact your administrator".

You will be unable to use SwyxWare with a client or another terminal device until the administrator has reactivated your account.

> ⚠ The system administrator account will not be locked.

The number of failed log-in attempts will be reset after a successful login.

The number of failed log-on attempts is irrelevant, when the administrator has established a forced password change, and the user attempts to log-on with his/her previous password.

7.2 CONNECTION TO SWYXSERVER

After starting SwyxWare Administration for the first time, the wizard for setting up a connection to a SwyxServer automatically opens. Create a connection to the SwyxWare set up during the SwyxServer installation by proceeding as described below.

The Windows user accounts that can log in with this user name (and the password belonging to this user name) are specified in the User Properties see *11.2.1.2 The "Authentication" Tab*, Page 165. This is the same login data that also uses for logging on.

How to connect to a SwyxServer

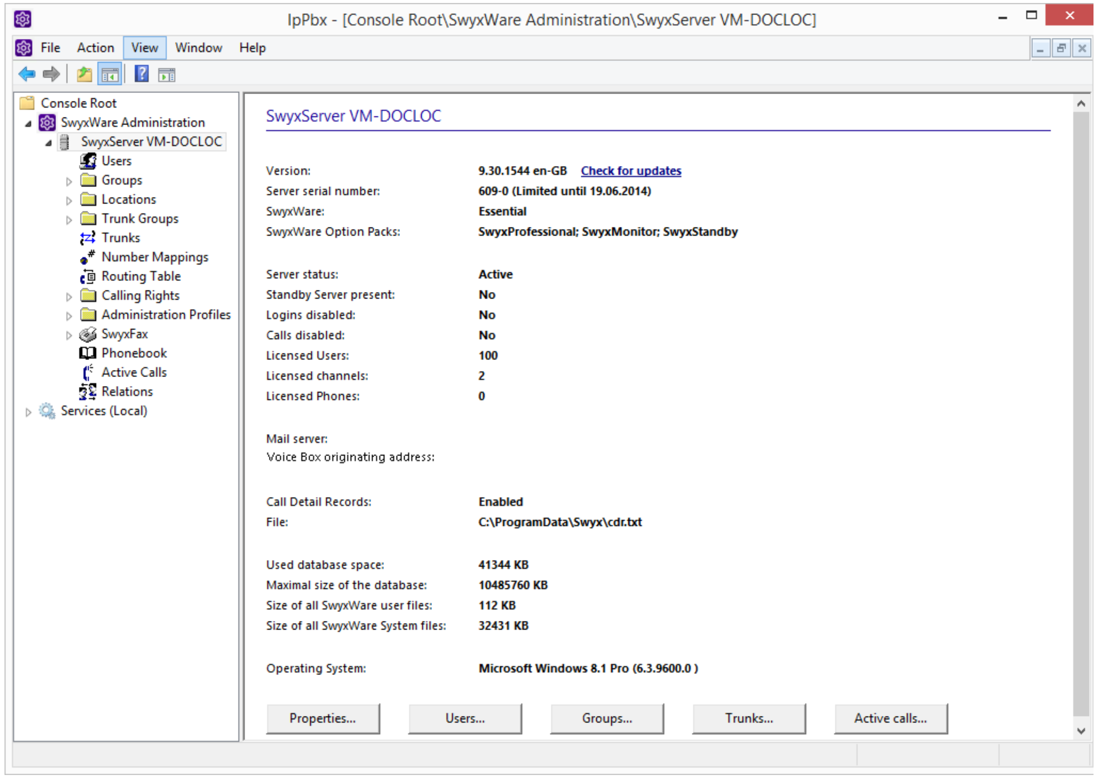
1. Click the "SwyxWare Administration" entry with the right mouse button to open the context menu.
2. Choose "Connect to a SwyxServer...".
3. Indicate whether you would like to connect with SwyxServer on the local computer or with SwyxServer in the network. Select a remote SwyxServer from the drop-down list.
4. After making your selection, click on "Finish".
   The connection to the selected server will now be established. If the connection to a SwyxServer was successful, a corresponding entry will be created for this server.
   The "SwyxWare Login" window will appear.
5. Follow the steps in section *7.1 Registration on SwyxWare Administration*, Page 80

If you do not have permanent licenses yet, you will be reminded of this here. To make the temporary licenses permanent, see *7.5.5 The "Licenses" Tab*, Page 91.

Dependent on administrator rights, you will see the current base settings for this server in the detail pane (*9.3 Administration profiles*, Page 143). The complete view, which is visible to a system administrator, is dealt with below. If individual areas of the administration cannot be accessed or if error messages occur during configuration, please contact your administrator.

7.3 USER INTERFACE OF SWYXWARE ADMINISTRATION

As system administrator or backoffice administrator, you can simplify the view of the administration by selecting "View | Standard" in the menu bar. The feature profiles and the change log are then hidden.



SwyxServer VM-DOCLOC

Version:	9.30.1544 en-GB Check for updates
Server serial number:	609-0 (Limited until 19.06.2014)
SwyxWare:	Essential
SwyxWare Option Packs:	SwyxProfessional; SwyxMonitor; SwyxStandby
Server status:	Active
Standby Server present:	No
Logins disabled:	No
Calls disabled:	No
Licensed Users:	100
Licensed channels:	2
Licensed Phones:	0
Mail server:	
Voice Box originating address:	
Call Detail Records:	Enabled
File:	C:\ProgramData\Swyx\cdr.txt
Used database space:	41344 KB
Maximal size of the database:	10485760 KB
Size of all SwyxWare user files:	112 KB
Size of all SwyxWare System files:	32431 KB
Operating System:	Microsoft Windows 8.1 Pro (6.3.9600.0)

On the right side of the administration window you'll find detailed information on SwyxWare installation:

- Software version (Click on the link "Check for updates" for information on update options.)
- Serial number
- SwyxWare Variants
- SwyxWare Option Packs
- Server status, number of users and channels
- Reseller information (only SwyxON)
- Logged on administrator (only SwyxON)
- Session expiry (only SwyxON)
- Configured mail server
- Memory location of Call Detail Records
- Memory space in the database, and the memory space already being used for users and system
  Before the files stored in the database reach the maximum size of the database, a corresponding message is output to the Event log.
- Operating System of the Computer

There are several entries under the server entry located on the left side of the SwyxWare Administration window.

The first entry is the "User" folder. If you click on this folder, a tabular list of all configured users will appear in the detail pane.

In this list there is a folder called "Groups" in which you will find all of the groups created on this server.

"Locations" contains the "default location" (created during the installation) and all other locations set up later by the Administrator. You will find in the sub-folders all the users, trunks and trunk groups belonging to this location.

The "Trunk Groups" folder includes a list of all available trunk groups. Their respective sub-folders list all trunks assigned to the respective trunk group.

The "Trunks" folder lists all trunks set up for this server.

The list of mappings between internal and external numbers is displayed under "Number mappings."

The "Routing Table" provides a table view of all routings defined for this server.

"Call Permissions" lists all available profiles which can be assigned to an individual user or a trunk group in relation to call authorization.

"Feature profiles" lists all profiles which allow a user to use the individual functions of SwyxWare. The "Standard" profile is created during installation.

The "Administration profiles" folder shows all profiles which allow a user various levels of administration.

Under "SwyxFax" you will find fax channels, active and stored documents, and an overview of the fax transfers.

In the "Phonebook" folder you will find all entries that have been entered in the Global Phonebook in addition to the users of this SwyxServer.

The "Change log" folder holds information about the changes made in the relevant timeframe to the user configuration, feature profile type or conference rooms.

"Active connections" shows a list of all connections - both internal and external - currently established through this server.

"Relationships" contains an overview of cross-server signaling relationships.

7.3.1 CONTEXT MENU IN THE SWYXWARE ADMINISTRATION

By using the Microsoft Management Console (MMC), you can start some functions directly in the SwyxWare Administration from the tree structure, with the context menu (right mouse button).

Create new elements

New users, groups, rights, profiles, locations, trunks etc. can be created in the context menu. The relevant Configurations Wizard starts up and the necessary parameters are queried.

Change existing elements

If you open the properties of an element in the context menu, you can make changes here. For details please refer to the sections relating to these elements.

Delete elements

In the context menu of individual elements, e.g. a profile, a location or a trunk group, you can delete this element provided it is no longer used.

Export lists

If a list of elements is displayed on the right-hand side, e.g. the list of administration profiles, you can export the list and the associated descriptions to a text file by selecting the menu item "Export list..." in the context menu of e.g. "Administration profiles".

Using Drag & Drop

You can change user properties with Drag & Drop.

Example:

On the right you have the list of users who use the call permission "Internal calls". If you drag a user to the call permission "European destinations", he is now assigned this call permission, and his entry under "Internal calls" disappears.

7.4 PRE-CONFIGURED USERS AND GROUPS

Some groups and users are created during a standard installation of SwyxServer.

The User "Operator"

The script "Operator" is installed for this user. The groups "Sales" and "Support" are installed together with this user. After the installation, a number is not yet assigned to the user "Operator".

See *22.5 Operator (AutoAttendant)*, Page 352.

In order to log in as Operator using SwyxIt! Classic, you must assign a Windows user account or a password to Operator. To do this, open the administration for the user "Operator" in the SwyxWare Administration.

See *11.2.1.2 The "Authentication" Tab*, Page 165.

The first time you log in as Operator using SwyxIt! Classic, the Recording Wizard will start and assist you in recording the necessary announcements. You can start this wizard once again at any time from the menu bar of SwyxIt! Classic (under Settings | Recording Wizard...).

The User "Conference"

This user is necessary for the integrated "Conference" function. It does not represent a single conference room, but is used to manage all conference rooms.

See *11.9.1 Conference Rooms*, Page 213.

The Group "Everyone"

The group "Everyone" includes all users, who are set up on this SwyxServer. Therefore, as members of this group, all users will be assigned the default call handling.

See *22.2 Default call handling*, Page 348.

The Groups "Sales" and "Support"

Both of these groups are created together with the user "Operator". The call handling for the operator forwards both of these groups. After installation, both groups receive the user "Operator" as only member.

See *22.5 Operator (AutoAttendant)*, Page 352.

7.5 CONFIGURING SWYXSERVER SETTINGS

Follow these steps in order to change the settings of a specific SwyxServer.

This is how you configure SwyxServer

1. Start the SwyxWare Administration and log in to the SwyxServer.
2. Click the SwyxServer entry with the right mouse button to open the context menu.
3. Select "Properties".
   You can now configure the global settings of the SwyxServer as described below.

In order to restart SwyxServer or other services after configuration, you can prevent new calls and logins. Current telephone calls can be completed without disturbance.

This is how you configure SwyxFax

1. Start the SwyxWare Administration and log in to the SwyxServer.
2. Click the SwyxFax entry with the right mouse button to open the context menu.
3. Select "Properties".

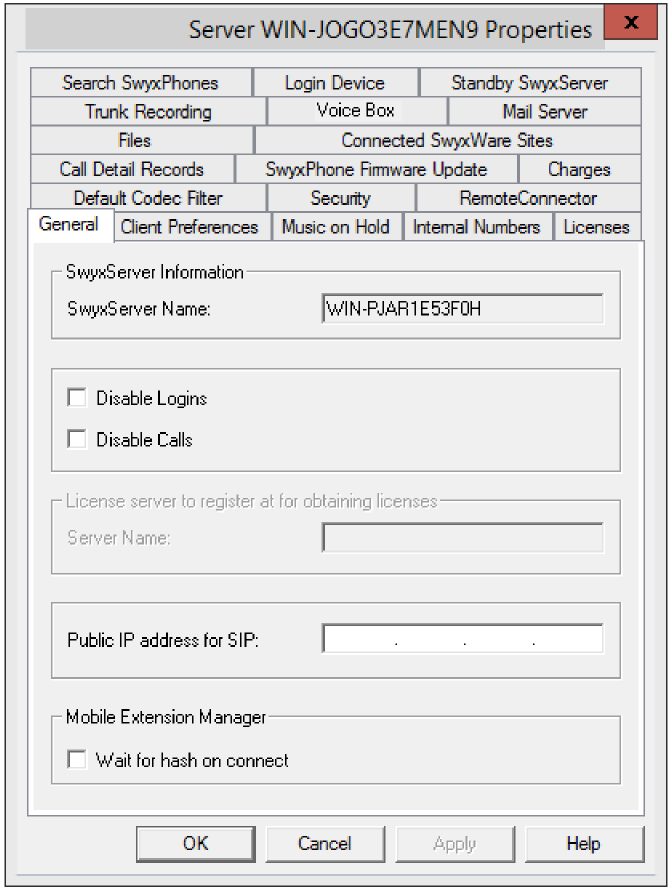
You can now configure the global settings of the SwyxFax Server as described in *24.5 Configuring SwyxFax Server*, Page 362.

How to prevent new logins and new calls

1. Open the context menu for SwyxServer and select "All Tasks | Disable Logins".
   All new logins to SwyxServer will be disabled.
2. Select "All Tasks | Disable Calls" to prevent new calls.
3. Alternatively you can activate the appropriate checkboxes in the SwyxServer properties on the "General" tab.
   The settings are activated as soon as you exit the properties with "OK".

You can now wait until all calls on this SwyxServer have been completed and then restart the computer.

7.5.1 THE "GENERAL" TAB



SwyxServer Information

SwyxServer Name: WIN-PJAR1E53F0H

□ Disable Logins

□ Disable Calls

License server to register at for obtaining licenses

Server Name:

Public IP address for SIP: . . .

Mobile Extension Manager

□ Wait for hash on connect

On this tab you will find general information about this server. You can also disable user logins or prevent new calls, e.g. to stop this server.

Information about SwyxServer

The name of the SwyxServer is shown here. The SwyxServer name cannot be changed later.

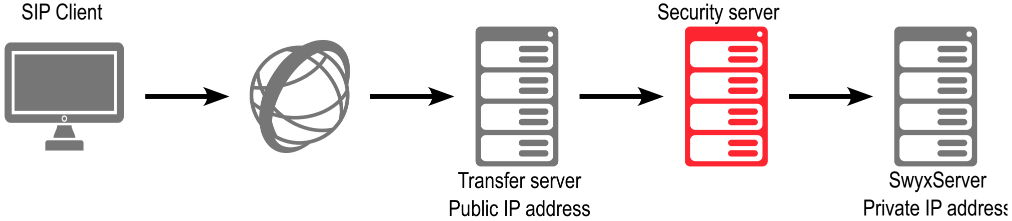
Activate the "Disable login" checkbox if you want to prevent new logins to this SwyxServer. Activate "Disable calls" if you want to prevent new calls being made via this server. These two functions allow you to wait until all calls through this SwyxServer have been completed and then pause the SwyxServer service, e.g. for maintenance purposes.

Licensing server (only for SwyxWare for DataCenter and SwyxON)

The corresponding licenses are entered on one server only, the license server. All other server installations obtain their licensing from this server. In this server installation, enter here the name of the licensing server.

Public IP address for SIP

In a SwyxWare for DataCenter scenario, the SwyxServer (front end server) is installed in the network of a service provider. Such a network is usually protected by a firewall to the Internet. A direct communication from outside into the private network behind the firewall is not permitted; all data traffic goes through a security server. The SwyxServer inside the private network is addressed from outside (Internet) via a transfer server. This transfer server has a public IP address and transfers the communication to the SwyxServer, which only has a private IP address within the network.



SIP clients such as SwyxIt! Classic, wanting to log in as SwyxWare users via the Internet will have to configure the public IP address of the transfer server as the SwyxServer (=SIP registrar/proxy). This transfer server transfers the login and all other CallControl messages to the SwyxServer.

In communication with the SIP clients who connect to the SwyxServer via the Internet, the SwyxServer needs this public IP address in order to specify them as senders. For this reason, the SwyxServer must be informed of the public IP address via which it can be reached from outside.

Enter here the public IP address via which the SwyxServer can be reached, if the SwyxServer is in operation behind a firewall and is to be accessed from outside. Leave the field blank if no public IP address is needed here.

In a standard SwyxWare installation, specifying a public IP address for the transfer server does not work. It will typically have a mixture of internal clients (within the company network) and external clients (on the Internet). In such a case, access to the SwyxServer must be set up via VPN for the external clients.

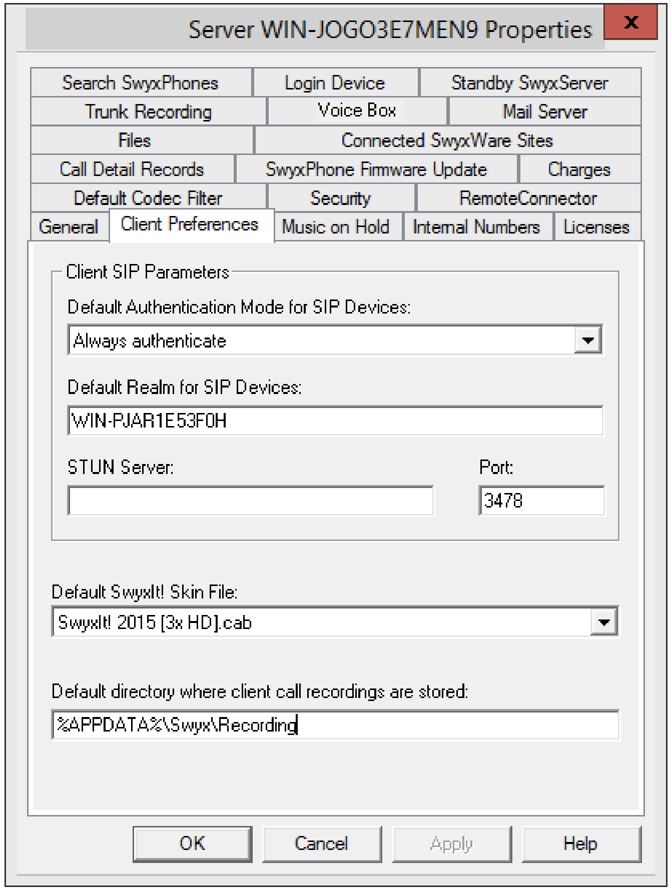
SwyxWare on Systems with Several IP Addresses

In special scenarios it can happen that the computer on which SwyxServer is installed uses several IP addresses.

You can read about this in the knowledge base:

https://service.swyx.net/hc/de

7.5.2 THE "CLIENT PREFERENCES" TAB



Client SIP Parameters

Default Authentication Mode for SIP Devices: Always authenticate

Default Realm for SIP Devices: WIN-PJAR1E53F0H

STUN Server:

Port: 3478

Default SwyxIt! Skin File: SwyxIt! 2015 [3x HD].cab

Default directory where client call recordings are stored: %APPDATA%\Swyx\Recording

General settings can be made on this tab for the telephony clients.

Client-SIP-Parameter

- Standard log-in mode for SIP devices
  Here you can define the standard login mode for all users, i. e. whether or not a SIP terminal device must be authenticated when logging on.

For SIP devices that are already logged in, a change of the login mode only takes effect with the next login.

- Standard log-in mode for SIP devices
  Define the standard realm for all users at this SwyxServer.

If you define the realm as FQDN, please make sure that the DNS name resolution between SwyxServer and the clients is working correctly and without delay. If configured correctly, names and IP addresses can be mutually retrieved with the "nslookup" command.

- STUN server
  Specify the STUN server and the associated port for use by the SIP devices. See *STUN*, Page 279.

Default Skin

Here you specify which skin will be used system-wide by SwyxIt! Classic as default (System Standard Skin).

All users who specified the System Standard Skin as the skin in the user configuration (*11.2.6.7 The "Skin" Tab*, Page 191) will receive this new skin in the next login.

All skin files which are saved in the database for all users are shown in the displayed drop-down list "Default skin (SwyxIt! Classic)".

Standard directory for client recordings

Here you will find the standard directory in which the user's voice recordings should be stored (default setting: %APPDATA%\Swyx\Recording). Dummies can be used here:

- Environment variable %APPDATA%
  %APPDATA% is defined on the client computer and denotes the directory for this user's application data. The following path, e.g., can thus be defined:
  %APPDATA%\Recordings
- SwyxWare User name [username]
  The dummy [username] is replaced by SwyxIt! Classic with the current SwyxWare- user name. The recordings can thus be stored in a directory within the domain, e.g \\fileserver\callrecordings\[username]\.

In the default setting the path is:

%APPDATA%\Swyx\Recording

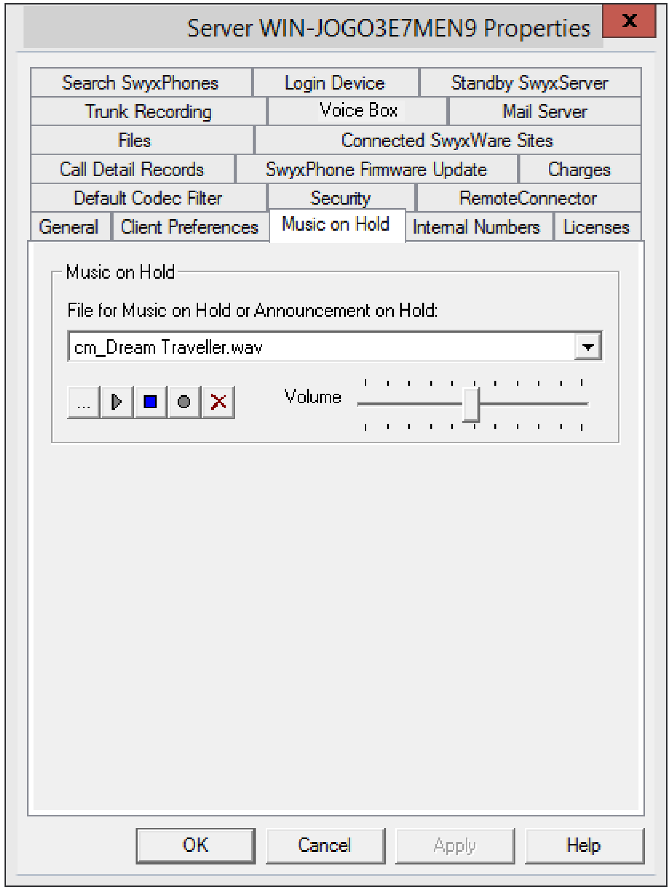
All recordings are then saved locally among the application data of the user account under which SwyxIt! Classic is running. If the user should be able to edit his recordings from other computers as well, please create a share for the user within the network and configure the path for the client recordings accordingly.

Please note that for saving the recordings SwyxIt! Classic uses the Windows user account under which it was started. The login data used by SwyxIt! Classic for logging on to SwyxServer is not taken into account.

If you want to specify a different directory for a single user, then define the directory in user properties (*11.2.6.3 The "Conversation Recording" Tab*, Page 187).

SwyxPhone users can only play back recordings if they log in to SwyxServer with SwyxIt! Classic. See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/recorded_calls_$.

7.5.3 THE "MUSIC ON HOLD" TAB



File for Music on Hold or Announcement on Hold: cm_Dream Traveller.wav

Define the music on hold or the announcement played during on Hold for all users of the SwyxServer. All files that have been stored (globally) in the database as music on hold will appear in the drop-down list. See *7.5.10 The "Files" Tab*, Page 97.

These hold music files all have the "16 kHz 16 Bit PCM mono" audio format. You can switch to another music on hold file by selecting the entry you want. You can search the network for other files in any WAV format using "Browse" (…). After you have chosen a WAV file, it will be converted into the above format and then saved in the database.

The Window functions used for conversion in this procedure may lead to a deterioration in the quality of the music on hold under some circumstances. In this case you should use a professional conversion program instead of the Windows conversion in order to create WAV files in the above mentioned format.

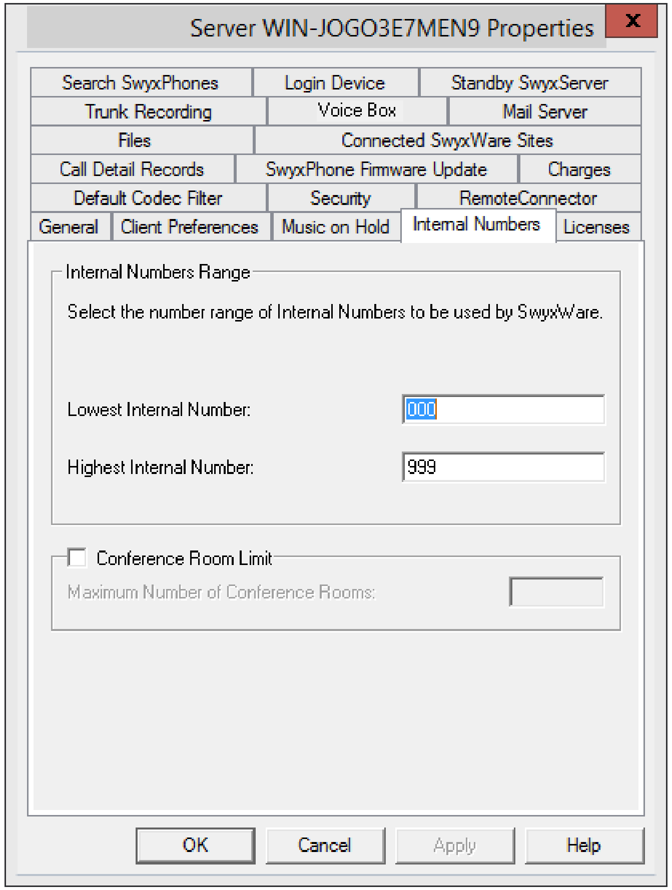
You can play the displayed file and record a new announcement here. The slider is used to adjust the volume of the music on hold.

The newly selected music on hold file will immediately be used for new calls on hold. Calls which were put on hold while the music on hold file was being changed will continue to hear the old music selection.

How to change the hold music

1. The SwyxServer "Properties" page opens.
2. Select the "Music on hold" tab.
3. Select the music on hold you want from the dropdown list or browse for the music on hold.
   If you choose a different music on hold, it will be converted into the format "16 kHz 16 Bit PCM mono" and stored in the database. The attributes of this file will be set, e.g. that the file is globally available, is write-protected etc.. If you want to change the name or description of the file, please open the "Files" tab (*7.5.10 The "Files" Tab*, Page 97).
   Here you can also record an announcement or listen to the selected music on hold.
4. Use the slider to change the volume of the music on hold.
5. Confirm your selection by clicking on "OK".

7.5.4 THE "INTERNAL NUMBERS" TAB



Internal Numbers Range

Select the number range of Internal Numbers to be used by SwyxWare.

Lowest Internal Number: 000

Highest Internal Number: 999

☐ Conference Room Limit

Maximum Number of Conference Rooms:

Internal Numbers Range

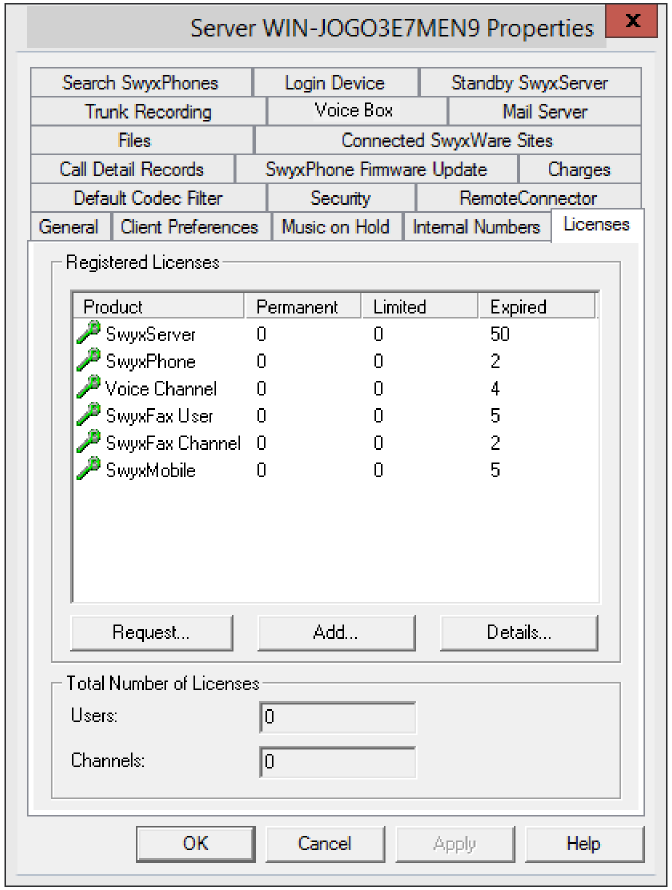
Specify the internal numbers range for this SwyxServer in these two fields. You can choose any range you like. Please enter the same number of digits in both fields, i.e. '000' to '999', not '0' to '999'.

See *10 Numbers and Number Mappings*, Page 146.

Number of conference rooms

This option is only useful in a SwyxWare for DataCenter scenario. The system administrator can limit the number of configurable conference rooms. Activate the option "Conference Room Limit" and enter how many rooms may be created as maximum on this server.

7.5.5 THE "LICENSES" TAB



Registered Licenses

Product	Permanent	Limited	Expired
SwyxServer	0	0	50
SwyxPhone	0	0	2
Voice Channel	0	0	4
SwyxFax User	0	0	5
SwyxFax Channel	0	0	2
SwyxMobile	0	0	5

Total Number of Licenses

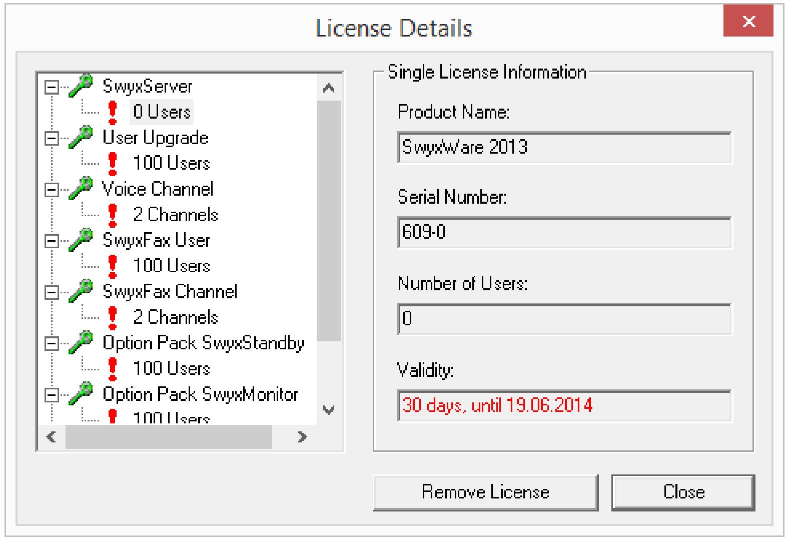
Users: 0

Channels: 0

In a SwyxWare for DataCenter installation, this tab is not visible if the option "Use licensing server" was activated on the "General" tab. If you administer the licensing server yourself, you will find only one license here, see *7.4 Pre-Configured Users and Groups*, Page 85.

In SwyxON your function profiles, conference rooms and fax channels including the maximum number available appear on this tab, see also h ttps ://help.enreach.com/swyxon/1. 00/Partner/Swyx/en-US/index.html#context/help/ordering_contingents_$ and h ttps ://help.enreach.com/swyxon/1.00/Partner/Swyx/en-US/index.html#context/help/ordering_conference_rooms_$.

This tab is used to manage the licenses for your SwyxWare products. For detailed Information related to the different licenses, click on "Details":



- SwyxServer
  - 0 Users
- User Upgrade
  - 100 Users
- Voice Channel
  - 2 Channels
- SwyxFax User
  - 100 Users
- SwyxFax Channel
  - 2 Channels
- Option Pack SwyxStandby
  - 100 Users
- Option Pack SwyxMonitor
  - 100 Users

Product Name: SwyxWare 2013

Serial Number: 609-0

Number of Users: 0

Validity: 30 days, until 19.06.2014

"Create request" will help you request a permanent license key from Enreach. You have the choice of sending the request directly per email or to create a file which will then be sent to Enreach in another manner. In response to this request you will receive a permanent license key as a file, which can be imported with the help of "Add license" in order to validate your license. The entry of the permanent license key always takes place on a file basis. Permanent license keys can be requested using the SwyxWare Administration. In addition to customer data, the hardware information of the computer on which SwyxWare is installed is recorded in the form of checksums. The use of checksums ensures that Enreach does not acquire knowledge concerning your actual hardware information. This data is then sent to Enreach. Based on this data, Enreach derives an *un*limited key for your SwyxWare installation which is then sent to you. The installation of SwyxWare on to another system (e.g. due to a failure of the previously used system) requires that you repeat the registration procedure.

"Add..." can also be used to enter a time-limited key (e.g. when licenses are purchased at a later time).

Please make sure to acquire a sufficient amount of user licenses for an Option Pack. Some Option Packs need the same number of licenses as the installation itself. After the installation of an Option Pack the *minimum* amount of user licenses is available.
If you find that you have too few users after you have installed an option pack, you can remove the license for the option pack. You will then have the original number of users. Please contact your dealer in order to receive an option pack with a sufficient user quantity.

The field "Total Number of Licenses" displays the number of users and channels which are working with SwyxServer at the moment. This number results from the different licenses.

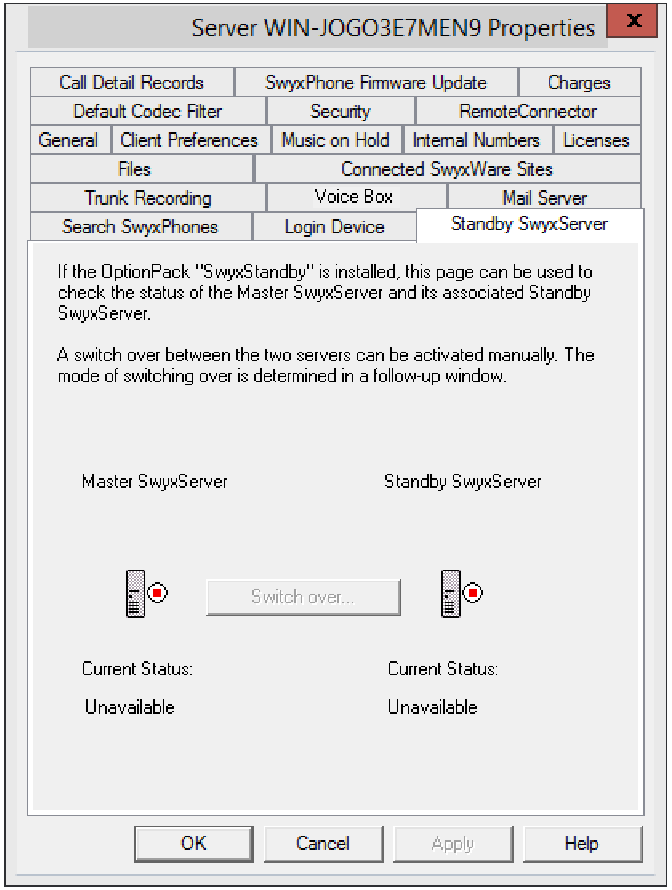
For online licensing information, see *3 Licensing via license key*, Page 28.

and

2 Online Licensing, Page 21

7.5.6 THE "STANDBY SWYXSERVER" TAB

As of SwyxWare 13, the standby functionality is not available.
Enreach will be happy to assist you in selecting a suitable high-availability solution, see *App. L: High Availability Solution for SwyxWare*, Page 457



If the OptionPack "SwyxStandby" is installed, this page can be used to check the status of the Master SwyxServer and its associated Standby SwyxServer.

A switch over between the two servers can be activated manually. The mode of switching over is determined in a follow-up window.

Master SwyxServer

Current Status:

Unavailable

Standby SwyxServer

Current Status:

Unavailable

Here, the Administrator can see which SwyxServer is active (green) and which is passive (red). On the master system you can switch manually between the active and passive system using "Switch over...". Manual switchover is not possible on the standby server.

It is recommended to use SwyxWare Administration to apply any configuration changes always to the active system.

See *23 Standby SwyxServer*, Page 358.

How to change server state manually (active/passive)

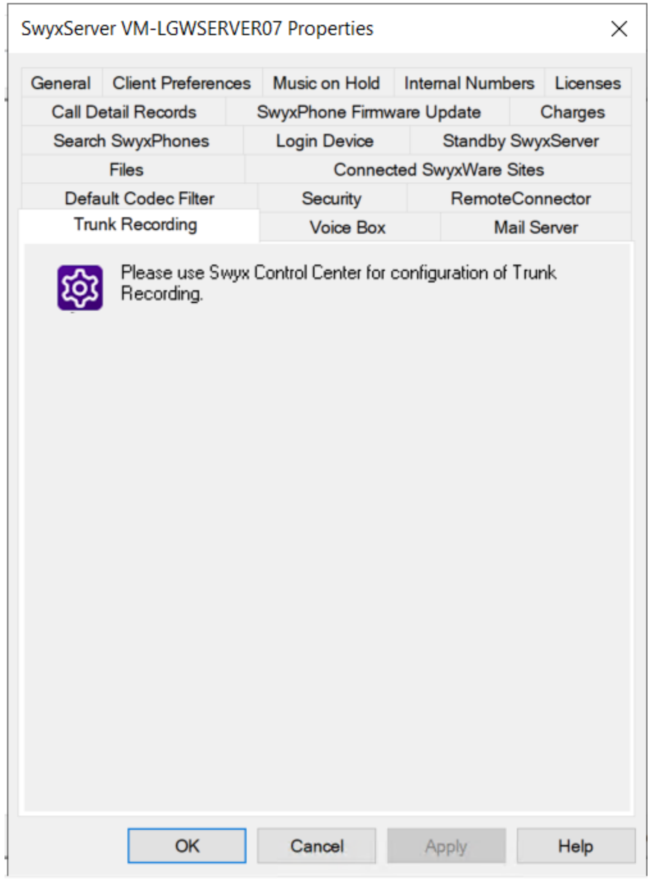
1 Connect to the master system and open the server properties.

2 Click "Switch over... " on the "Standby Server" tab.
A window appears in which you can specify whether you want to switch over immediately or only when no more calls are active.

3 If you click "OK" here, the switch is then made according to the specified procedure.

You can only change the state of the server from the master system, on a standby system a switchover isn't possible.

7.5.7 THE "TRUNK RECORDING" TAB


SwyxServer VM-LGWSERVER07 Properties

Please use Swyx Control Center for configuration of Trunk Recording.

As of version 13.27, trunk recordings can be managed by SwyxWare. They can be stored in the database, in the file system or in an S3 object store. The configuration of the storage location is done via the Swyx Control Center. See https://help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/index.html#context/DataStorage.

When updating SwyxWare, the previous management of recordings can be retained.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

Ensure that all parties on the call are made aware at the beginning of the call that the call is being recorded in accordance with the requirements of the Telecommunications Act. Recording without the express consent of all participants in the conversation is considered unauthorized.

Records in the destination directory cannot be deleted automatically. In order to meet the valid data protection regulations, it may be necessary to delete the Files manually.

Currently excluded from permanent recording are trunks of type SwyxLink, which are managed remotely, and all SIP Gateway trunks.

Internal calls, i.e. calls between two users logged in to the same SwyxServer, are not recorded.

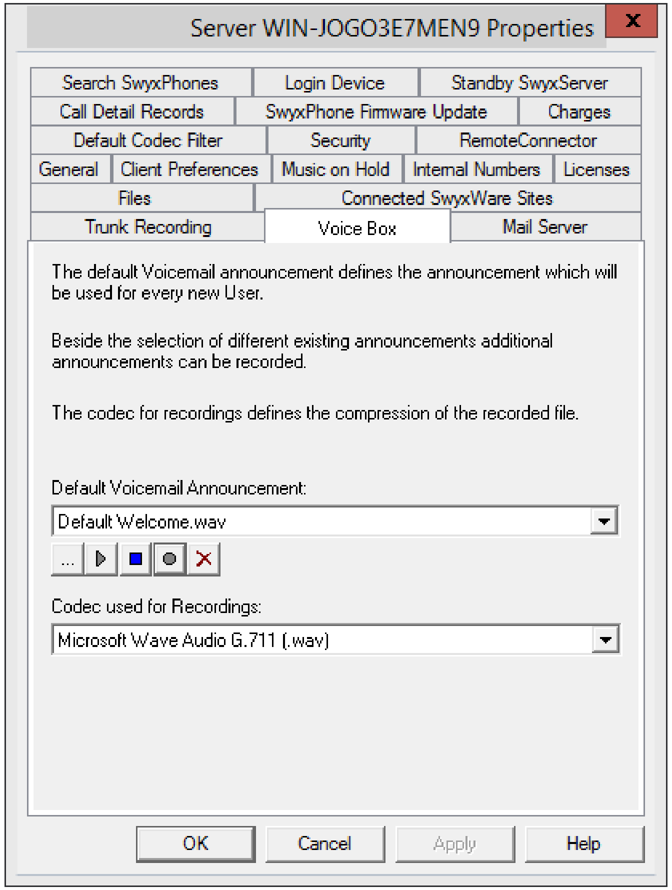
Recording must also be activated in the properties of a trunk group, otherwise no recording takes place. See *Record all Trunk Calls*, Page 229.

Calls over SwyxLink trunks can only be recorded if they are locally administered on this server. Calls via SIP gateway trunk (e. g. SwyxConnect) can not be recorded.

Trunk Recordings within SwyxWare for DataCenter

A provider that makes trunk recordings for its customers can make these available to the customer by using the Microsoft Internet Information Server (IIS) or another access via FTP or HTTP (WEBDAV). Access to the directory with the recordings of a trunk can then be individually granted.

7.5.8 THE "VOICE BOX" TAB



The default Voicemail announcement defines the announcement which will be used for every new User.

Beside the selection of different existing announcements additional announcements can be recorded.

The codec for recordings defines the compression of the recorded file.

Default Voicemail Announcement: Default Welcome.wav

Codec used for Recordings: Microsoft Wave Audio G.711 (.wav)

The parameters for Voice Box can be specified on this tab.

"SwyxVoicemail" must be activated in the user's feature profile.

Default Voice Box announcement

The Voice Box announcement which is pre-selected for all users is selected in this field. All Voice Box Announcement Files which are made globally available and which are stored in the database will appear in the drop-down list. These hold music files all have the "16 kHz 16 Bit PCM mono" audio format. You can search the network for other files in any WAV format using "Browse" (...). After you have chosen a WAV file, it will be converted into the above format and then saved in the database.

If the SwyxIt! Classic telephony client is also installed on your administration computer, you also have the option of using audio equipment to record a Voice Box announcement. When you click on "Record" (●), you will be asked for a file name. Then click on "Start" to begin recording. To stop the recording, click on "Stop" (■). "Delete" (✕) is used to delete the selected file. Please note that you can only delete files which you have created.

If the caller enters the DTMF number ‘0’ during the announcement, the Voice Box will be interrupted and the call will immediately connect to an operator(*22.5 Operator (AutoAttendant)*, Page 352).

Codec used for Recordings

Voice messages are recorded with the Opus codec by default during a new installation. The previously selected compression remains in place during an update. Alternatively, other built-in compressions can be used. The compression to be used can be set for all users andall groups, or individually for each user andeach group. The following settings are possible:

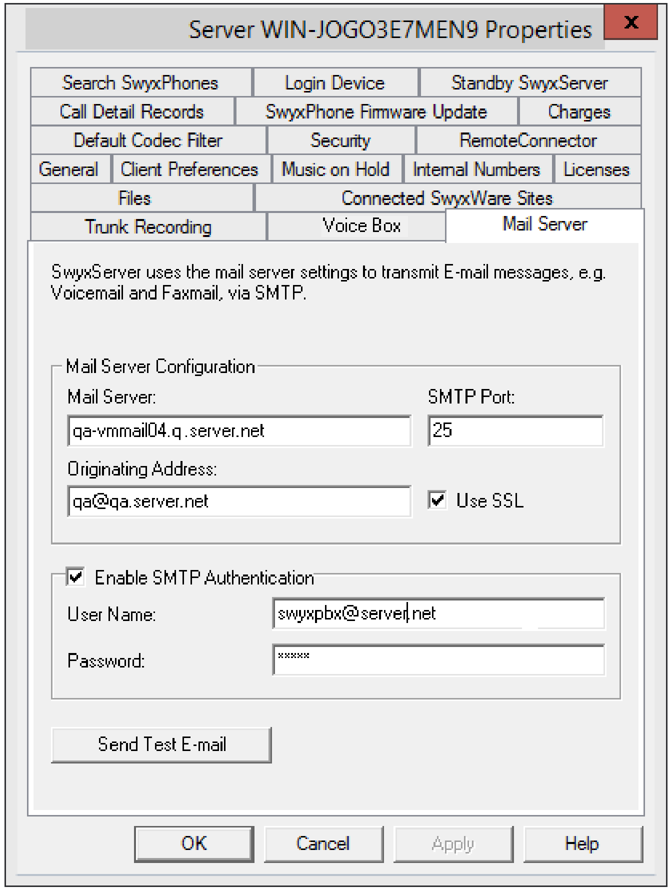
Name	Explanation
Open standard RFC6716 (.opus)	Dynamically adjustable bit rate. Best audio quality/storage space ratio (default setting after reinstallation)
Microsoft WAV Audio PCM	Standard WAV file, not compressed
Microsoft WAV Audio G711	WAV file, G.711 compressed

Name	Explanation
Microsoft WAV Audio GSM	WAV file, GSM compressed

7.5.9 THE "MAIL SERVER" TAB

The following parameters are used to enable SwyxServer to send email:

- Requests for permanent licenses can be sent via this mail server (*7.5.5 The "Licenses" Tab*, Page 91).
- With the Option Pack SwyxECR you can e.g. send emails from use of the Graphical Script Editor. that only specify at what time a call was received from which number.
- If the SwyxFax Option Pack is installed, then mail server is used to deliver fax mails to users (*24.8 Fax forwarding as Faxmail or printed document*, Page 375).
- From a SwyxWare for DataCenter, monthly usage reports are sent from the licensing server, see SwyxON*7.5.12 The "Usage Reports" Tab*, Page 102. These mail server settings are also used for this.
- Welcome and password reset e-mails are delivered to SwyxWare users via the e-mail server you have specified.



SwyxServer uses the mail server settings to transmit E-mail messages, e.g. Voicemail and Faxmail, via SMTP.

Mail Server Configuration

Mail Server: qa-vmmail04.q.server.net

SMTP Port: 25

Originating Address: qa@qa.server.net

☑ Use SSL

☑ Enable SMTP Authentication

User Name: swyxpbx@server.net

Password: *****

Mail Server Configuration

The explicit address of the SMTP mail server you use is entered in this field. All recorded voice messages and welcome e-mails are delivered to the SwyxWare user via this SMTP server. You can use a symbolic name, a DNS name, or a direct IP address in order to identify the SMTP server.

Enter the SMTP port for connecting the mail server.

Enter into the "sender address" field the email sender address for all voice messages, which SwyxServer will use to make deliveries to SwyxWare users (e.g. SwyxServer@company.com). This address must be chosen in correlation to the SMTP mail server used. Some SMTP mail servers support any choice of originating address, others require that the address be in the same form as the address which already exists for you. In any case, the domain label (e.g. "@company.com") should be identical to one of the domains managed by the mail server.

The date format of the voice message depends on the language setting within the Windows operating system, i.e. a computer with the language English (United States) will also provide an American date format (mm/dd/yy) for the voice messages.

Activate the checkbox "Use SSL" if you want to use a secure connection to the mail server, i.e. encoding the transferred data.

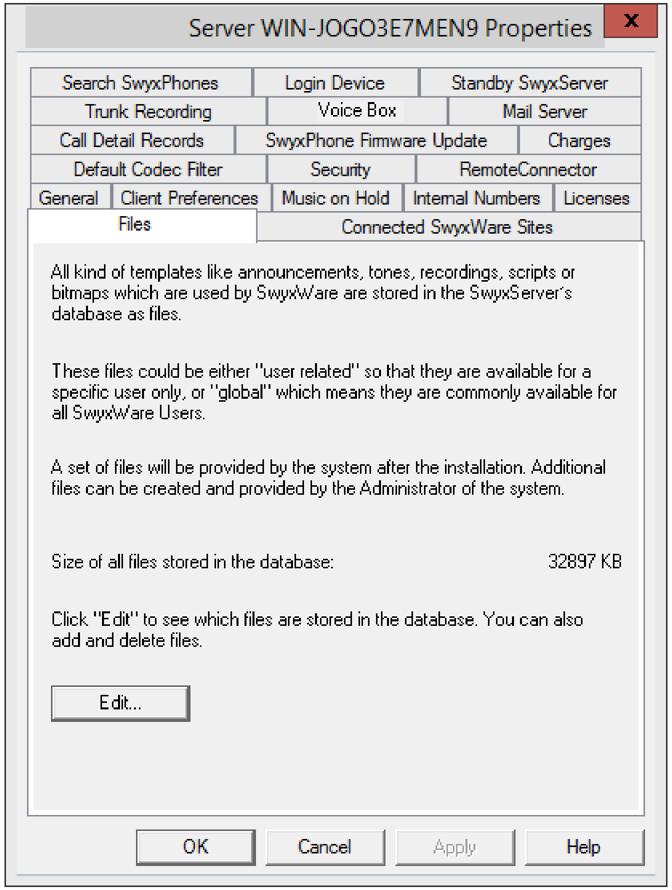
Enable SMTP authentication

Mail server authentication is supported in line with specification RFC 2554. The specific processes supported here are "LOGIN", "PLAIN", "CRAM-MD5".

Activate the checkbox and enter the username and password with which SwyxServer is to authenticate itself on the mail server configured above.

You can send a test email here which will be sent from SwyxServer to the specified sender address via the specified mail server.

7.5.10 THE "FILES" TAB



All kind of templates like announcements, tones, recordings, scripts or bitmaps which are used by SwyxWare are stored in the SwyxServer's database as files.

These files could be either "user related" so that they are available for a specific user only, or "global" which means they are commonly available for all SwyxWare Users.

A set of files will be provided by the system after the installation. Additional files can be created and provided by the Administrator of the system.

Size of all files stored in the database: 32897 KB

Click "Edit" to see which files are stored in the database. You can also add and delete files.

During installation the necessary files are stored in the database. These files include e.g. all ring tones, music on hold, announcements and scripts as well as an individually adaptable template for welcome E-mails, but no fax files.

Here you can see how much storage space these files take up.

You can edit, delete or add files here, e. g. the template for welcome E-mails. Open the list of files with "Edit..."

When saving and processing personal data, observe the respective applicable legal data protection regulations.

Personal data cannot be deleted automatically from the data base. In order to meet the valid data protection regulations, it may be necessary to delete the corresponding entries manually.

How to edit the template for welcome E-mails

1 Select the "WelcomeMailTemplate.html" file from the list.

2 Click on the "Save as..." button, and select a memory location.

3 Edit the template with any HTML editor by, for example, changing the E-mail texts, removing or adding configurations or adapting the logo.
To add configurations, use the variables provided. A list of all the variables is provided as a comment at the beginning of the template.
If necessary, you can change the default configurations for clients directly in the URL:

Configuration	Available values	Explanation
username	as preconfigured in the system	User name as preconfigured in the system
password	as preconfigured in the system	The password of the user, as preconfigured in the system
internalurl	as preconfigured in the system	SwyxServer-Address within the company network
externalurl		The public endpoint via the authentication service is accessible outside the company network.
connectionmode (This value is not interpreted by SwyxIt! Classic)	Preset to "auto"	Connection mode preset: available network is used automatically
	"Standard"	Internet
remoteconnectormode	Preset to "auto"	RemoteConnector use preset: is used automatically
	"always"	RemoteConnector is used always
connectiontype (This value is not interpreted by SwyxIt! Classic)	preset: "business"	Connection type for data transfer preset: via VoIP
	"private"	via cellular network
	"request"	You are asked before each telephone call which connection type is to be used
oem (This value is not interpreted by SwyxIt! Classic)	"swyx"	These values are set automatically by the installation and must not be changed.
	"tcom"	

You must replace special characters with the corresponding hexadecimal code, e. g. comma='%2C', space='%20', colon='%3A' etc.

The server type and OEM variant configurations are determined automatically by the installation.

4 Click on the "Add..." button to save the edited file in the database.

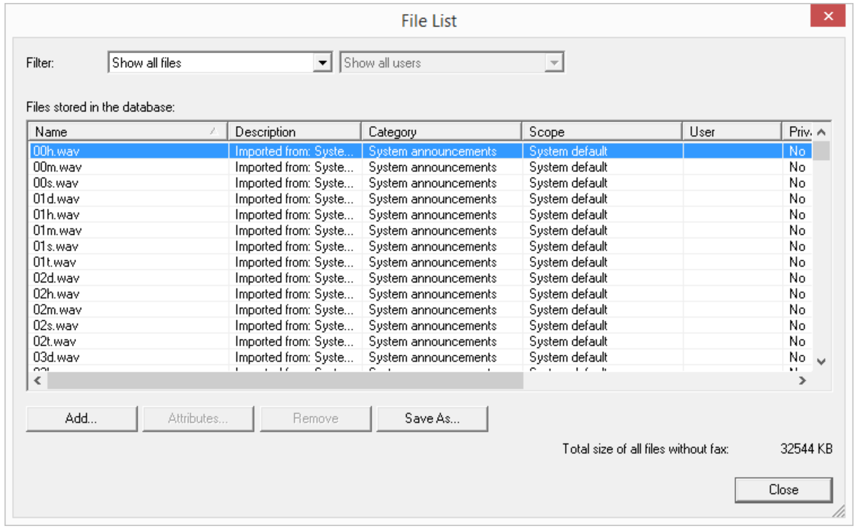
You may not change the file name of the template because otherwise the file will not be recognized by the system.

When adding the file, you must select the area "Global" and the category "Templates".

For further settings, see *7.5.10.1 Add files*, Page 99.

5 Click on the "OK" button in the dialog window "Add file to the database".

See also *How to send a Welcome email*, Page 173.



Filter: Show all files | Show all users

Files stored in the database:

Name	Description	Category	Scope	User	Priv.
00h.wav	Imported from: Syste...	System announcements	System default		No
00m.wav	Imported from: Syste...	System announcements	System default		No
00s.wav	Imported from: Syste...	System announcements	System default		No
01d.wav	Imported from: Syste...	System announcements	System default		No
01h.wav	Imported from: Syste...	System announcements	System default		No
01m.wav	Imported from: Syste...	System announcements	System default		No
01s.wav	Imported from: Syste...	System announcements	System default		No
01t.wav	Imported from: Syste...	System announcements	System default		No
02d.wav	Imported from: Syste...	System announcements	System default		No
02h.wav	Imported from: Syste...	System announcements	System default		No
02m.wav	Imported from: Syste...	System announcements	System default		No
02s.wav	Imported from: Syste...	System announcements	System default		No
02t.wav	Imported from: Syste...	System announcements	System default		No
03d.wav	Imported from: Syste...	System announcements	System default		No

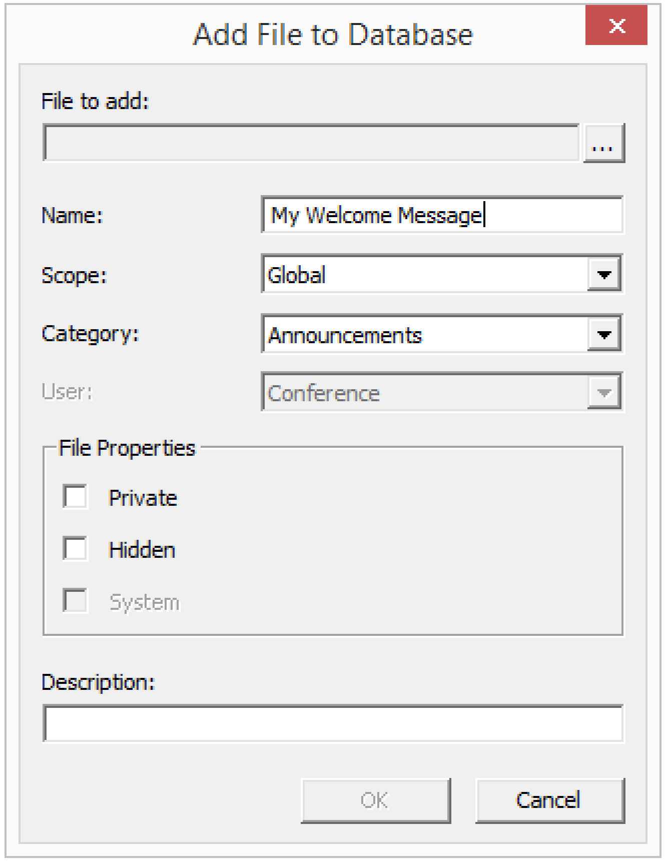
Total size of all files without fax: 32544 KB

You can choose which files are displayed for you:

- Show all files
- Show user files
  User files are assigned to an individual user. Only the user himself, an administrator or SwyxServer, if e.g. it processes Call Routing Manager scripts, have access to these files. All files generated with a SwyxIt! Classic or the SwyxWare Administration, such as scripts and announcements, are saved as private files. An exception is the file 'Name.wav', which contains the name of the user.
- Show user-specific standard files
  During installation these files are stored for a particular user (e. g. Operator) as standard files in the database. This user can then use these files unchanged. If the files, e. g. an announcement, are subsequently changed, then they are saved as user-specific files and are not changed again in a later SwyxWare update.
- Show global files
  These files (e.g. skins or Call Routing Manager rules) can be used by any user. If they are changed by the user, the changed file is saved as a user-specific file.
  These global files enable e.g. the administrator to create templates for all SwyxWare users, which they can then use with personal data. For example, a company-wide standardized skin can be stored here, which the users can further develop as they wish; or a call routing script, which the users can then personalize with their own announcement and their number.
  Global files with the same name as a system file are given preference; for example, a new global announcement with the name 'Standard_announcement.wav' replaces the supplied system file of the same name.
  Global files remain unchanged in a SwyxWare update.
- Show system standard files
  These files are stored in the database during the SwyxWare installation, and may be renewed in an update.
  If a file is private, it can only be used by the SwyxServer. Otherwise it is available to all users.
  In SwyxWare versions prior to 6.10, these files were stored in the directory Share\Data.

7.5.10.1 ADD FILES

If you add a new file, you can set the properties of this file. However, you can also change these properties later, by editing "Attributes...".



Add File to Database

File to add:

Name: My Welcome Message

Scope: Global

Category: Announcements

User: Conference

File Properties

☐ Private

☐ Hidden

☐ System

Description:

If you are adding a file, you enter the path and the file name in the "File:" field, or search for the file.

When adding a file you specify the name under which it should be saved in the database, and the scope of this file's availability:

- Global
  This file will be available to all users who are logged in to this SwyxServer.
- System standard
- User
  Here you select the user to which this file should be assigned. This file is then available only to the selected user.
- Default for user
  Here you select the user to which this file should be assigned. This file is then available only to the selected user.

This scope is defined when adding the file, and cannot be changed afterwards.

Category

Specify the category to which this file belongs. The following categories are available:

- Ring tones
- Fax Cover Graphics
- Fax Cover Page
- Fax Header
- Call Routing scripts
- Bitmaps
- Announcements
- Music on Hold
- System announcements
- Sample announcements
- Recording List
- Skins
- DCF Custom Provisioning
- Others

File Properties

Specify the properties of this file:

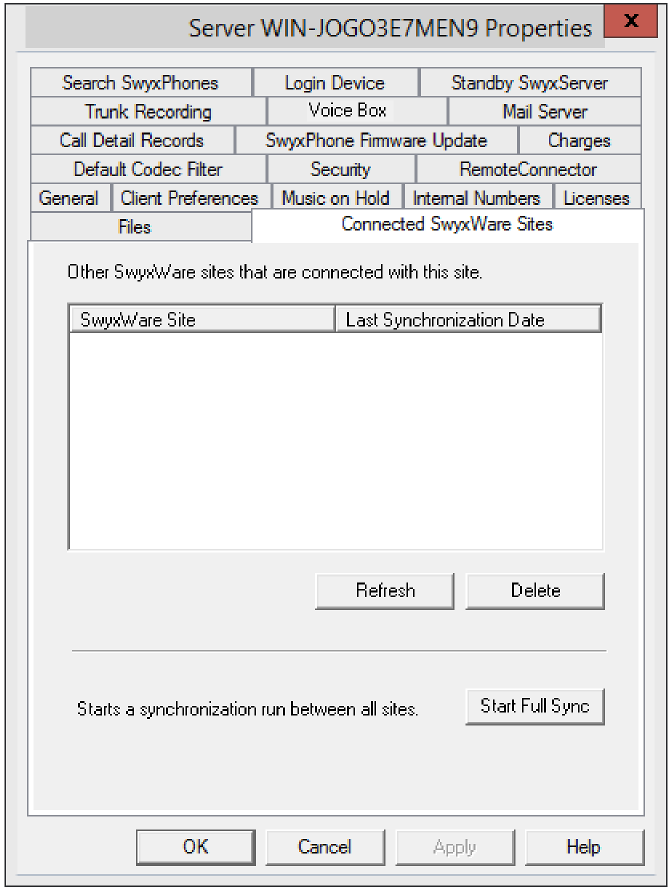
Property	Explanation
Private	This file is only accessible to the user himself, e.g. in one of his scripts. Example: Call Routing script with password

Property	Explanation
Hidden	This file does not appear in the selection drop-down lists. Example: The file '20m.wav' (twenty minutes) belongs to the time announcement, and does not appear for the selection of a welcome message.
System	This file was created during installation, and is always write-protected.

Description

The description can contain more detailed information about this file.

7.5.11 THE "CONNECTED SWYXWARE SITES" TAB



Other SwyxWare sites that are connected with this site.

SwyxWare Site	Last Synchronization Date

Starts a synchronization run between all sites.

On this tab you can see all the SwyxServers connected to this SwyxServer, and the date of the last synchronization.

Here you have the possibility of manually removing data which e.g. is left behind after deletion of a SwyxLink trunk.

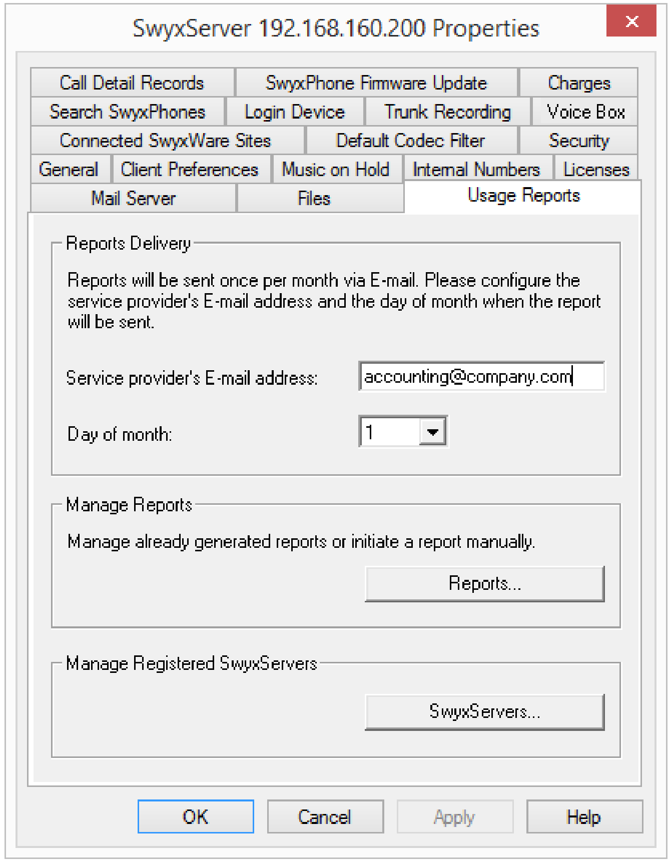
You can also start a manual synchronization of the connected SwyxServers here. The data of the local SwyxServers is sent to all connected servers, and the connected servers for their part send data to this SwyxServer.

A synchronization otherwise occurs whenever a server is restarted, or if changes are made to the user data.

See *17 SwyxLink (Server-Server Connection)*, Page 292.

7.5.12 THE "USAGE REPORTS" TAB

This tab "Usage Reports" appears only on the licensing server within a SwyxWare for DataCenter installation.



Reports will be sent once per month via E-mail. Please configure the service provider's E-mail address and the day of month when the report will be sent.

Service provider's E-mail address: accounting@company.com

Day of month: 1

Manage already generated reports or initiate a report manually.

In SwyxWare for DataCenter, the license is centrally entered on a licensing server only, and all other installed servers reference to this licensing server (*Licensing server (only for SwyxWare for DataCenter and SwyxON)*, Page 87). The reporting is then also activated on this licensing server. This service arranges for a daily data collection relating to the configured users and functions. The data is stored in the reporting database. This service also sends a monthly report, which is used for charging for the installed user numbers and functions, to the E-mail address given here for the service provider and to Enreach.

If this service is inactive for a lengthy period (a maximum of seven days), the license lapses on the licensing server, and consequently for all installed SwyxServers.

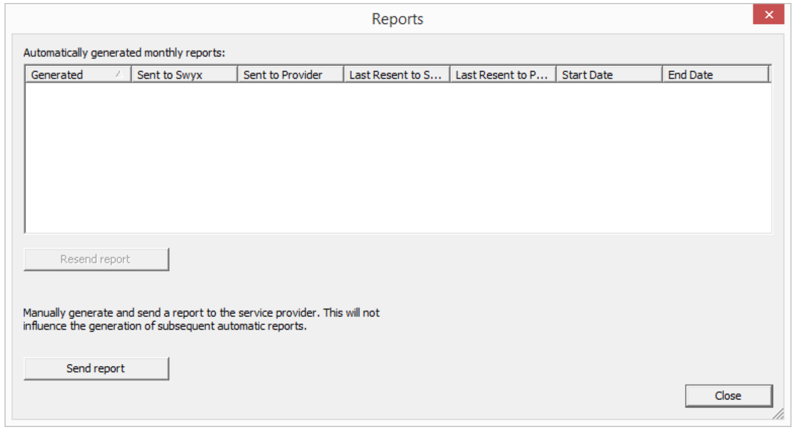
Enter in the field "Service provider's Email address" ("provider's email address) the email address to which the monthly report should be sent.

In the field "Day of month", specify the day of the month on which the monthly report should be sent. If you choose '31', the report is always sent on the last day of the month.

Report management

If you want to have an overview of the reports that have already been sent, or you want to resend reports or send a report with the data of the current billing period, click on "Reports...".

Reports



Reports

Automatically generated monthly reports:

Generated	Sent to Swyx	Sent to Provider	Last Resent to S...	Last Resent to P...	Start Date	End Date

Manually generate and send a report to the service provider. This will not influence the generation of subsequent automatic reports.

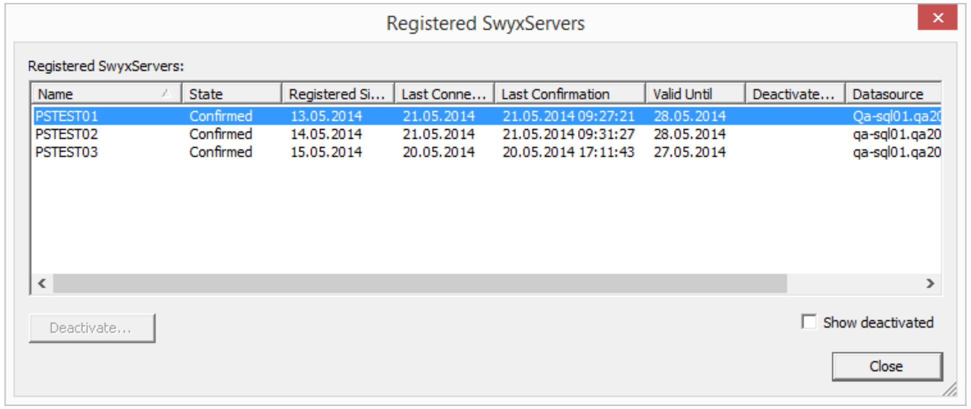
The list "Automatically generated monthly reports" contains all monthly reports that have already been generated and sent. If a report is sent again, the date when it was last sent is entered in the relevant column. The period for which a report was created can be found in the "Start Date" ("from") or "End Date" ("to") columns.

"Resend report" ("Bericht erneut senden") resends a report that is highlighted in this list, both to Enreach and to the service provider.

To obtain the current status of the database in the open billing period, you can send an intermediate report. This report records all data since the last monthly report up to the last daily data entry. Sending this report does not reset the reporting, i.e. next monthly report still records the complete billing period, beginning with the dispatch time of the preceding monthly report. This intermediate report is not saved, i.e. it does not appear in the list of reports sent.

Manage registered SwyxServer

Click on "SwyxServers..." to obtain an overview of the servers that get their licenses from this licensing server.



Registered SwyxServers

Registered SwyxServers:

Name	State	Registered Si...	Last Conne...	Last Confirmation	Valid Until	Deactivate...	Datasource
PSTEST01	Confirmed	13.05.2014	21.05.2014	21.05.2014 09:27:21	28.05.2014		Qa-sql01.qa20
PSTEST02	Confirmed	14.05.2014	21.05.2014	21.05.2014 09:31:27	28.05.2014		qa-sql01.qa20
PSTEST03	Confirmed	15.05.2014	20.05.2014	20.05.2014 17:11:43	27.05.2014		qa-sql01.qa20

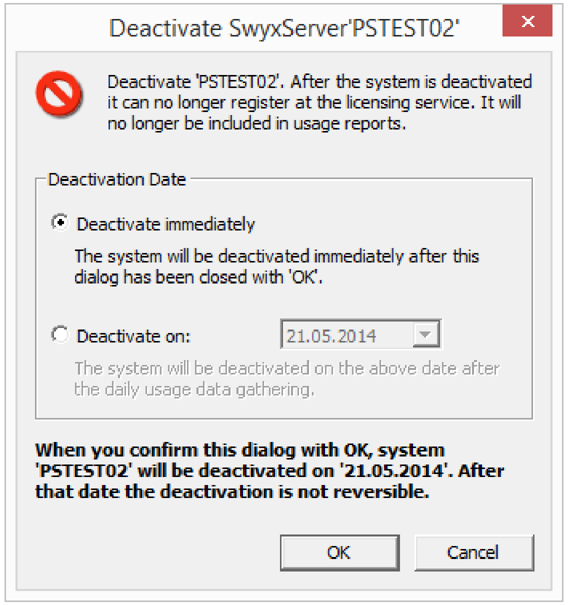
From here you can find out how long the server has been registered, its last registration date, and how long the registration is still valid. You can also find out which database on which computer (data source) a SwyxServer uses.

The "State" ("Status") column may contain the following values:

- Not yet Confirmed:
  SwyxServer Is registered, but could not yet be checked by the licensing service. The server is not licensed and may not be used.
- Confirmed:
  SwyxServer Is registered and has successfully been checked by the licensing service. The server is active and may be used.
- Expired:
  The last successful SwyxServer check by the licensing service took place more than seven days ago. The server is not licensed and may not be used.
- Deactivated:
  SwyxServer is deactivated and will not be reflected in the invoice. The server is not licensed and may not be used.
  If the server is deactivated or the deactivation is limited, the last valid invoice date is displayed in the "Deactivate On" column.

Activate/Deactivate

You can deactivate a single SwyxServer. To do so, highlight the SwyxServer you want to deactivate, and click on "Deactivate...".



Deactivate SwyxServer'PSTEST02'

Deactivate 'PSTEST02'. After the system is deactivated it can no longer register at the licensing service. It will no longer be included in usage reports.

Deactivation Date

● Deactivate immediately

The system will be deactivated immediately after this dialog has been closed with 'OK'.

○ Deactivate on: 21.05.2014

The system will be deactivated on the above date after the daily usage data gathering.

When you confirm this dialog with OK, system 'PSTEST02' will be deactivated on '21.05.2014'. After that date the deactivation is not reversible.

You can choose between

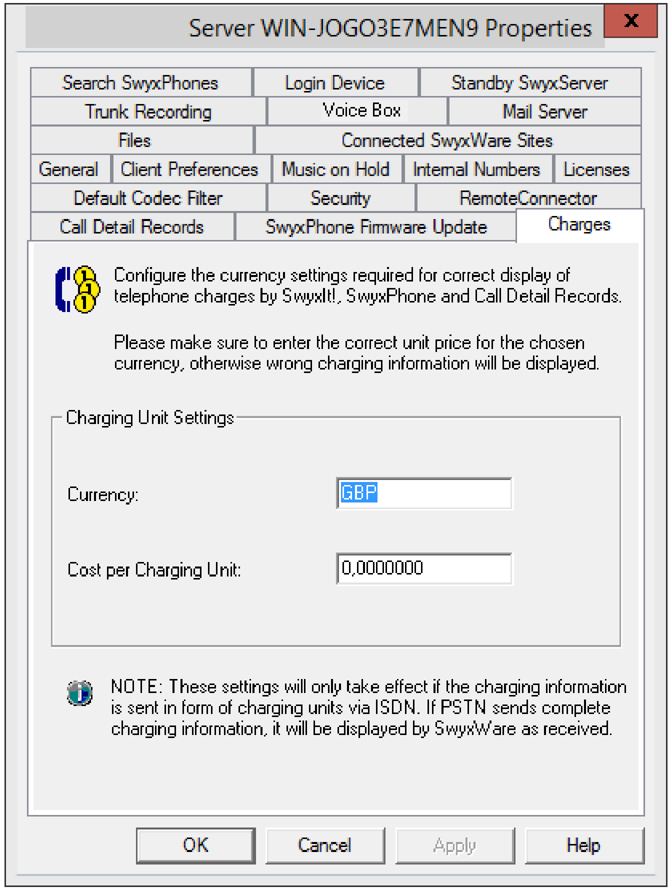
- Deactivate immediately
  The selected server is deactivated after the next daily data entry (reporting).
- Deactivate on:
  The selected server is deactivated on a specified day after the daily data entry.

> The deactivation of a system is not reversible! Deactivation can only be revoked before the deactivation date. To do this, highlight the relevant server in this list, and click on "Reactivate". The deactivation is fully revoked.

Checkbox "Show deactivated"

If you only want active serves to appear in the "Registered SwyxServers" list, please deactivate the "Show deactivated" check-box. If active, the list also displays servers that have already been deactivated.

7.5.13 THE "CHARGES" TAB



Server WIN-JOGO3E7MEN9 Properties

Configure the currency settings required for correct display of telephone charges by SwyxIt!, SwyxPhone and Call Detail Records.

Please make sure to enter the correct unit price for the chosen currency, otherwise wrong charging information will be displayed.

Charging Unit Settings

Currency: GBP

Cost per Charging Unit: 0,0000000

NOTE: These settings will only take effect if the charging information is sent in form of charging units via ISDN. If PSTN sends complete charging information, it will be displayed by SwyxWare as received.

After each call unit a call-charge pulse is transmitted from the public telephone network (AOC=Advice of Charge). This pulse can be used for charging information. On the "Charges" tab you can configure the currency to be used for displaying the charges and the costs per call unit.

In SwyxWare for DataCenter and SwyxON, contact your service provider about fees.

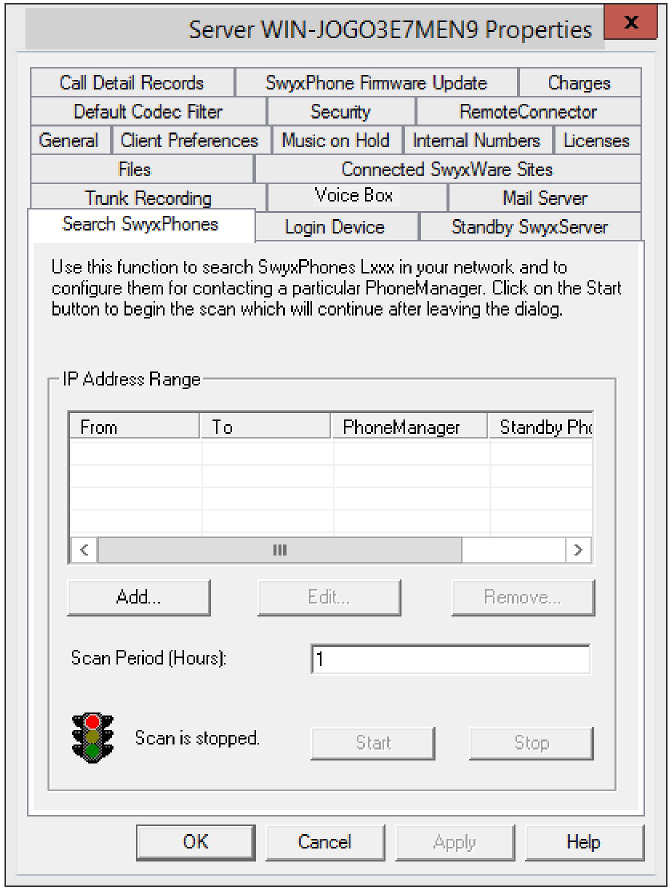
The way in which information is transmitted via pulses can vary depending on the telecommunication provider. Each pulse can transmit three types of information: the number of units spent, the price per unit and the currency. Not all of this information can be transmitted (e.g. in most cases, Deutsche Telekom delivers only the number of spent units, whereas units and the price are transmitted in Switzerland). In cases in which only the number of charged units is transmitted, SwyxServer uses the values configured here in order to calculate the charges.

Please note that, when calculating the charges, the information delivered by the pulse have priority compared to the information specified here.

These charges will be displayed in the Call Detail Records, on the telephony client and on SwyxPhone.

If you leave the field for the unit charge empty or if you enter the value ‘0’ no charges will be displayed.

7.5.14 THE "SEARCH SWYXPHONES" TAB



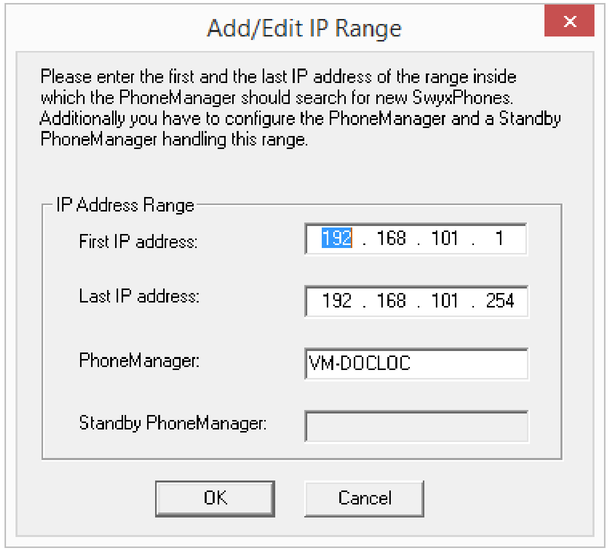
Use this function to search SwyxPhones Lxxx in your network and to configure them for contacting a particular PhoneManager. Click on the Start button to begin the scan which will continue after leaving the dialog.

Scan Period (Hours): 1

Scan is stopped.

The connection of the IP telephones to your PhoneManager is configured here. When the scan is started, it assigns the IP address of the responsible PhoneManager to all addressed telephones within the given IP address range.

If you would like to add a new PhoneManager, click on "Add...". A new window, "Add/Edit IP Range", will appear.



Please enter the first and the last IP address of the range inside which the PhoneManager should search for new SwyxPhones. Additionally you have to configure the PhoneManager and a Standby PhoneManager handling this range.

IP Address Range

First IP address: 192 . 168 . 101 . 1

Last IP address: 192 . 168 . 101 . 254

PhoneManager: VM-DOCLOC

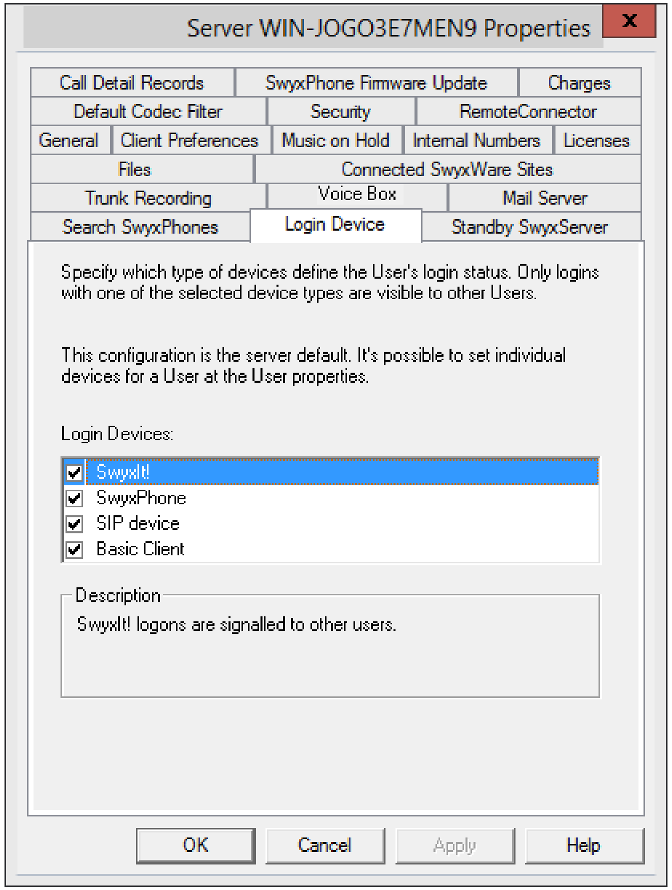
Standby PhoneManager:

Enter here the range of the IP addresses in your network, in which the SwyxPhone should be searched for, and the corresponding PhoneManager or Standby PhoneManager, and confirm this with "OK".

Enter how many hours the PhoneManager should scan for SwyxPhones and start the scan.

Please note that the scan for the phones will create minimal, yet continuous traffic in the network. For this reason, the scan is subjected to a time limit.

7.5.15 THE "LOGIN DEVICE" TAB



Specify which type of devices define the User's login status. Only logins with one of the selected device types are visible to other Users.

This configuration is the server default. It's possible to set individual devices for a User at the User properties.

Login Devices:

☑ SwyxIt!
☑ SwyxPhone
☑ SIP device
☑ Basic Client

Description

SwyxIt! logons are signalled to other users.

Terminal types

Whether the users signal their status (logged in, speaking, is called) among each other or not, is defined in the relationships of the users or groups. Here you specify, which type of terminal signals the Log-on status of the user, if several terminal types are logged in to the same user account.

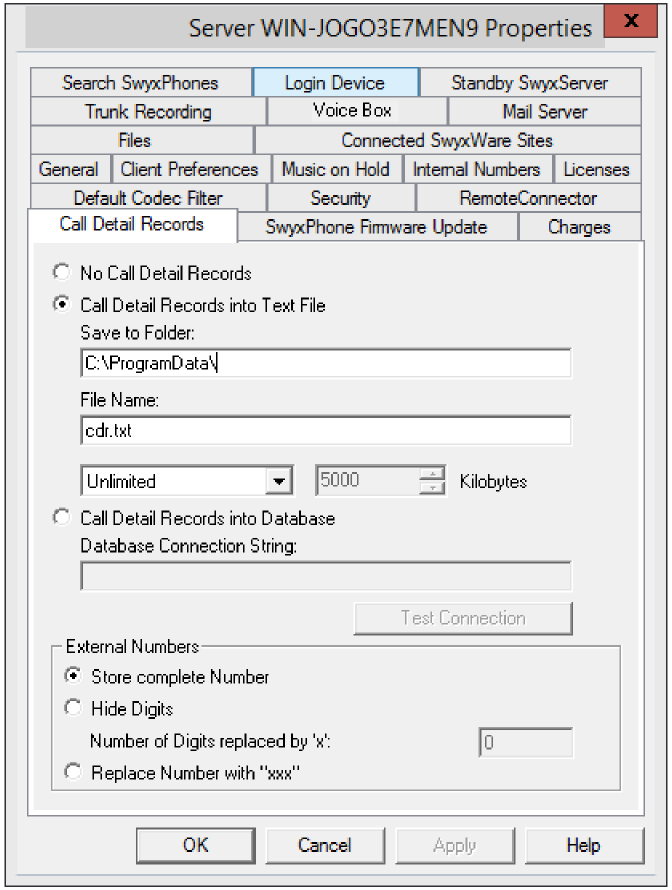
Define here which standard settings should be uses for the user. You can also configure individual settings for individual users (*11.2.6.11 The "Login Device" Tab*, Page 196).

> *Example:*
>
> *For example, if a user has a SwyxPhone on his desk and a SwyxIt! Classic installed on his computer, he can check his status by SwyxIt! Classic signal. He is then logged in when his computer is switched on and SwyxIt! Classic has started. Is SwyxIt! Classic not started, he can still use his SwyxPhone. However, the status "logged off" is signalled to internal employees and call routing. If the user speaks with SwyxPhone the status "Speaking" is signalled to the employees, for call routing his status remains "logged off".*

Some cases can also be mentioned specifically for the various offered by Enreach :

- Basic Client
  Activate the end device type "Basic Client" if the Swyx Mobile App (Windows Phone) status should be signalized.
- SwyxPhone Lxxx
  If the status signaling needs to be dependent upon SwyxPhone Lxxx, then activate the 'SIP device' option here.

7.5.16 THE "CALL DETAIL RECORDS" TAB (CDR)



○ No Call Detail Records

● Call Detail Records into Text File

Save to Folder: C:\ProgramData\

File Name: cdr.txt

Unlimited ▾ 5000 Kilobytes

○ Call Detail Records into Database

Database Connection String:

External Numbers

● Store complete Number

○ Hide Digits

Number of Digits replaced by 'x': 0

○ Replace Number with "xxx"

SwyxWare allows you to record information concerning connected calls, so-called "Call Detail Records", in a text file. Recording is preset as deactivated.

When you activate "Call Details Record in Text File" you will activate the recording of this data in a text file.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

Here, you define the file and the directory where SwyxServer will save the Call Detail Records.

You can restrict recording either according to file size or in terms of time. If the maximum file size or number of days (standard: 7 days) is exceeded, a new file with the same name plus a counter will be created and filled. The existing files are only deleted if you select time restriction.

Please observe the respective applicable legal regulations. Please observe this in particular if you change the settings for memory restriction.

Call details records can also be saved in a database. To do this, activate "Call Detail Records in Database" and enter the database connection sequence. You can use "Test Connection" to test the connection to the database.

Single connection information cannot be deleted from the database. Please observe the respective applicable legal regulations. Please observe this in particular if you select the database as the memory location.

If you do not wish to maintain a record, activate "No Call Detail Records". This option is set by default.

For detailed information regarding the format of the file saved, please refer to *App. A: Call Detail Records (CDR)*, Page 398.

External numbers

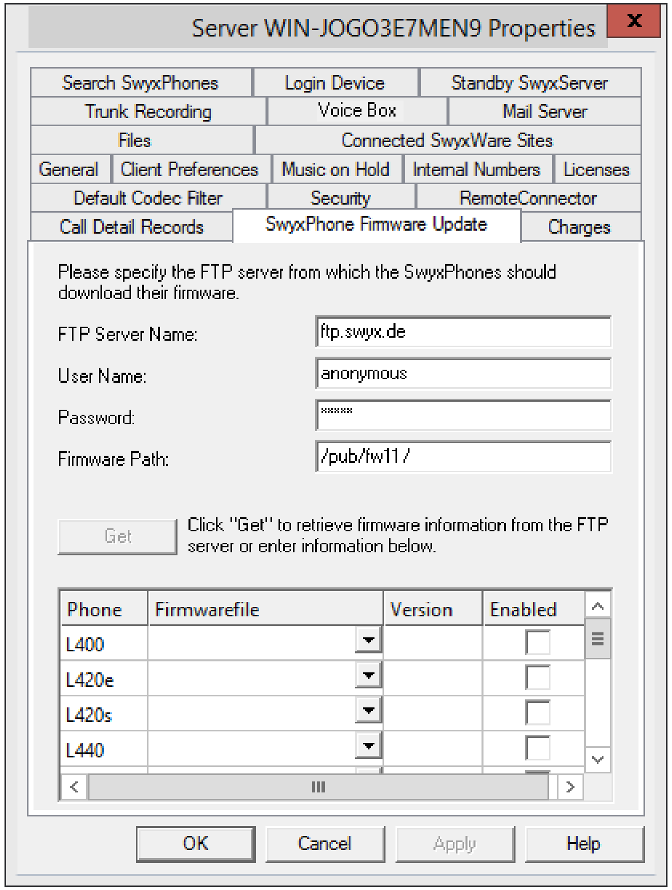
Specify the format in which external numbers are stored in the file. You have the following options:

- Save entire number
  The entire external number is saved in the call detail records.
- Hide digits
  You have the option of only storing external numbers in part by replacing some of the digits with 'X'. Specify how many digits (from the end) are to be replaced.
- Replace number with 'XXX'
  The entire external number is replaced with 'XXX'. In this case you will not be able to see anymore whether the call was, e.g. an international or a local call.

Please observe the respective applicable legal regulations. Please observe this in particular if you select the database as the memory location, see *8.3 Private and business calls*, Page 123.

It is not possible to hide those numbers only which were dialed using the public line access. In this case, apply digit replacement for all calls.

7.5.17 THE "SWYXPHONE FIRMWARE UPDATE" TAB



Please specify the FTP server from which the SwyxPhones should download their firmware.

FTP Server Name: ftp.swyx.de

User Name: anonymous

Password: *****

Firmware Path: /pub/fw11/

Click "Get" to retrieve firmware information from the FTP server or enter information below.

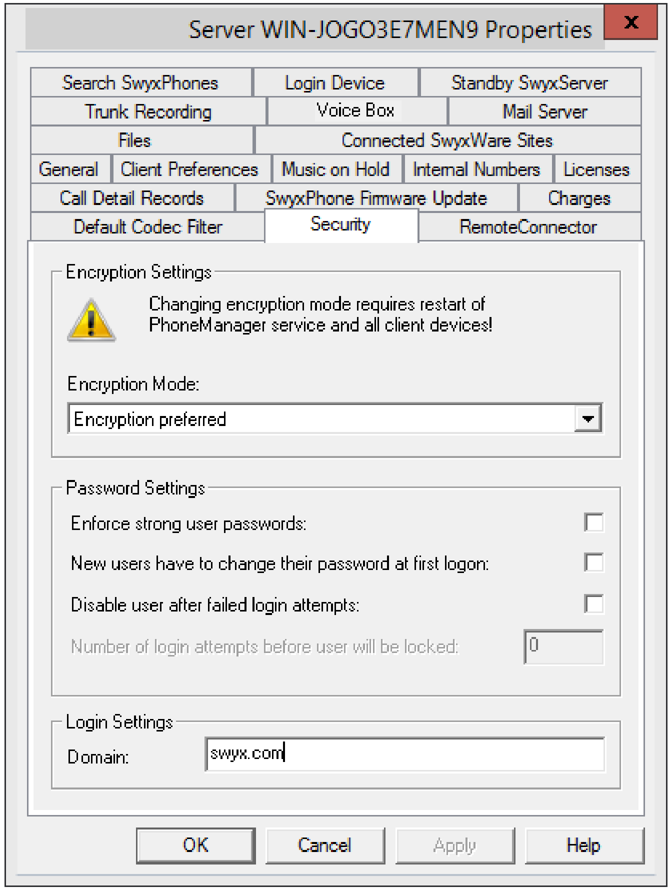
Phone	Firmwarefile	Version	Enabled
L400			☐
L420e			☐
L420s			☐
L440			☐

On this tab you can set the data for an automatic firmware update for SwyxPhone, such as the FTP server from which the software is going to be loaded, the corresponding user name and password and the path for the new firmware. "Get" provides you with a selection list of all available firmware files. Define in the drop-down list, which firmware should be distributed to which SwyxPhone.

If you have activated automatic update, the server will check the firmware version of SwyxPhone when you log in. If SwyxPhone identifies a software version other than the one defined here, the SwyxPhone user will be given the opportunity to update the firmware. See *20.2.4 Automatic Firmware Update for a SwyxPhone Lxxx*, Page 335.

It may happen that the PhoneManager requests an Update of the SwyxPhone firmware. The menu of the SwyxPhone points out if the automatic updates is not activated.

7.5.18 THE "SECURITY" TAB



Encryption Settings

Changing encryption mode requires restart of PhoneManager service and all client devices!

Encryption Mode: Encryption preferred

Password Settings

Enforce strong user passwords: ☐

New users have to change their password at first logon: ☐

Disable user after failed login attempts: ☐

Number of login attempts before user will be locked: 0

Login Settings

Domain: swyx.com

This tab is used to set the encryption mode and password rules for SwyxServer in general.

Encryption settings

Encryption mode is determined globally for SwyxServer in this area, which means the settings you choose here will influence the encryption settings in user and trunk properties.

If you set the encryption mode to "No encryption" here, the mode in the user and trunk properties is likewise set to "No encryption"; if you select "Encryption mandatory" here, then the setting "Encryption mandatory" also appears there. In both cases, the mode cannot be changed within the user and trunk properties. The field is then deactivated.

A change of the encryption mode requires a restart of all client devices.

The SwyxLink trunk and the SIP trunk are exceptions in this context. In the SwyxLink trunk, the encryption mode is taken from the server settings and cannot be changed. You can configure encryption for SIP trunks in the SIP trunk group settings. See *Exceptions*, Page 342.

See *21 Encryption*, Page 342.

Password settings

In this area, you can force password rules for better user account protection.SwyxWare-Administrators and users will then have to meet additional security conditions when logging on to SwyxServer.

Logging on to terminal devices and SIP registrations as well as authentication via Windows user accounts are not affected by these password settings.

The default configuration is for all rules to be deactivated.

The following rules can be configured:

- Force complex user passwords:

  If this control field is activated, only those user passwords will be permitted that are at least eight characters long and meet at least three of the following four character classes:

  - upper-case letters such as: [A-Z]

  - lower-case letters such as: [a-z]

  - Numbers [0-9]

  - Non-alphanumeric characters (special characters), such as: Dot, comma, brackets, space, double cross (#), question mark (?), percent sign (%), ampersand (&).

Alphabetic characters (such as: ß, ü, ä, è, ô) and non-Latin characters (such as: φ, π, β) are no special characters and are regarded as letters.

In SwyxON, the policy for complex passwords is enforced by default and cannot be overridden by any administrator.

When the "force complex password" rule is activated in server configuration and/or user configuration, then the user will be able to continue to use the current password until the user decides to change the password or until the administrator forces password change.
You can force users to change their passwords or to use complex passwords. See *11.2.1.2 The "Authentication" Tab*, Page 165.

If the "Force complex user password" option is enabled for the user, the last passwords of the user will be taken into account during the change. The user cannot reuse the last three passwords.

Regardless of the password settings, an attempt to re-enter the current password during password change will be checked by the system and will not be permitted.

- Deactivate user after failed login attempts
  If this checkbox is activated, then the system will lock user account based on a predetermined number of failed login attempts (e.g. password entered incorrectly multiple times). The corresponding users will be deactivated and will not be able to use terminal devices or clients.
  This option can only be used together when the parameter "Number of unsuccessful logins before deactivation" is set.

Following activation, this rule will apply for all users and administrators. System administrators are the only ones who are not locked.

Only an administrator can activate a user. See *11.4 Activate/deactivate or delete users*, Page 207.

- Number of unsuccessful logins before deactivation.
  This entry field is used to set the number of attempts a user may use to SwyxServer login. Only values "3" to "20" are used.

The number of failed log-in attempts will be reset for the corresponding user after one successful login. After resetting the SwyxServer services or after changing between master and standby server, this number is reset to zero for all users.

The number of failed log-on attempts is irrelevant, when the administrator has established a forced password change, and the user attempts to log-on with his/her previous password.

If a user has been deactivated, then the user will be shown the corresponding notification and an instruction to contact the administrator. See *7.1.2 Limited number of log-in attempts*, Page 82.

Log in settings

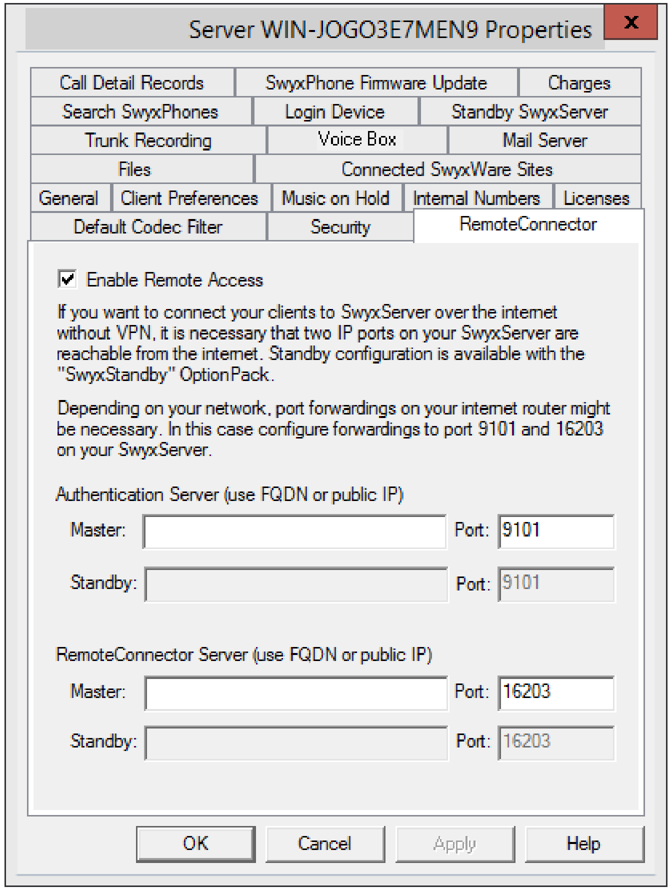
The user name in UPN format should be used for logging on to SwyxWare Administration and clients.

In this area, you can configure a UPN-Suffix.

See also *11.2.1.2 The "Authentication" Tab*, Page 165.

7.5.19 THE "REMOTECONNECTOR" TAB

The configuration on this tab is supported only for compatibility with the older SwyxWare installations.
Use Swyx Connectivity Setup Tool to define the RemoteConnector settings, see *6.3 RemoteConnector Configuring*, Page 74



☑ Enable Remote Access

If you want to connect your clients to SwyxServer over the internet without VPN, it is necessary that two IP ports on your SwyxServer are reachable from the internet. Standby configuration is available with the "SwyxStandby" OptionPack.

Depending on your network, port forwardings on your internet router might be necessary. In this case configure forwardings to port 9101 and 16203 on your SwyxServer.

Authentication Server (use FQDN or public IP)

Master: Port: 9101

Standby: Port: 9101

RemoteConnector Server (use FQDN or public IP)

Master: Port: 16203

Standby: Port: 16203

You can configure SwyxServer for Internet connections with your Clients using this tab.

Enable remote access

If support for direct internet connections to the clients is required, activate the check-box.

Authentication server (FQDN or public IP)

Enter the public server address and the port into the corresponding fields to allow Swyx clients to reach the server via InternetSwyxServer.

The registered public address of the authentication service must be configured within the respective settings on the Client computers.

If you use a different standard port and not 9101, it has to be explicitly input in the Client settings.

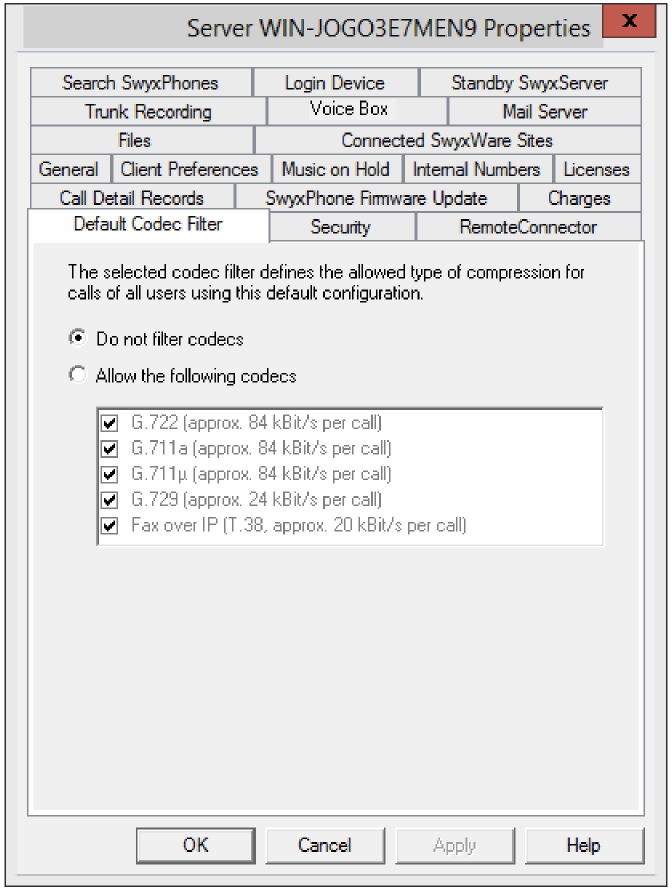
See *26.1 Internet connection via RemoteConnector*, Page 385.

RemoteConnector Server (FQDN or public IP)

Enter the public server address and the SwyxRemoteConnector server port in the respective fields. The standard ports for the SwyxRemoteConnector are 16203 or 57203.

See *26.1 Internet connection via RemoteConnector*, Page 385.

7.5.20 THE "DEFAULT CODEC FILTER" TAB



The selected codec filter defines the allowed type of compression for calls of all users using this default configuration.

● Do not filter codecs

○ Allow the following codecs

☑ G.722 (approx. 84 kBit/s per call)
☑ G.711a (approx. 84 kBit/s per call)
☑ G.711µ (approx. 84 kBit/s per call)
☑ G.729 (approx. 24 kBit/s per call)
☑ Fax over IP (T.38, approx. 20 kBit/s per call)

With the help of the codec filter, you can define how voice is compressed for transmission. Specify globally here for the SwyxServer whether codecs should be filtered, and if so, which codecs should be permitted.

Selection	Meaning
Do not filter Codecs	When "Do not filter codecs" is selected, all media data whatever the codec is transferred without change to the destination (transparent mode). This setting allows foreign Codecs unknown to SwyxServer to be used, e.g. Video.
G.729 (around 64 kbit/s per call)	Voice, high bandwidth. The voice data is transmitted in HD audio quality.
G.711a (around 64 kbit/s per call)	Voice, high bandwidth. The voice data is slightly compressed.
G.711µ (around 64 kbit/s per call)	
G.729 (around 24 kbit/s per call)	Voice, low bandwidth. The voice data is heavily compressed.
Fax over IP (T.38, around 20 kbit/s per call)	Fax. In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration.

You can also specify the codec filters individually per user within the user properties. The parameters specified here for the selected user are then discarded. See *11.2.1.10 The "Codec Filter" Tab*, Page 176.

The transparent mode (option "Do not filter codec") enables users to take part in calls with new codecs which were previously unknown to SwyxServer.

In non-transparent mode, SwyxServer checks whether the codec used for the voice data in a call is configured as permitted. If it isn't, the call will be rejected. An error message will appear.

In a new installation and in an update, "Do not filter codecs" is set as default. Thus, all codecs are activated.

7.6 GLOBAL PHONEBOOK

The Global Phonebook lists all SwyxWare users of this SwyxServer as well as all users of SwyxServers connected to this server via a SwyxLink trunk. To enable the display of a user in the Phonebook, the "Show in Phonebook" must be activated in the user's properties, see *11.2.2.1 The "Numbers" Tab*, Page 177.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

Personal data cannot be deleted automatically. In order to meet the valid data protection regulations, it may be necessary to delete the entries manually, see *This is how you change or delete entries in the Global Phonebook*, Page 114

With an Intersite connection via a SwyxLink trunk, the users of all connected servers are also visible in the Global Phonebook of the SwyxPhones.

The right to edit the Global Phonebook is defined by the administration profiles. See *9.3 Administration profiles*, Page 143.

Entries in the Global Phonebook can also be made with SwyxIt! Classic. In that case only entries can be edited that do not pertain to any configured users. The right to change entries is granted by respective administrator profiles (*9.3 Administration profiles*, Page 143). See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/changing_global_phonebook_$.

Other (external) numbers can be entered in the "Global Phonebook" by the administrator. These numbers are then available to all users in the global phonebook. Especially in the case of connection of other sub-telecommunication systems, these subscribers can be integrated into the phonebook in this manner. In this way, all employees are listed in one Phonebook.

Show in Phonebook

Entries in the Global Phonebook which are not to be shown in the Phonebook will still be used for the name resolution. If a call is initiated from these numbers, the name of the user will be displayed to the called party.

Example:

A subscriber A has both a phone in his office (123) and another phone in the laboratory (456). The office telephone is now entered in the telephone book (entry: "Subscriber A, 123"), where all employees should call if they want to reach A. The laboratory telephone is also entered in the telephone book (entry: "Subscriber A (laboratory), 456"), but the entry is invisible. If A himself calls another employee from the laboratory, the name is accordingly resolved and the employee sees in his display or his caller list "Call from subscriber A (laboratory)".

How to enter additional users in the Global Phonebook

1. Open the SwyxWare Administration and choose the SwyxServer.
2. Choose the "Phonebook" folder.
3. Click with the right mouse button on the phonebook.
   The context menu will appear.
4. In the context menu, select "Add Phonebook Entry...".
   The wizard for "Add Phonebook Entry" will appear.
5. Enter the name, the phone number and, if necessary, a description for the new entry.
6. Activate the checkbox "Show in Phonebook", if the entry should be displayed in the Global Phonebook.
   If this function is deactivated, the entry will be used only for name resolution.
7. Confirm your entry with "OK".
   The new entry will appear in the Global Phonebook.

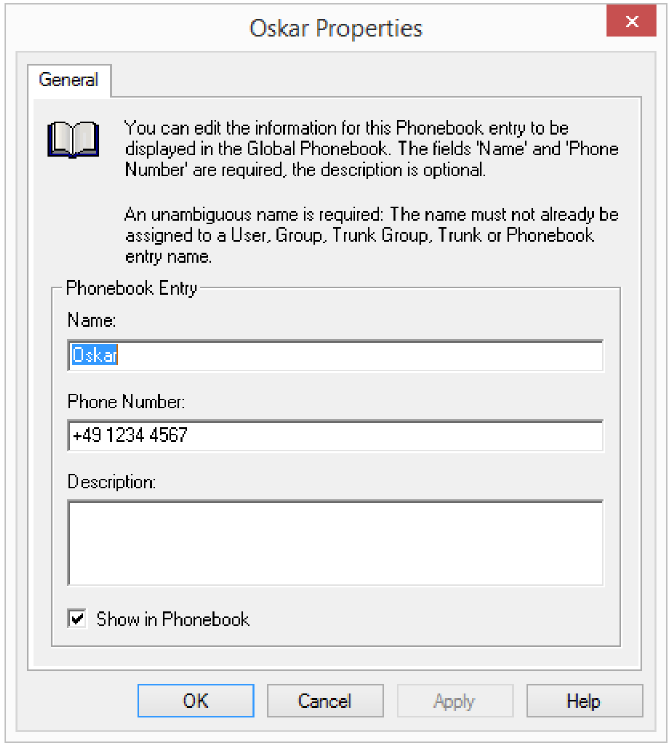
This is how you change or delete entries in the Global Phonebook

1. Open the SwyxWare Administration and choose the SwyxServer.

2 Choose the "Phonebook" folder.

3 Right-click on the entry that you would like to change or delete.

- If you would like to delete an entry, select "Delete" in the context menu.
- If you would like to change an entry, select "Properties" in the context menu..
  The "Properties" page opens.



You can edit the information for this Phonebook entry to be displayed in the Global Phonebook. The fields 'Name' and 'Phone Number' are required, the description is optional.

An unambiguous name is required: The name must not already be assigned to a User, Group, Trunk Group, Trunk or Phonebook entry name.

Phonebook Entry

Name: Oskar

Phone Number: +49 1234 4567

Description:

☑ Show in Phonebook

Enter your changes here and confirm them with "OK". The fields "Name" and "Phone number" may not remain empty, the description is optional.
Activate the checkbox "Show in Phonebook", if this entry should be displayed to all users in the phonebook. If the checkbox is not selected, the phonebook entry will only be consulted for name resolution.

The selected entry is deleted or changed.

Please note that the name of the phonebook entry must be unique within SwyxWare. This means that no other user, trunk, trunk group, group or external phonebook entry may have the same name. This is checked by the administration.

Only the additional Phonebook entries appear in the list of Phonebook entries. You cannot change or delete the entries of the users that are configured for this SwyxServer. To do so, select the "Properties" page for the corresponding user, see*11.2.2.1 The "Numbers" Tab*, Page 177.

Global abbreviated dialing

In SwyxWare, global speed dial codes (e.g. #01, #02) can be defined for use by all users of this SwyxServer. The administrator creates an entry for this purpose in the Global Phonebook, with the following format:

```
Name: #numeric character string, #, *>, number:
<number>
```

To name an example, if a speed dial of this kind (such as #11) is dialed now on a SwyxPhone, then the SwyxServer will interpret it as a name, i.e. the SwyxServer will attempt to find a phone number for the name selected and then dials it according to the standard conversion rules (trunk-dependent) with or without country code and/or area code.

Example:

There is this entry in the Global Phonebook:

Name: #11, number: +44 456 789012

If a (SwyxPhone) user dials "#11" on his or her phone, then it is interpreted as a name, and the number resolved for it out of the Global Phonebook, '+44 456 789012,' is dialed.

The exceptions are names beginning with '##'. This character string always leads to a direct call to the user himself or his script and is used, for example, to retrieve the voice messages of your own voice box with '##10'. This can then also e.g. be put on the correspondingly labeled button in the SwyxPhone D510.

All name entries starting with a number or # are forbidden in the personal phonebook.

7.6.1 THE IMPORT AND EXPORT OF PHONEBOOKS

You can import a Phonebook or a user list, such as in cases when needed from another branch office. Prerequisites for import from a list are that the entries must each be in a separate line and the fields of an entry must be in quotation marks and separated by a semi-colon.

If there is a connection via a SwyxLink trunk to the SwyxServer of the branch office, the users of the other server will automatically be visible in the Global Phonebook of this SwyxServer, and vice versa. This means there is no need to import the phonebook. See *17 SwyxLink (Server-Server Connection)*, Page 292.

To create user lists from the SwyxWare Administration, see *11.7 Export User List*, Page 212.

Example:

"Schmidt,Eva";"+442311234567 89";"Description"

"Doe,John";"+44231999888777";"Description"

Furthermore, you can export Phonebook entries to a CSV file in this format. You can specify which Phonebook entries should be exported.

How to import entries into the Global Phonebook

1 Open the SwyxWare Administration and choose the SwyxServer.

2 Click with the right mouse button on "Phonebook".

3 Select the entry "Import Phonebook..." from the context menu.
The import wizard for the Phonebook will open.

4 Select the source file:
Enter the file (*.CVS) from which the Phonebook entries should be imported.
In the lower field you will see a preview of the entries.
Click on "Next>".

5 Select the Phonebook entries to be imported:
Deactivate the checkbox in front of the entries that you do not want to import.
Click on "Next>".

6 Delete existing phonebook:
Define whether all existing Phonebook entries should be deleted before the import takes place.
Click on "Next>".

7 Add appendix to the entry name:
Indicate whether the names of the imported entries should get an appendix, and enter this appendix.

In instances like importing entries from another branch office, we recommend you include the corresponding site in order to make distinguishing among subscribers in the Global Phonebook easier for users of telephony clients.

8 Choose the update mode for the Phonebook:
The following options are available if the same entry (including the appendix) already exists:

- Update existing entry
  Overwrites the phone number and description in an existing entry.
- Rename new entry
  The new entry is automatically renamed before import takes place, e.g. ‘John Doe’ is renamed to ‘John Doe(2)’.
- Skip new entry
  Entries to be imported, which already exist in the Phonebook, will be skipped.

9 Start import process

All entries which names are already in use within SwyxWare, will be skipped during the import.

Finally, you will get an overview of the parameters entered. Confirm this with "Next>".
The selected entries will be imported.

10 To close the import wizard, click on "Finish".

How to export entries from the Global Phonebook

1 Open the SwyxWare Administration and choose the SwyxServer.

2 Click with the right mouse button on "Phonebook".

3 Select the entry "Export Phonebook..." from the context menu.
The export wizard for the Phonebook will open.

4 Deactivate the checkboxes for the phonebook entries you do not wish to export. Indicate whether the description of the entries should also be added.

5 On the next page of the wizard, define where the exported file (*.CSV) should be stored and whether an existing file with the same name should be overwritten or whether the data created should be appended to this file.
Furthermore, you can indicate whether the names of the fields (column names) in the first row of the file should also be saved.

6 Finally, you will get an overview of the parameters entered. Confirm this with "Next>".
The selected entries will be exported.

7 To close the export wizard, click on "Finish".
The telephone entries are exported according to the selected parameters.

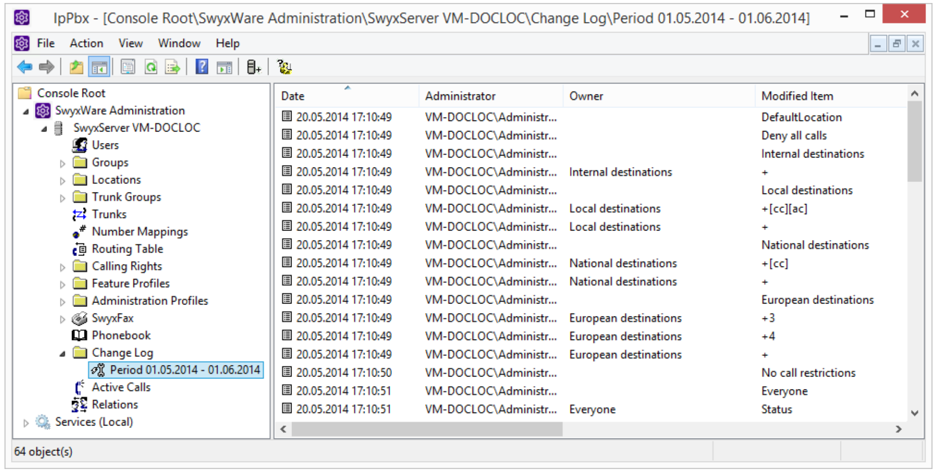
Please remember that the Global Phonebook only contains the additional entries. You can obtain the list of SwyxWare users and groups for this SwyxServer by exporting the user list, see *How to export the user list*, Page 212.

Entries from the phonebook do not show the status in the SwyxIt! Classic.

7.7 CHANGE LOG

Changes that are made to the configuration of users or trunks, or to the feature profiles or the conference rooms, are logged and saved. This means that it is always possible to track which administrator made which changes.

When saving and processing personal data, observe the respective applicable legal data protection regulations.



IpPbx - [Console Root\SwyxWare Administration\SwyxServer VM-DOCLOC\Change Log\Period 01.05.2014 - 01.06.2014]

Date	Administrator	Owner	Modified Item
20.05.2014 17:10:49	VM-DOCLOC\Administr...		DefaultLocation
20.05.2014 17:10:49	VM-DOCLOC\Administr...		Deny all calls
20.05.2014 17:10:49	VM-DOCLOC\Administr...		Internal destinations
20.05.2014 17:10:49	VM-DOCLOC\Administr...	Internal destinations	+
20.05.2014 17:10:49	VM-DOCLOC\Administr...		Local destinations
20.05.2014 17:10:49	VM-DOCLOC\Administr...	Local destinations	+[cc][ac]
20.05.2014 17:10:49	VM-DOCLOC\Administr...	Local destinations	+
20.05.2014 17:10:49	VM-DOCLOC\Administr...		National destinations
20.05.2014 17:10:49	VM-DOCLOC\Administr...	National destinations	+[cc]
20.05.2014 17:10:49	VM-DOCLOC\Administr...	National destinations	+
20.05.2014 17:10:49	VM-DOCLOC\Administr...		European destinations
20.05.2014 17:10:49	VM-DOCLOC\Administr...	European destinations	+3
20.05.2014 17:10:49	VM-DOCLOC\Administr...	European destinations	+4
20.05.2014 17:10:49	VM-DOCLOC\Administr...	European destinations	+
20.05.2014 17:10:50	VM-DOCLOC\Administr...		No call restrictions
20.05.2014 17:10:51	VM-DOCLOC\Administr...		Everyone
20.05.2014 17:10:51	VM-DOCLOC\Administr...	Everyone	Status

64 object(s)

In a SwyxWare for DataCenter and SwyxON installation, these changes are relevant for customer invoicing.

The changes are stored in the database. In the SwyxWare Administration, the changes are grouped into periods in the "Change log" directory.

In SwyxWare for DataCenter and SwyxON, this period correspond to the reporting period.

At most, the last twelve months (SwyxWare for DataCenter and SwyxON: 12 billing periods) are displayed.

The change log cannot be deleted automatically from the database. In order to meet the valid data protection regulations, it may be necessary to delete the entries manually, see *Delete change log*, Page 119.

Who can view the change log?

The change log can only be viewed by administrators who have one of the following administrator profiles:

- System Administrator
- Backoffice Administrator
- Reseller Administrator
- Customer Administrator

To display the change log directory, please use the extended view (View | Extended) in the SwyxWare Administration.

Format of the entries

The following details are recorded for each change

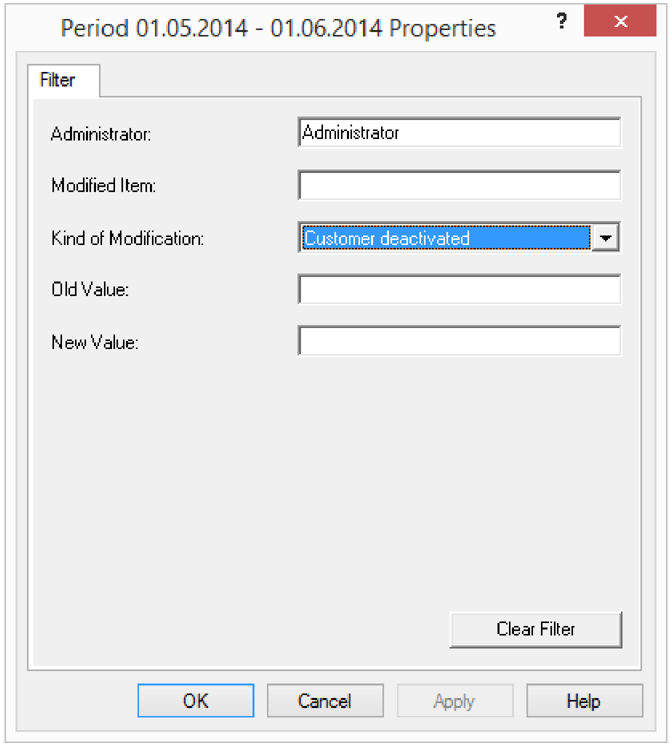
- Date of change
- User who made the change (Windows user or SwyxWare user)
- A configuration object (trunk, user, user group) that is affected by the change.
- Changed parameter (feature profile, user, voice or fax channel, conference)
- Type of change
- Change property (if applicable)
- Original value (if available)
- New value (if available)

Search in change log

You can search for entries in the displayed page (change log of a particular period).

How to search for an entry in the Change Log

1 In the context menu for the period, click on "Properties".
A filter mask will open:



Period 01.05.2014 - 01.06.2014 Properties

Administrator: Administrator

Modified Item:

Kind of Modification: Customer deactivated

Old Value:

New Value:

2 You have various filter criteria here:

- Administrator
  Enter here the name of the administrator who changed the parameter.
- Changed parameter
  Here you can give the name of the trunk or the feature profile.
- Type of change
  Select a type from the drop-down list.
- Old Value
- New Value

3 After you click "OK", this display filter is applied to all time periods, so that you can have these displayed stepwise by highlighting them in turn.

Export change log

The change log can be exported. Do this by selecting the entry "Export list..." in the context menu of the relevant period, and specifying a memory location. The file is saved, according to your specifications, as a tab- or comma-separated file.

Delete change log

A finalized period can be removed from the log.

To do so, highlight the desired time frame and select "delete" in the context menu.

Prior to deletion, a dialog window will appear recommending to back-up the corresponding period. As applicable, select the storage site and file name, then confirm by clicking on "OK."

The file is saved as a tab- or comma-separated file based on your specification. The period is removed from the change log.

⚠ It is only possible to delete periods with at least one recording.

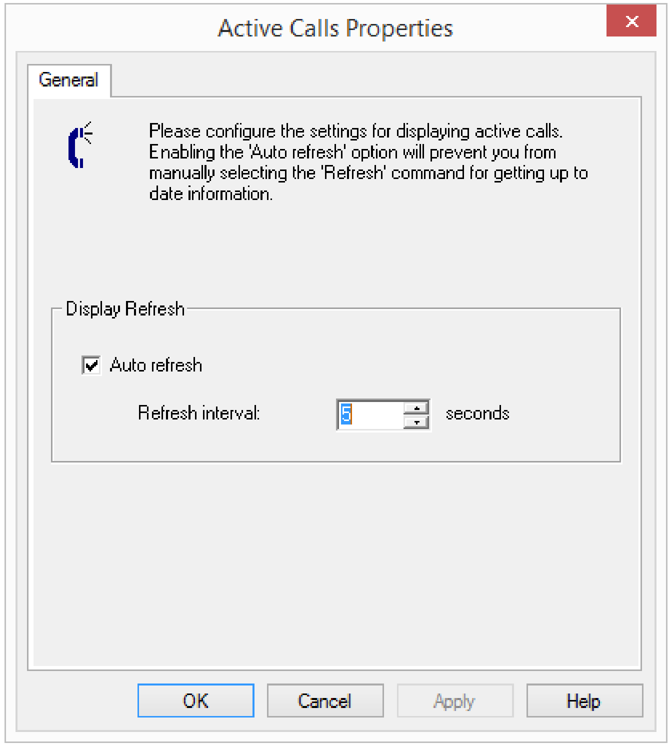
7.8 ACTIVE CALLS

In this directory, you can see which connections are active at the moment.

The following detail information can be displayed for every single connection:

- Origination Number
- Origination Name
- Called Number
- Called Name
- Destination Number
- Destination Name
- Status
- Start Time
- Duration
- Charges
- Project
- Start Trunk, (Trunk over which the call comes in)
- Destination Trunk (Trunk over which the call leaves the server)

In the context menu of "Active Calls", choose "Properties".


Active Calls Properties

General

Please configure the settings for displaying active calls. Enabling the 'Auto refresh' option will prevent you from manually selecting the 'Refresh' command for getting up to date information.

Display Refresh

☑ Auto refresh

Refresh interval: 5 seconds

Here you can set the time interval (5 to 100 seconds) for the update of this information.

If the checkbox is not selected, the display will not be updated automatically. You can update the display using the context menu.

If there are connections active, then you can interrupt them by selecting "Delete" in the context menu. Before the connection is disconnected, you must confirm a security query.

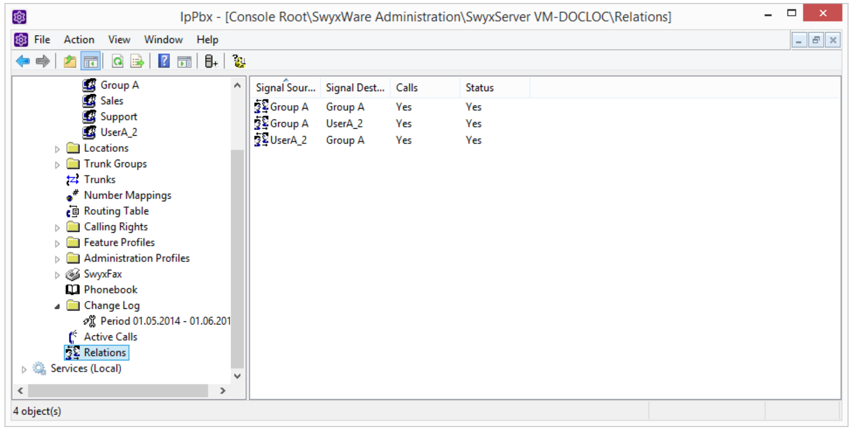
In the SwyxWare Administration "Active Calls" context menu, you'll find the option "Export list...". This allows a list of the current connections to be exported to a text file.

7.9 RELATIONSHIPS

In this directory, you can see what relationships exist between users and groups. It is not possible to edit the relationships at this point. For relationship configuration, see ***11.2.8 The "Properties..." Dialog: The "Relationships" Tab***, Page 202.

Example:

Users of the group "Group A" signal user "User A_2" about their status. Conversely, user "User A_2" signals his status to all users of the group "Group A".



Signal Sour...	Signal Dest...	Calls	Status
Group A	Group A	Yes	Yes
Group A	UserA_2	Yes	Yes
UserA_2	Group A	Yes	Yes

7.10 BACKING UP THE SWYXWARE DATABASE

You can back up the database, or restore a previously backed up database.

In SwyxON the backup of the database is provided by the service provider.

You can use the program "IpPbxConfig.exe" to back up the SwyxWare database locally and restore it at a later time. You'll find the program in the SwyxWare program directory. Backing up the database is done by making an entry the command line:

```
IpPbxConfig.exe /backup [/file "<Backup File>"]
```

If you call the parameter "/backup" without the parameter "/file", a database backup will be generated in the SwyxWare standard backup directory. A unique file name is automatically assigned (e.g. "IpPbx-Backup-2010-10-18-15-56-07.dat"). If you specify a file name without a path in the parameter '"/file", the file is likewise written to the above directory. When an absolute path is input, the file is stored as specified. A file of the same name already present is not overwritten.

To restore the SwyxWare database, enter in the command line

```
IpPbxConfig.exe /restore /file "<Backup File>"
```

To stop Swyx services automatically and restart them automatically after the backup is restored, use the additional parameters "/stop" and "/start".

Note that the database server must have writing access on the directory used for the backup, and reading access for the recovery of the database.

Backing up the database during an update

The Configurations Wizard automatically updates the existing local database of an older SwyxWare installation. In addition, a backup copy of the existing database is made before the update takes place. You will find this backup copy in the SwyxWare standard backup directory.

If the database is on a different computer, then please back this up before the update.

> Please note that in a SwyxWare for DataCenter installation it is not possible to do an automatic database backup before an update by the Configuration Wizards. The administrator must back up the database himself before an update, using the backup systems of the database server.

Please refer to the Knowledgebase for more advice on database maintenance

https://service.swyx.net/hc/de

7.11 UNINSTALLING

SwyxWare is uninstalled via the Control Panel.

> Deinstallation must be implemented by the SwyxWare service provider in SwyxON.

To uninstall SwyxWare

1. If the Active Directory extension is installed, remove this before uninstalling with the help of the program IpPbxAdExtConfig in the SwyxWare program directory.
   See *Removal of the Active Directory extension*, Page 425.
2. Open the Windows Control Panel (Start | Settings | Control Panel).
3. Double-click on "Software".
4. Select the option "SwyxWare" found under "Change or Remove Program".
5. Click on "Remove".
6. Confirm the message asking whether you really want to uninstall SwyxWare with "Yes".
   The uninstall process will be carried out automatically.
7. Click on "Close" to close the window.
   When uninstalling, files that were used in conjunction with SwyxWare but weren't copied to the server during installation will not be removed.
   The database holding the SwyxServer user and configuration data is not deleted, regardless of whether this is installed on the same computer or on another computer. If necessary, it should be deleted manually.
8. Delete database:
   - In an environment with SwyxWare for DataCenter, you uninstall the database as for the installation according to the information from Microsoft.
   - To delete the database of a SwyxWare, uninstall the Microsoft Data Engine and then delete the files
     ippbx.mdf
     ippbx_log.ldf
     in the directory C:\Programs\Microsoft SQL Server\data. C:\Programs\Microsoft SQL Server is the MSDE installation directory.
     Once you have uninstalled the Microsoft Data Engine, you must restart your computer before you can reinstall MSDE and SwyxWare.

8 LOCATIONS

Location is a user and trunk group property, which groups together site-dependent parameters.

A location represents all site-dependent parameters such as codes, prefixes and time zones, but also PBX settings such as the public line access prefix.

With the help of these location parameters, dialed numbers are composed into a canonical number during operation. Call permissions and routings are then compared with this canonical number within SwyxWare.

Example:

A subscriber in London (country code 44, area code 20, public line access 0) dials the sequence of digits "0123456". The dialed number is then composed as follows:

The leading zero is interpreted as a public line access, and the sequence "123456" is left. As the first digit is no longer 0, the sequence is interpreted as a local number. With the location data, this then gives the canonical number "+4420123456". The routing records and Calling Rights are then checked for this number.

In the SwyxWare Administration you'll find the configured locations in the "Location" directory, with their respective associated users, groups and trunks under them.

8.1 EMERGENCY CALL DETECTION

STOP

In the case of emergency calls, a location determination is always necessary.
This function can only be performed via your telephony provider (e.g. provision of number ranges with corresponding area codes).
Contact your provider to ensure that the caller's location is determined correctly.

Emergency calls in Germany, Austria and Switzerland

In the DACH countries, the numbers 110 and 112 are reserved for emergency calls. If 110 or 112 is dialed, the following special treatments are applied:

- Any configured number suppression is ignored. The outgoing call number is always signaled.
- If the user has not configured a public phone number, a valid phone number of the SIP trunk used is signaled to ensure that the call is not rejected by the provider.
- Existing configured or licensed trunk channel limits are ignored. The call is always delivered.
- If more than one external trunk is configured and available, preference is always given to the trunk whose assigned location matches the location of the emergency caller.

As of SwyxWare version 14.00, the numbers 110 and 112 cannot be assigned to internal users.
If an emergency number has already been assigned to one or more users, make sure that there are no assignments for these numbers in your configuration.

8.2 DEFAULT LOCATION

The default location is the location assigned to a new user. In SwyxWare Administration, it has a different icon compared to the other locations. If you want to assign all other new users a different location as default, then, in the properties of the new default location, select the option "Set this Location as the default Location" (*8.4.1 The "General" Tab*, Page 124).

How to create a new location

1 Start SwyxWare Administration.

2 Click "Locations" with the right mouse button to open the context menu.

3 Select "Add location..."
The wizard for adding a location will open.

4 Location name:
Enter the name of the location and, if applicable, a brief description. The name must be unambiguous within SwyxWare.
If you would like the location you are creating to be used as the default for all users and trunk groups subsequently set up, activate the "Set this Location as the Default Location" checkbox.
Click on "Next>".

5 Codes and prefixes for the location
The following parameters specify how numbers dialed by a user (or trunk group) of this location are to be interpreted by SwyxWare.

Example:

A user has the location London (codes 44, 20, prefixes 00, 0, public line access prefix 0). This user now dials 0456789. SwyxWare interprets the first 0 as the public line access prefix and the number sequence 456789 as a local number. This results in the canonical number +4420 456789.

Own country code
Here you define your country code. For the United Kingdom, it is '44'.
Own area code
Enter your area code here without the preceding '0', for example, '20' for London or '161' for Manchester.
Prefix for international calls
The code for international calls is entered in this field. In Germany, this code is '00'.
Prefix for long distance calls
Here you enter the digit(s) which must be dialed in order to make a long distance call. In Germany, the digit required for long distance calls is always '0'.
Click on "Next>".

6 Private Branch Exchange related Properties:
Public Line Access
This is the number that SwyxWare users must first dial in order to make external calls. Default value: ‘0’.
You are able to enter several Public Line Accesses separated by a semicolon, e.g. to differentiate private and business calls using a different Public Line Access.
Route undeliverable calls to Internal Number:
If a call is directed to a number, which is within the number range of SwyxServer but has not been assigned to a user, this call will be forwarded to the number listed here. You can enter the number directly or select it from the list of SwyxWare numbers. It can also be a number of a connected SwyxServer.
Click on "Next>".

7 Time zone:
Select the time zone this location is assigned to. The time zone is required for evaluating time-dependent restrictions, for example for routing.

Example:

A Trunk Group (e. g. ISDN, Location Germany) is enabled only from 6 p.m. to 8 p.m. If a user in England now calls at 7:15 p.m. local time a number in Germany (German local time 8:15 p.m.), the ISDN Trunk Group is disabled for this call.

8.3 PRIVATE AND BUSINESS CALLS

Several different public line access prefixes can be configured for a location (*How to create a new location*, Page 122). This allows you to distinguish between business and private calls. Different routings can be defined for these different public line access prefixes (*14 Routing*, Page 239).

Analyzing calls by different public line access prefixes allows you to later create call detail records (*App. A: Call Detail Records (CDR)*, Page 398).

8.4 EDIT LOCATION

You can also change existing locations, e.g. by adding further public line access prefixes or deleting them.

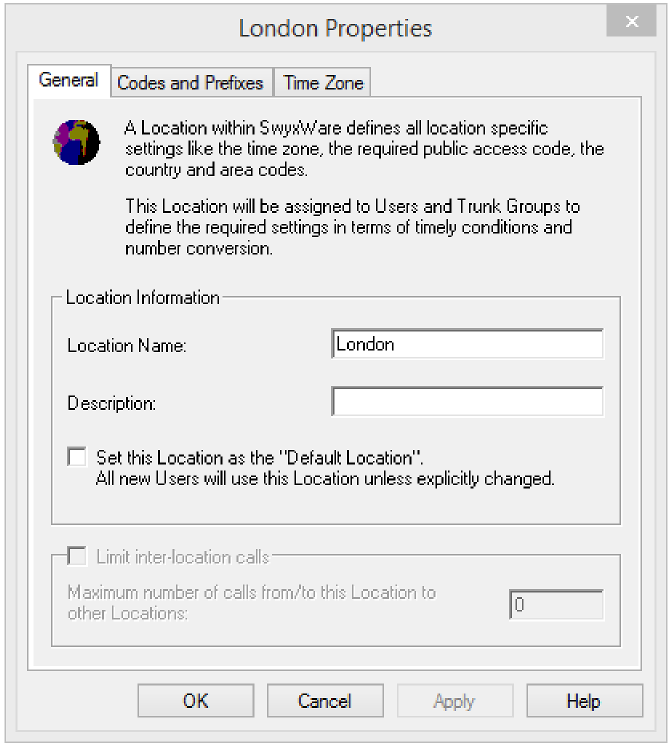
How to change an existing location

1 Start SwyxWare Administration.

2 Open the list of locations.

3 In the context menu for the location, select "Properties".
You can now configure the settings for the location as described below.

8.4.1 THE "GENERAL" TAB


London Properties

General | Codes and Prefixes | Time Zone

A Location within SwyxWare defines all location specific settings like the time zone, the required public access code, the country and area codes.

This Location will be assigned to Users and Trunk Groups to define the required settings in terms of timely conditions and number conversion.

Location Information

Location Name: London

Description:

□ Set this Location as the "Default Location".
All new Users will use this Location unless explicitly changed.

□ Limit inter-location calls

Maximum number of calls from/to this Location to other Locations: 0

Enter the general information for the location on this tab:

Location Information

The name of the location and, if applicable, a brief description can be found here. The name must be unambiguous within SwyxWare.

Activate the checkbox "Set this Location as the Default Location" if you want this location to be used as default for all users and trunk groups subsequently created.

Restricting calls between the locations

The connection between two locations is always limited. You can limit the number of possible connections between the two locations, in order e.g. to reserve bandwidth of this connection for other applications too. In this case too - as in the limiting of calls over a trunk - between 24 kbit/s (compressed) and 84 kbit/s (uncompressed) bandwidth is needed per call.

The voice compression must be configured individually for each user; for SwyxPhone that can be defined in the SwyxWare Administration, for SwyxIt! it can only be configured locally in the client.

Select this checkbox, if you want to allow only a certain number of calls from/to this location. Enter the maximum number of connections for this location.

Connections are not only direct calls but also all connections to SwyxServer e.g. to a script. For instance, if you hold a call and start a second call, you have **two** connections to the SwyxServer.

Conference and limitation of the calls to a location

As many lines are needed for a conference as there are participants, plus two (maximum) further lines for setting up the conference.

If you want to use the conference functionality, specify the number of calls to this location as at least 4; for scenarios with more than one location, configure at least 5. These numbers apply for a three-way conference. The number is correspondingly increased for each further participant in a conference.

Example:

At location A a subscriber initiates a conference with

3 participants from his location A,

5 participants who are at location B and

2 further participants from location C, as well as

1 external participant.

The following number of lines is needed in each case:

Location A: 6 lines (1 initiator + 3 participants, 2 lines for the conference setup)

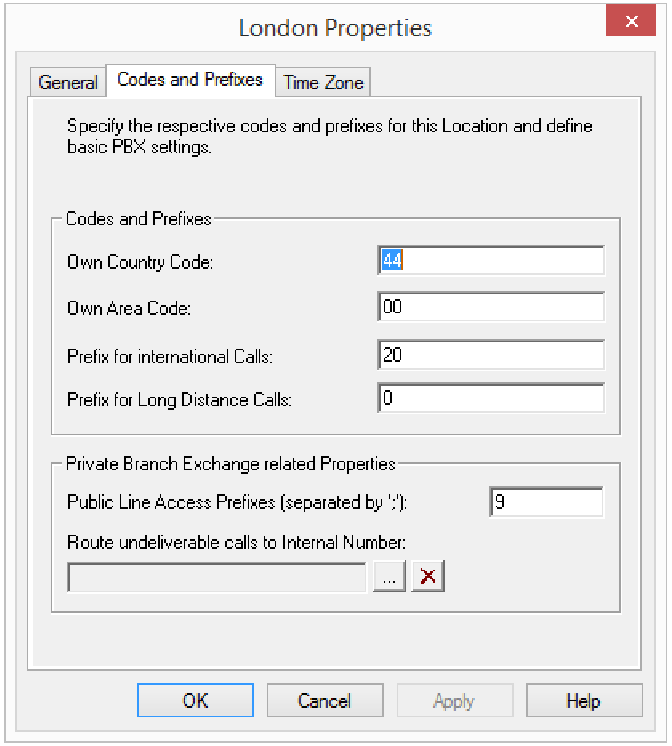
Location B: 5 Lines

Location C: 2 Lines

Location of the trunk over which the external call comes in: 1 Line

If all participants in a conference are assigned to the same location, a maximum of one line is needed for setting up the conference. This means that with 7 participants at location A, the limit must be at least 8 lines.

8.4.2 THE "CODES AND PREFIXES" TAB


London Properties

Specify the respective codes and prefixes for this Location and define basic PBX settings.

Codes and Prefixes

Own Country Code: 44

Own Area Code: 00

Prefix for international Calls: 20

Prefix for Long Distance Calls: 0

Private Branch Exchange related Properties

Public Line Access Prefixes (separated by ';'): 9

Route undeliverable calls to Internal Number:

Enter the codes, prefixes and public line access prefixes for the location on this tab.

The following parameters specify how numbers dialed by a user (or trunk group) of this location are to be interpreted by SwyxWare.

Example:

A user has the location London (codes 44, 20, prefixes 00, 0, public line access prefix 0). This user now dials 0456789. SwyxWare interprets the first 0 as the public line access prefix and the number sequence 456789 as a local number. This results in the canonical number +4420 456789.

Codes and Prefixes

- Own country code
  Here you define your country code. For the United Kingdom, it is '44’.
- Own area code
  Enter your area code here without the preceding '0', for example, '20' for London or '161' for Manchester.
- Prefix for international calls
  The code for international calls is entered in this field. In Germany, this code is '00'.
- Prefix for long distance calls
  Here you enter the digit(s) which must be dialed in order to make a long distance call. In Germany, the digit required for long distance calls is always '0'.

Phone Numbers in the USA

In the USA, local numbers always consist of 10 digits preceded by the country code for the USA (1):

Own country code: 1

Own area code: The first three digits of the local, ten-digit number

Prefix for international calls: 011

Prefix for long distance calls: 1

Phone Numbers in Switzerland

In Switzerland, a subscriber number always consists of an area code and a subscriber line number.

Therefore, the following general SwyxServer settings must be made within the SwyxWare Administration:

Own country code: 41

Own area code: according to the local public network without the preceding zero.

Prefix for international calls: 00

Prefix for long distance calls: 0

In Switzerland you must also note that you must always enter the complete number including the long distance code and the area code for outgoing calls, even local calls. SwyxWare will automatically fulfill these requirements if the user initiates a call with the canonical number (+41 ...).

Private Branch Exchange related Properties:

- Public Line Access

  This is the number that SwyxWare users must first dial in order to make external calls. Default value: '0'.

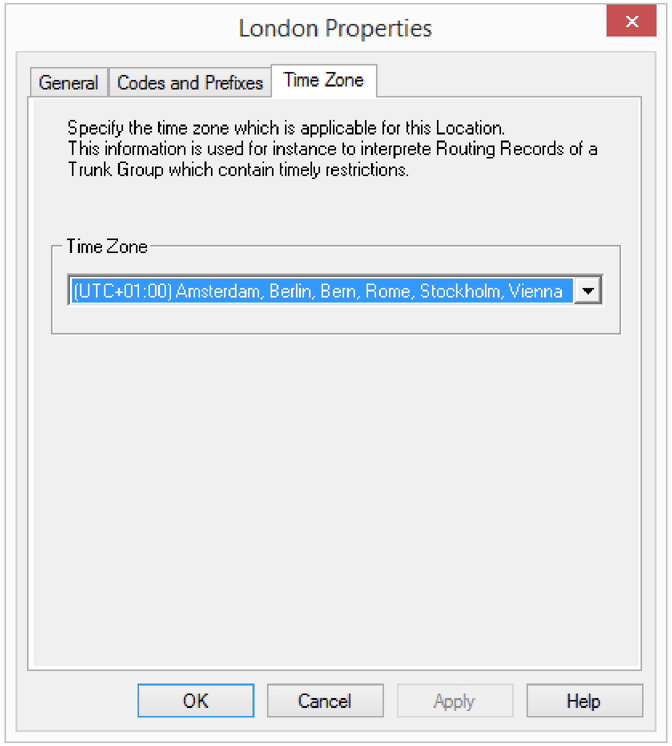
  You are able to enter several Public Line Accesses separated by a semicolon, e.g. to differentiate private and business calls using a different Public Line Access.

- Route undeliverable calls to Internal Number:

  If a call is directed to a number which is within the number range of SwyxServer but has not been assigned to a user, this call will be forwarded to the number listed here. You can enter the number directly or select it from the list of SwyxWare numbers. It can also be a number of a connected SwyxServer.

> If the number selected here is no longer present, an error message is displayed until you have selected another number for the routing of undeliverable calls. This can be the case, for example, if the number has been deleted, or you have selected the number of a connected server to which there is no longer a connection.

8.4.3 THE "TIME ZONE" TAB



Specify the time zone which is applicable for this Location.
This information is used for instance to interprete Routing Records of a Trunk Group which contain timely restrictions.

Time Zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Enter the time zone for the location on this tab.

The time zone this location is assigned to is given here. The time zone is required for evaluating time-dependent restrictions, for example for routing.

Example:

A Trunk Group (e. g. ISDN, Location Germany) is enabled only from 6 p.m. to 8 p.m. If a user in England now calls at 7:15 p.m. local time a number in Germany (German local time 8:15 p.m.), the ISDN Trunk Group is disabled for this call.

How to delete a location

1 Start SwyxWare Administration.

2 Open the list of locations.

3 In the context menu for the location, select "Delete".
The location is deleted if it is not referenced by a user or a trunk group.

If the location is still in use, you cannot delete it. In this case please ensure that the location is assigned neither to a user nor to a trunk group by checking the "Location" column in the list of users / trunk groups and changing the configuration of the user or trunk group if necessary.

For a better overview you can sort users and trunk groups by location in the SwyxWare Administration.

9 PROFILES

Several User Rights are combined to Profiles

In SwyxWare different Calling Rights or the usage of special features can be assigned to a User. A differentiation is made between

- Call Permissions
  The permission to make calls e.g. with certain numbers or via dedicated trunks.
  See *9.1 Call Permissions*, Page 128.
- Feature Profile
  A feature profile defines which individual functions are generally available to this user.
  See *9.2 Function profile*, Page 137.
- Administration profile
  A user can be assigned an administration profile. This defines what rights the user has when he connects to his SwyxServer with the help of the SwyxWare Administration.
  See *9.3 Administration profiles*, Page 143.

9.1 CALL PERMISSIONS

Call rights are defined within SwyxWare for users and trunk groups.

For each user, these rights define

- where a call may be made to (e.g. local),
- with what public line access (e.g. private or business) and
- via which trunk group this call may go out.

The call permissions are defined using so-called profiles, which are then assigned to individual users or trunk groups.

Such a profile can be composed of several individual permissions. But each user and each trunk group has only precisely one call permission.

Various simple call permissions are offered in the standard installation (*9.1.1 Call permissions in the standard installation.*, Page 134).

If there are special requirements for call permissions, which the standard profiles do not satisfy, the SwyxWare administrator can define his own call permissions, customized specifically for the needs of the installation.

To define call permissions in detail, see *9.1.2 Create Call Permission*, Page 134.

Call Permissions and Routing

The call permissions are independent of the routing (*14 Routing*, Page 239). Routings define how a call leaves the system, i.e. how it can be forwarded depending on the trunk group and the time conditions. Routes are a property of the SwyxServer.

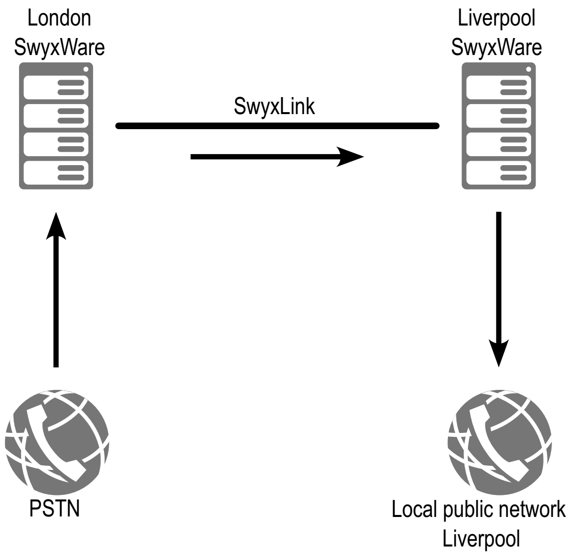
Call permissions are user and/or trunk group characteristics. They define which rights are granted to an incoming call, i.e. if and how a call will be transmitted.

Call permission of a user

A user's call permission states what calling rights this user has within SwyxWare. For example, he can have the right to make national calls, but not international ones. If a SwyxWare user forwards a call (e.g. with a script), the forwarded call receives the user's rights.

Example:

There is a SwyxWare installation with two servers, one in Liverpool and one in Liverpool. The two SwyxServers are connected to each other over a SwyxLink.



The called user in London has the right to telephone via ISDN within London (locally), but not nationally:

```
Entry in the user's call permission:
Allow call +4420*; Trunk group "ISDN London"
```

The called user in London also has the right to make calls to Liverpool via a SwyxLink trunk "SwyxLink London-Liverpool":

```
Entry in the user's call permission:
Allow call +44151*; Trunk group "SwyxLinkLondon-
Liverpool"
```

In its call permission, the trunk group "SwyxLink London-Liverpool" allows local calls via ISDN. (This is configured on the Liverpool side!):

```
Entry in the call permissions of the trunk group
"SwyxLink London-Liverpool" on the Liverpool side:
Allow call +44151*; Trunk group "ISDN Liverpool"
```

If the SwyxWare user is called and if a route to the Liverpool local public network is set up, then a caller calling in London is routed via the SwyxLink trunk to Liverpool and there into the Liverpool local public network.

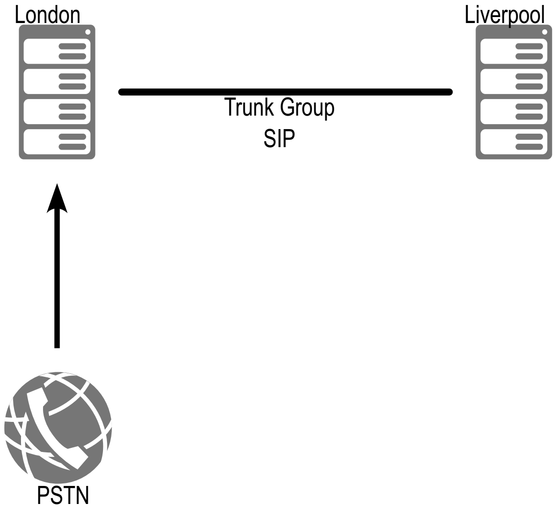
Call permission of a trunk group

A call permission is assigned to each trunk group. All calls that come in via a trunk group inherit the call permission of this trunk group.

Thus, if an incoming call cannot be assigned to any user within the SwyxWare system, it must leave this system (e.g. via another trunk group). For this forwarding, it receives the call permission of the trunk group via which it came into this system.

Example 1

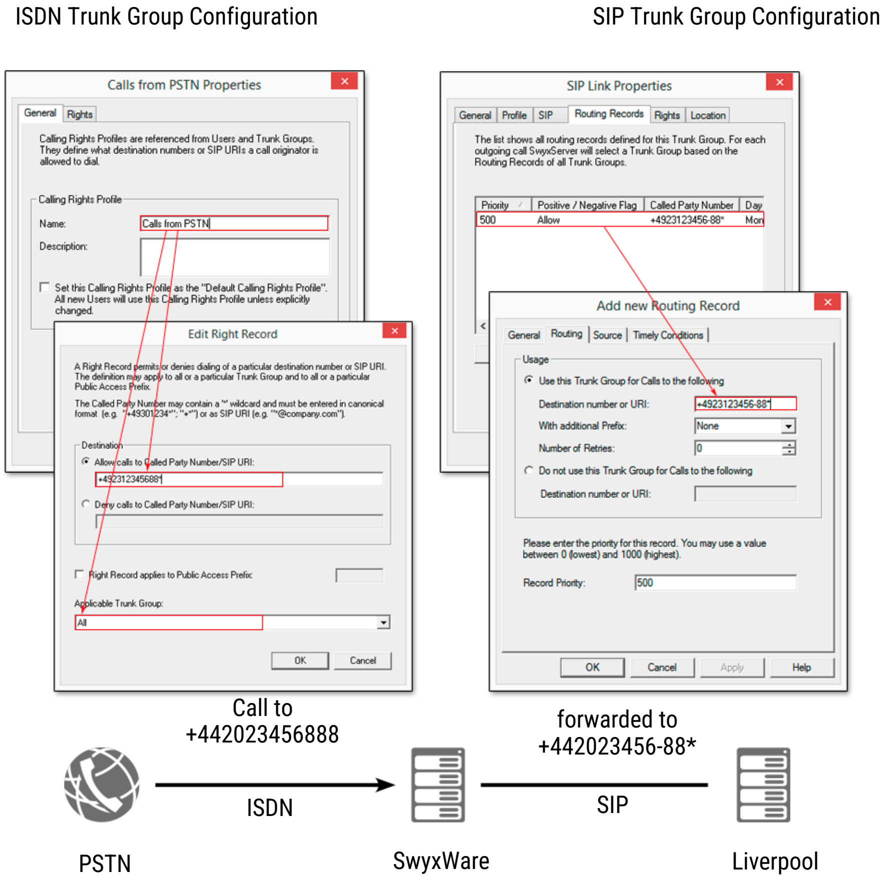
There is a SwyxWare installation with two servers, one in Liverpool and one in Liverpool. The two SwyxServers are connected to each other over a SIP trunk.



A call comes in from the public network via the ISDN trunk group to the London number 020 23456-888. This number is not assigned to a user within SwyxWare, but there is forwarding for the number range 020 234567-88* via a SIP trunk group. In order for this call to be forwarded via this SIP trunk group, the corresponding permission must exist in the ISDN trunk group, which has received the call, i.e. the call that has been received by the trunk group must have the permission to leave the system via the SIP trunk:

```
Entry in the call permission of the ISDN trunk group:
```

```
Allow call +4420 23456-88*; Trunk group "SIP"
```



Calls from PSTN Properties

General | Rights

Calling Rights Profiles are referenced from Users and Trunk Groups. They define what destination numbers or SIP URIs a call originator is allowed to dial.

Calling Rights Profile

Name: Calls from PSTN

Description:

□ Set this Calling Rights Profile as the "Default Calling Rights Profile". All new Users will use this Calling Rights Profile unless explicitly changed.

Edit Right Record

A Right Record permits or denies dialing of a particular destination number or SIP URI. The definition may apply to all or a particular Trunk Group and to all or a particular Public Access Prefix.

The Called Party Number may contain a "*" wildcard and must be entered in canonical format (e.g. "+49301234*"; "+*") or as SIP URI (e.g. "*@company.com").

Destination

● Allow calls to Called Party Number/SIP URI: +492312345688*

○ Deny calls to Called Party Number/SIP URI:

□ Right Record applies to Public Access Prefix:

Applicable Trunk Group: All

OK | Cancel

SIP Link Properties

General | Profile | SIP | Routing Records | Rights | Location

The list shows all routing records defined for this Trunk Group. For each outgoing call SwyxServer will select a Trunk Group based on the Routing Records of all Trunk Groups.

Priority	Positive / Negative Flag	Called Party Number	Day
500	Allow	+4923123456-88*	Mon

Add new Routing Record

General | Routing | Source | Timely Conditions

Usage

● Use this Trunk Group for Calls to the following

Destination number or URI: +4923123456-88*

With additional Prefix: None

Number of Retries: 0

○ Do not use this Trunk Group for Calls to the following

Destination number or URI:

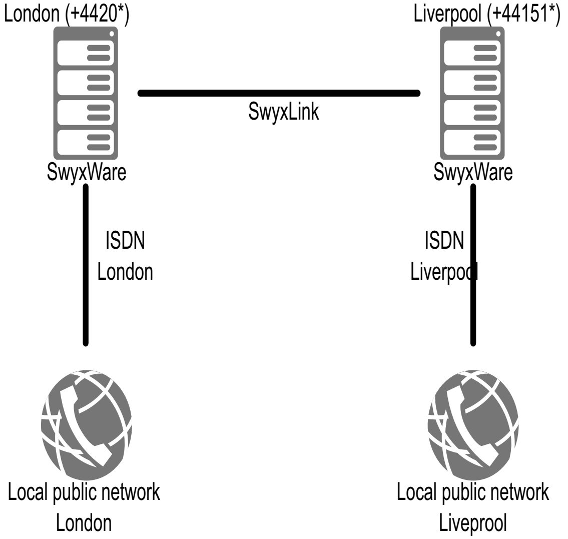
Please enter the priority for this record. You may use a value between 0 (lowest) and 1000 (highest).

Record Priority: 500

OK | Cancel | Apply | Help

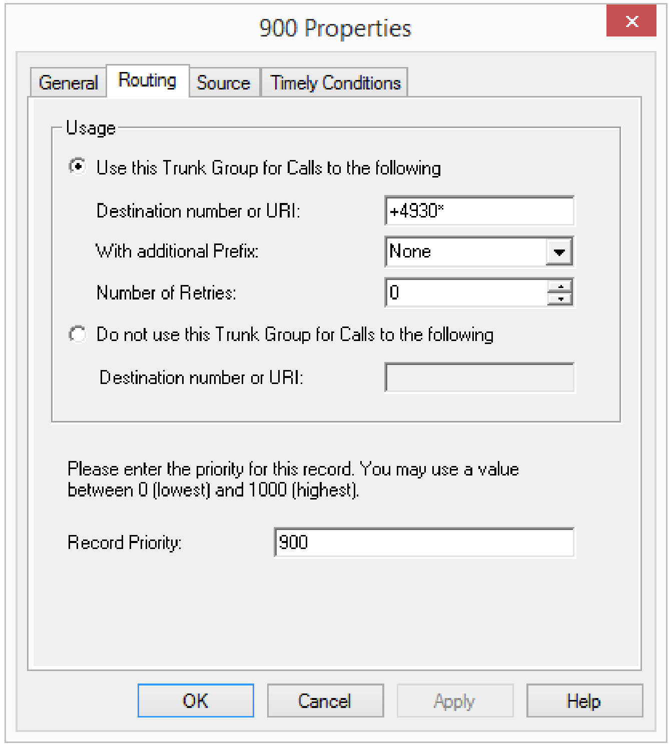
Example 2

There is a SwyxWare installation with two SwyxServers, one in London and one in Liverpool. The two SwyxServers are connected to each other over a SwyxLink.



In order that calls to Liverpool can in principle go via this SwyxLink, a routing record must be set up on the server in London to forward all calls to Liverpool via the SwyxLink to Liverpool.

```
Routing record in London:
Allow call +44 151*; Trunk group "SwyxLink London-
Liverpool"; Priority 900
```



Usage

● Use this Trunk Group for Calls to the following

Destination number or URI: +4930*

With additional Prefix: None

Number of Retries: 0

○ Do not use this Trunk Group for Calls to the following

Destination number or URI:

Please enter the priority for this record. You may use a value between 0 (lowest) and 1000 (highest).

Record Priority: 900

A user has the location London (prefix: 020). In the first place he can make local calls in London via ISDN:

```
Entry in the user's call permission:
Allow call +44,20*; Trunk group "ISDN London"
```

He also has the right to make calls to Liverpool via a SwyxLink trunk "SwyxLink London-Liverpool":

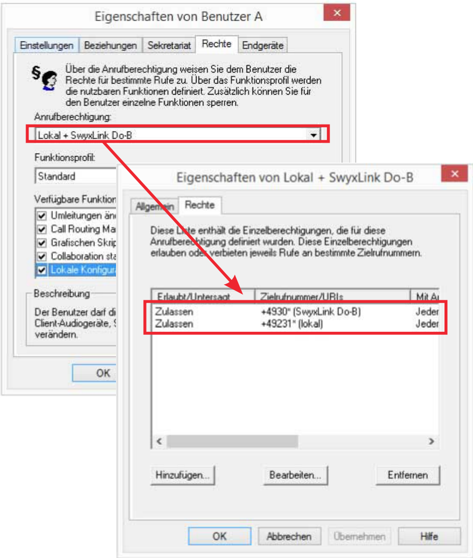
```
Entry in the user's call permission:
Allow call +44151*; Trunk group "SwyxLinkLondon-
Liverpool"
```

In its call permission, the trunk group "SwyxLink London-Liverpool" allows local calls via ISDN into the Liverpool local public network. (This is configured on the Liverpool side!):

```
Entry in the call permissions of the trunk group
"SwyxLink London-Liverpool" on the Liverpool side:
Allow call +44 151*; Trunk group "ISDN Liverpool"
```

The user in London can thus call Liverpool via the SwyxLink, and there telephone locally via ISDN into the public telephone network.

Profile User A



Über die Anrufberechtigung weisen Sie dem Benutzer die Rechte für bestimmte Rufe zu. Über das Funktionsprofil werden die nutzbaren Funktionen definiert. Zusätzlich können Sie für den Benutzer einzelne Funktionen sperren.

Anrufberechtigung: Lokal + SwyxLink Do-B

Funktionsprofil: Standard

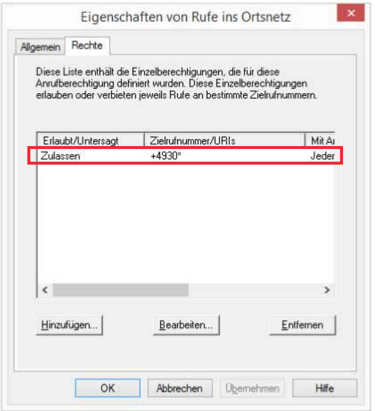
☑ Umleitungen än
☑ Call Routing Ma
☑ Grafischen Skrip
☑ Collaboration sta
☑ Lokale Konfigura

Der Benutzer darf di Client-Audiogeräte, S verändern.

Diese Liste enthält die Einzelberechtigungen, die für diese Anrufberechtigung definiert wurden. Diese Einzelberechtigungen erlauben oder verbieten jeweils Rufe an bestimmte Zielrufnummern.

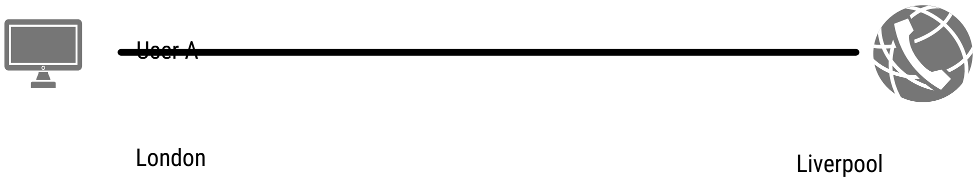
Erlaubt/Untersagt	Zielrufnummer/URIs	Mit A
Zulassen	+4930* (SwyxLink Do-B)	Jeder
Zulassen	+49231* (lokal)	Jeder

ProfileSwyxLink



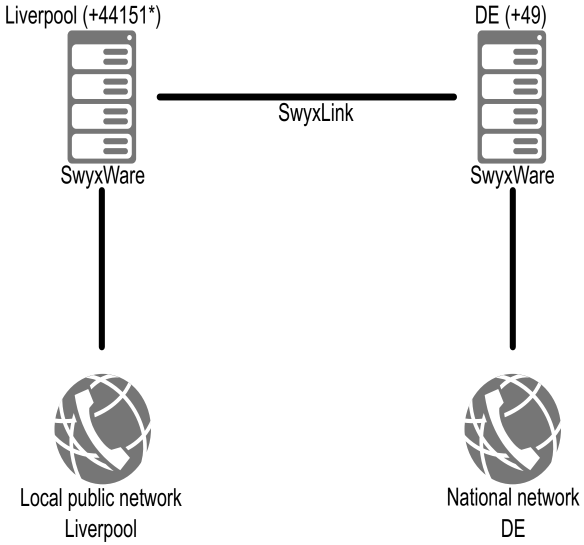
Diese Liste enthält die Einzelberechtigungen, die für diese Anrufberechtigung definiert wurden. Diese Einzelberechtigungen erlauben oder verbieten jeweils Rufe an bestimmte Zielrufnummern.

Erlaubt/Untersagt	Zielrufnummer/URIs	Mit A
Zulassen	+4930*	Jeder



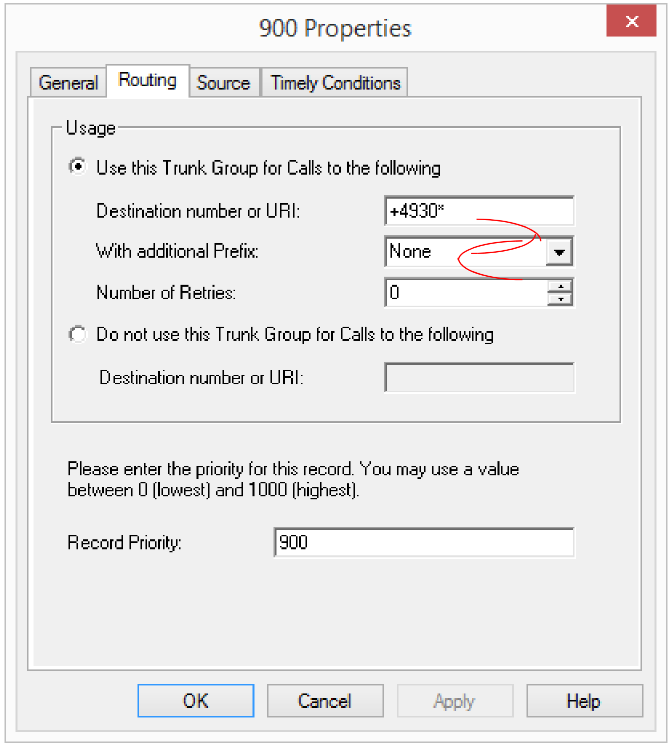
Example 3:

There is a SwyxWare installation with two SwyxServers, one in Liverpool and one in Germany. The two SwyxServers are connected to each other over a SwyxLink.



To be able to make calls to England via this SwyxLink, a routing record must be set up on the server in Liverpool to forward all calls to Germany (prefix +49) via the SwyxLink to Germany.

```
Routing record in Liverpool:
Allow call +49*; Trunk group "SwyxLink DE"; Priority
900
```



900 Properties

General | Routing | Source | Timely Conditions

Usage

● Use this Trunk Group for Calls to the following

Destination number or URI: +4930*

With additional Prefix: None

Number of Retries: 0

○ Do not use this Trunk Group for Calls to the following

Destination number or URI:

Please enter the priority for this record. You may use a value between 0 (lowest) and 1000 (highest).

Record Priority: 900

The user has the right at his Liverpool location to telephone internally.

```
Entry in the user's call permission:
Deny call +*; Trunk group "All"
Allow call *; Trunk group "All"
```

But he has the right to phone Germany (prefix 49) via SwyxLink:

```
Entry in the user's call permission:
Allow call +49*; Trunk group "SwyxLink DE"
```

In Germany the "SwyxLink DE" is configured in such a way that calls coming in via this trunk group have the right to initiate national calls via ISDN into the public network:

```
Entry in the call permission for SwyxLink DE in
Germany:
```

```
Allow call +49*; Trunk group "ISDN DE"
```

The user in Liverpool is now able to call Germany via SwyxLink, and there to make calls into the entire national telephone network; but he cannot call locally in Liverpool.

Such a constellation could e. g. make sense for a support employee, who only makes phone calls to Germany.

For private calls, a further permission can be set up with a public line access for private calls. e. g.

```
Entry in the user's call permission:
Allow call +44151*; Trunk group "ISDN Liverpool";
Public line access 8 (private)
```

Call permission for SwyxLink trunk groups

SwyxLink trunk groups represent the connection between two SwyxWare installations. Every SwyxLink trunk is configured on both sides, on one side locally and on the other side remotely (*16 SIP Links*, Page 278).

A call that takes place over this connection inherits the call permission of the side on which it leaves this trunk; or, to put it another way, it receives the call permission of the trunk group which routes this call into SwyxWare.

Example:

There are two SwyxWare installations in London and Liverpool, which are connected to a SwyxLink "London-Liverpool".

The SwyxLink "London-Liverpool" is managed locally in London and remotely in Liverpool.

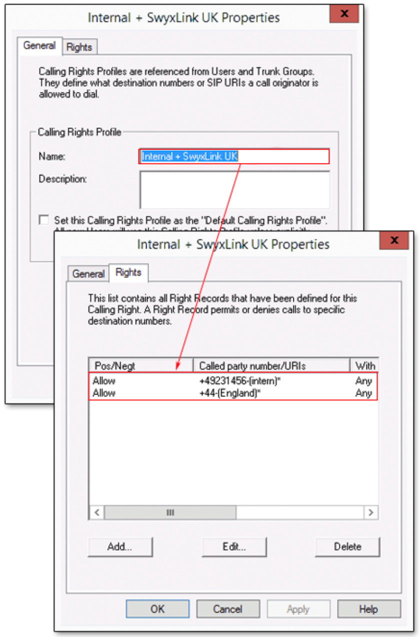
In London there is a call permission for the relevant trunk group, allowing only internal calls:

```
Entry in the call permission of SwyxLink "London-
Liverpool" in London:
Allow call *; Trunk group "All"
Deny call +*; Trunk group "All"
```

In Liverpool a profile was set up for the assigned trunk group, allowing calls via ISDN into the local network in Liverpool.

Profile User A

Profile SwyxLink



Internal + SwyxLink UK Properties

Calling Rights Profiles are referenced from Users and Trunk Groups. They define what destination numbers or SIP URIs a call originator is allowed to dial.

Calling Rights Profile

Name: Internal + SwyxLink UK

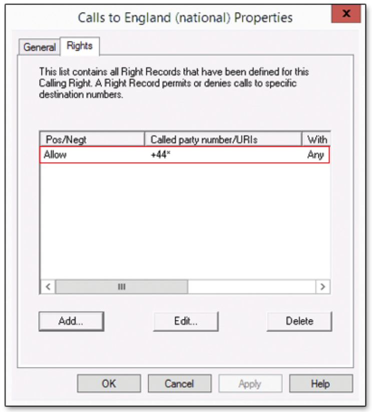
Description:

□ Set this Calling Rights Profile as the "Default Calling Rights Profile".

Internal + SwyxLink UK Properties

This list contains all Right Records that have been defined for this Calling Right. A Right Record permits or denies calls to specific destination numbers.

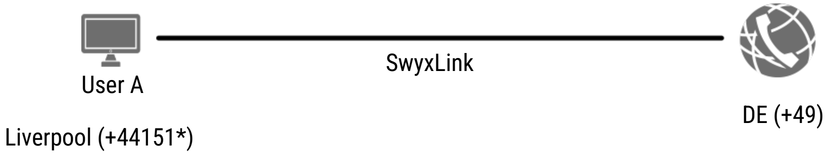
Pos/Negt	Called party number/URIs	With
Allow	+49231456-(intern)*	Any
Allow	+44-(England)*	Any



Calls to England (national) Properties

This list contains all Right Records that have been defined for this Calling Right. A Right Record permits or denies calls to specific destination numbers.

Pos/Negt	Called party number/URIs	With
Allow	+44*	Any



```
Entry in the call permission of SwyxLink "London-
Liverpool" in Liverpool:
Allow call +44151*; Trunk group "ISDN Liverpool"
```

If a user from London now calls Liverpool via the SwyxLink "London-Liverpool", his call can be forwarded there into the Liverpool local network (call permission on the Liverpool side!).

On the other hand, if a user from Liverpool now calls London via the SwyxLink "London-Liverpool", his call can only be forwarded to an inter-

nal employee, and not into the Liverpool local network (call permission on the Liverpool side!).

9.1.1 CALL PERMISSIONS IN THE STANDARD INSTALLATION.

In the standard installation, a few simple call permissions are already available:

Call Permission	Description
Deny all calls	No outgoing calls can be initiated. This configuration can make sense for a user (script) who should only be called.
Internal calls	Only calls to internal SwyxWare subscribers can be initiated.
Calls into local public network	Only local calls, i. e. within the area code, can be made
National destinations	Only calls within a country (same country code) can be initiated.
European destinations	Only calls within Europe can be made, i.e. the country code must start with 3 or 4.
No call restrictions	There are no call restrictions.

Call permissions that were granted in an earlier SwyxWare version (internal, local, national and international) are mapped on to the corresponding call permissions during an update to the current version. Only the rights that were assigned to the user are considered here, but not the rights that he may have received within the scope of a group membership.

9.1.2 CREATE CALL PERMISSION

If there are special requirements for call permissions, which the standard profiles do not satisfy, the SwyxWare administrator can define his own call permissions, customized specifically for the needs of the installation.

You can specify the call permissions in very precisely differentiated detail when defining them. Various parameters are available for selection for this purpose:

- Allow or deny call
  You can formulate the call permission positively (allow) or negatively (deny).
- Destination numbers or URIs
  You can use dummies in the definition, e.g. for country and local area codes, or '*' for any digits or letters (*10.5 Placeholder*, Page 152).
- Public line access codes
  You can use various public line access codes, e.g. in order to differentiate between private and business calls.
- Use of the trunk group
  Depending on the trunk group used for the outgoing call, e.g. ISDN or SIP, other call permissions can be specified.
  With the help of the trunk permission, individual users can also be forced to use e.g. only certain trunks.

  Example:

  The normal office worker is permitted only to telephone over the SIP trunk, while the manager is also permitted - e.g. if the SIP connection fails - to phone using the ISDN access to the public network.

This is how you define a call permission

1. Open the SwyxWare Administration and choose the SwyxServer.
2. On the left side of the SwyxWare administration window, click with the right mouse button on "Call Permissions" and select the entry "Add Call Permission..." in the context menu.
   The "Add New Call Permission" wizard appears.
3. Name and description of the call permission
   Enter a unique name and a short description for the profile.
4. Click on "Next>".
5. Add single permissions to call permissions
   You can specify several permissions for this profile here.
6. Click on "Add".

7 The following window appears:

- Destination:

  Activate the option "Allow calls to Called Party number/SIP URI" or "Deny calls to Called Party number/SIP URI" . For each entry in the profile, you can only either allow calls (positive) or deny them (negative).

  Specify the call numbers or URIs in the relevant fields. You can use dummies here, e.g. in order to define larger ranges (e. g. all calls in the Netherlands +31* or all calls to *@company.com).

  If you want, define a public line access for this right. If the option is not activated, the definition applies to all public line accesses.

  Several public line access codes separated by semicolons can be entered here.

  Example:

  All calls to numbers beginning with +44900 (activation of "Allow calls to Called Party number/SIP URI" and +44900) are allowed, but only for private purposes. For private calls you have specified a second public line access, e. g. "8" (**8 Locations**, Page 122).*

  This allows you to recognize all calls to 0900 numbers as private numbers in the Call Detail Records (CDR), and analyze them accordingly.

- Applicable Trunk group:

  You can specify here whether all trunk groups or only one particular trunk group may be used for the permission defined above.

  Example:

  All calls for private purposes (activation of "Allow calls to Called Party number/SIP URI" and +) will be allowed. For private calls you have specified a second public line access, e. g. "8" (**8 Locations**, Page 122).*

  Now you can specify that for capacity reasons, only one particular trunk group may be used for private calls, e. g. the SIP trunk group.

8 Then click on "OK".
The new call permission is created and is immediately available.

> ⚠ When defining the profile for gateways, use a dummy e. g. [AC] for the local area code (***10.5 Placeholder***, Page 152). When a call is forwarded via a gateway, the local area code of the relevant gateway is used for the permission, and not the local area code of the user location. This means that a standard profile (e. g. local calls) can be used at various locations.

Example:

If you want to create a call permission that basically allows local calls via all trunk groups, but only for a specific public line access (in this case '8'), you configure the following parameters:

*Allow call +[CC][AC]**

Trunk group "All"

Public line access 8 (private)

You can then use this profile independently of the trunk group's location. In each case, the code which was defined for the trunk group's location is used.

9.1.3 CHANGE CALL PERMISSION

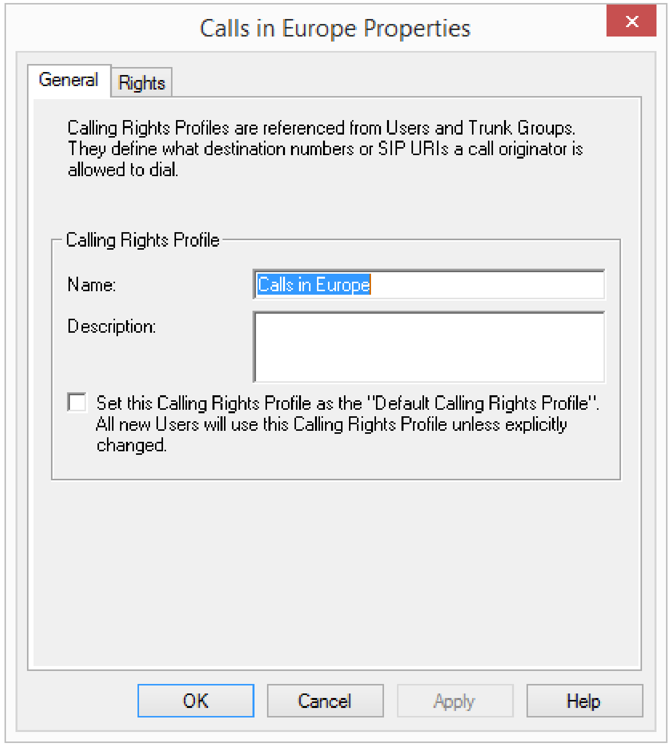
You can change, expand or delete an existing call permission at any time. The changed profile is valid at once for all users and trunk groups who use this call permission.

This is how you edit a call permission

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare administration window, open the directory "Right Profiles" and double-click on the profile you want to edit.
The "Properties of..." window will appear.

9.1.3.1 PROPERTIES CALL PERMISSION GENERAL TAB


Calls in Europe Properties

Calling Rights Profiles are referenced from Users and Trunk Groups. They define what destination numbers or SIP URIs a call originator is allowed to dial.

Calling Rights Profile

Name: Calls in Europe

Description:

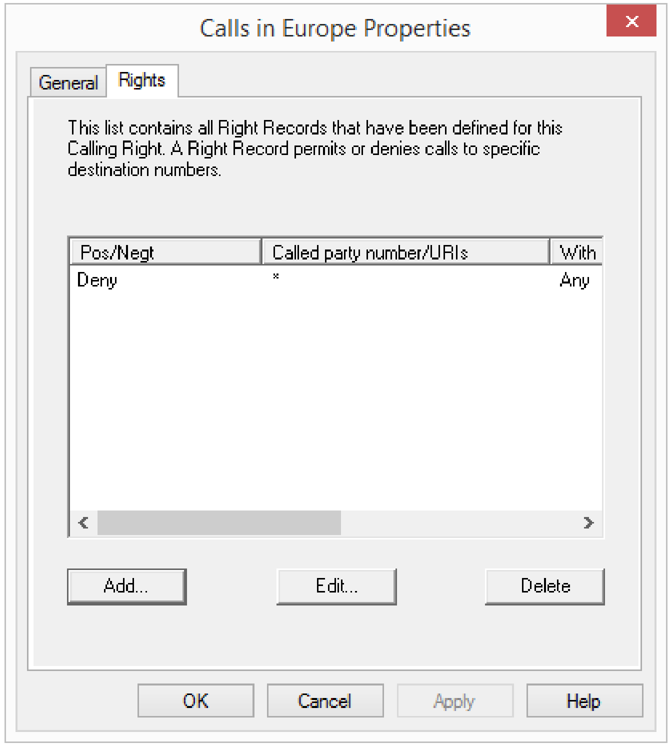
□ Set this Calling Rights Profile as the "Default Calling Rights Profile". All new Users will use this Calling Rights Profile unless explicitly changed.

On this tab you will find the name and a brief description of the call permission.

Default Calling Right

If you want to use this profile as the standard profile for all new users, activate the relevant checkbox.

9.1.3.2 CALLING RIGHT - THE "RIGHTS" TAB


Calls in Europe Properties

This list contains all Right Records that have been defined for this Calling Right. A Right Record permits or denies calls to specific destination numbers.

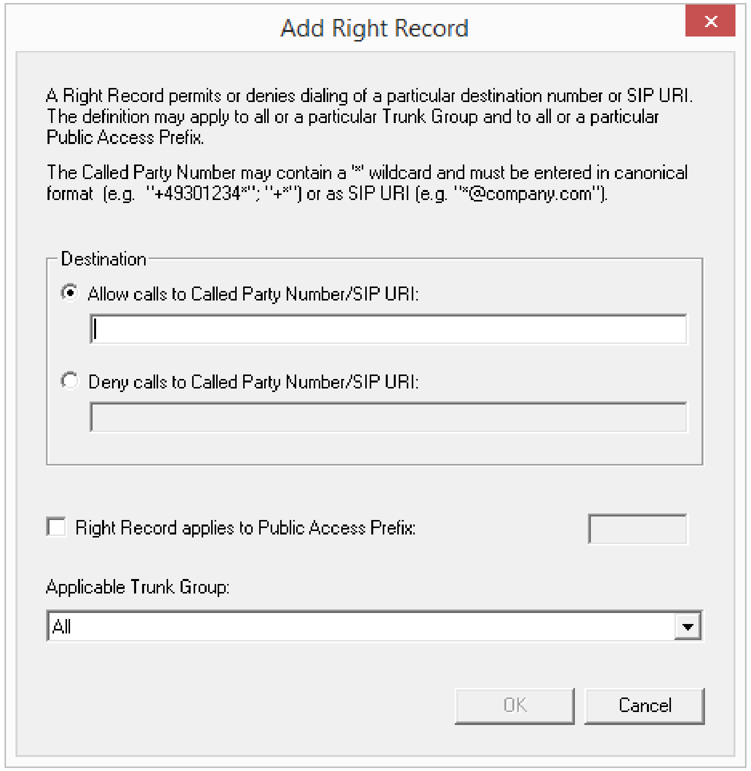
Pos/Negt	Called party number/URIs	With
Deny	*	Any

This tab holds the list of individual permissions covered by this profile. You can add to, change or delete the individual entries here.

This is how you change an individual profile entry

1 Click on "Edit" or "Add...".
The following window appears:

- Destination:
Activate the option "Allow calls to Called Party number/SIP URI" or "Deny calls to Called Party number/SIP URI" . For each entry in the profile, you can only either allow calls (positive) or deny them (negative).
Specify the call numbers or URIs in the relevant fields. You can use dummies here, e. g. in order to define larger ranges (e. g. all calls



A Right Record permits or denies dialing of a particular destination number or SIP URI. The definition may apply to all or a particular Trunk Group and to all or a particular Public Access Prefix.

The Called Party Number may contain a "*" wildcard and must be entered in canonical format (e.g. "+49301234*"; "+*") or as SIP URI (e.g. "*@company.com").

Destination

● Allow calls to Called Party Number/SIP URI:

○ Deny calls to Called Party Number/SIP URI:

□ Right Record applies to Public Access Prefix:

Applicable Trunk Group: All

in the Netherlands +31* or all calls to *@company.com).
If you want, define a public line access for this right. If the option is not activated, the definition applies to all public line accesses.

Example:

All calls to numbers beginning with +44900 (activation of "Allow calls to Called Party number/SIP URI" and +44900) are allowed, but only for private purposes. For private calls you have specified a second public line access, e.g. "8" (see chapter 5, Sites,page98).*

This allows you to recognize all calls to 0900 numbers as private numbers in the Call Detail Records (CDR), and analyze them accordingly.

- Applicable Trunk group:
  You can specify here whether all trunk groups or only one particular trunk group may be used for the permission defined above.

Example:

All calls for private purposes (activation of "Allow calls to Called Party number/SIP URI" and +) will be allowed. For private calls you have specified a second public line access, e.g. "8" (see chapter 5, Sites,page98).*

Now you can specify that for capacity reasons, only one particular trunk group may be used for private calls, e. g. the SIP trunk group.

2 Then click on "OK".
The new or amended call permission is created and is immediately available.

This is how you delete a call permission

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare administration window, open the directory "Call Permissions" and open the context menu of the right record you want to delete.

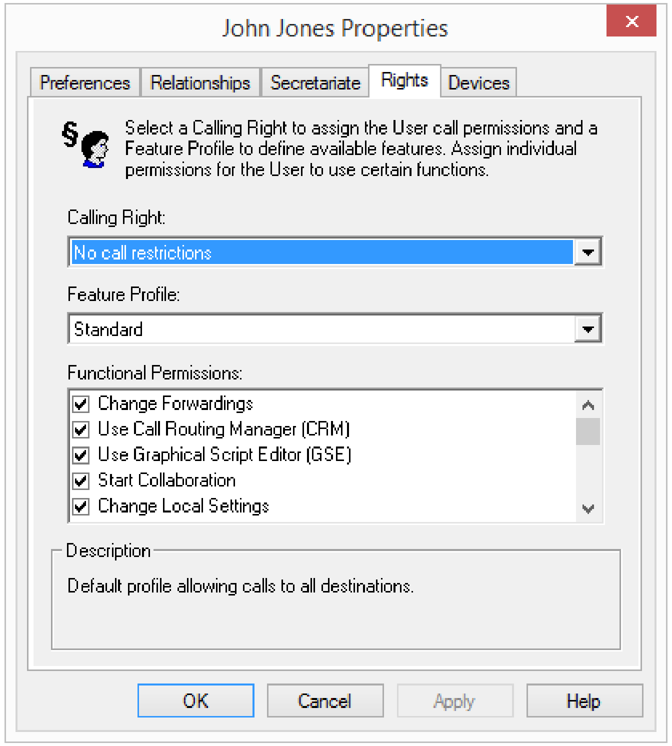
3 Select "Delete".
If this call permission is still being used by a user or a trunk group, you cannot delete the profile.
If the call permission is not in use, it is deleted.

9.2 FUNCTION PROFILE

The feature profile determines which SwyxWare functions a user can use. The profile "Standard" is pre-configured and includes all licensed options. It will be used for all new created users.

> If the directory "Feature profiles" cannot be seen, activate the entry "Advanced" in the menu bar under "View".

When creating a user, the administrator selects a feature profile for this user from the drop-down list. The feature profile contains the functional range available to the user. A different predefined feature profile can subsequently be selected at any time by the administrator. The change takes place as soon as the administrator confirms the user's properties with "OK".



John Jones Properties

Select a Calling Right to assign the User call permissions and a Feature Profile to define available features. Assign individual permissions for the User to use certain functions.

Calling Right: No call restrictions

Feature Profile: Standard

Functional Permissions:

☑ Change Forwardings
☑ Use Call Routing Manager (CRM)
☑ Use Graphical Script Editor (GSE)
☑ Start Collaboration
☑ Change Local Settings

Description: Default profile allowing calls to all destinations.

It is possible here to grant the user rights to use advanced SwyxWare functionalities. To change the feature profile, select another profile from the selection list or create a new feature profile.

9.2.1 FEATURE PROFILES FOR ONLINE LICENSING

See *2 Online Licensing*, Page 21

9.2.2 FEATURE PROFILES IN THE STANDARD INSTALLATION

In SwyxWare the feature profile "Standard" is pre-configured.. This profile contains all available functions, depending on the option packs installed (*3.2.6 Options and Option Packs*, Page 33).

This profile is also assigned to the users "Conference", and "Operator".

You can create profiles which provide a different combination of functions for a user. You can also specify whether this profile should be used as the default profile for all new users.

The following functions are available for selection when creating a feature profile:

Functions	Explanation
SwyxBasicFunctionality	The user is able to log in, to make phone calls and to forward calls. This functionality is the basis for all other functions.
SwyxCTI	Control a SwyxPhone or a SwyxIt! with CTI SwyxIt! (SwyxWare component)
SwyxFax	The user can use SwyxFax, either directly as a printer or the SwyxFax Client. Requirement: SwyxFax license or SwyxProfessional option
SwyxVoicemail	The user can use a voice box, i.e. the user has an answering machine that can record voice messages and forward them to the user as an e-mail. The user can check these messages by remote enquiry, and also remotely configure his announcements and Call Forwarding Unconditional. (Integral part of the SwyxWare)
SwyxRecord	The user can record calls spontaneously, i.e. during a call with SwyxIt!, the conversation or parts of it can be recorded spontaneously. Requirement: SwyxRecord or SwyxProfessional option

Functions	Explanation
SwyxBCR	Basic Call Routing The user can use the Call Routing Manager (create scripts and run them). Requirement: SwyxBCR*- or SwyxProfessional option
SwyxECR	Extended call routing With the help use of the Graphical Script Editor., the user can define a complex set of rules and represent it graphically. Requirement: SwyxECR or SwyxProfessional option
SwyxAdHocConference	The user (SwyxIt! and SwyxPhone) can initiate conferences spontaneously. Requirement: SwyxConference license resp. SwyxProfessional option
SystemPhone	The user can use a system phone as a terminal in addition to SwyxIt!. In this context, a system phone is a device which is not listed in the SwyxPhone Whitelist and therefore requires a SwyxPhone license. Requirement: SwyxPhone License
SwyxMonitor	A user with the corresponding authorization can intrude on calls of this user. Requirement: SwyxMonitor Option
Swyx Connector for Notes	The user can use SwyxIt! with Lotus/IBM/HCL Notes. Requirement: Swyx Option Pack for IBM Notes
Swyx VisualContacts	The user can use Swyx VisualContacts. Requirement: Licensed option Swyx VisualContacts
Swyx Connector for DATEV	The user can use Swyx Connector for DATEV. Requirement: Licensed option Swyx Connector for DATEV
Swyx VisualGroups	The user can use Swyx VisualGroups. Requirement: Licensed option Swyx VisualGroups Standard or Enhanced
Feature Pack for Certified SIP phones	This option offers the possibility to use extended SwyxWare functionalities, such as CTI, integration of the global phone book and various system phone functions, with certified third-party SIP phones. The scope of functions depends on the provider and telephone model.
SwyxCTI+	With CTI SwyxIt!, a third person device or an external phone can be controlled via its phone number. Requirement: Licensed option SwyxCTI+

SwyxBCR is included in SwyxWare.

The usage of SwyxWare functions is defined in the user properties, and is not immediately identical to the feature profile.

Example 1:

*A user's profile must contain the SwyxECR feature, so that a script (which was created e.g. by the administrator for this user with use of the Graphical Script Editor.) can also be used by this user. To prevent this user from changing the script himself, Graphical Script Editor is deactivated, see **11.2.10 The "Properties..." Dialog: The "Rights" Tab**, Page 203.*

9.2.3 FEATURE PROFILES IN SWYXWARE FOR DATACENTER AND SWYXON

You are already supplied with a few simple feature profiles in the standard installation of SwyxWare for DataCenter and SwyxON. The feature profiles are predefined by the provider or the reseller. Each feature profile is individually listed in the invoice.

Feature profiles normally differ in their functional range. On the other hand, such feature profiles may also differ only in the price to be calculated later.

SwyxWare for DataCenter

Feature Profile	Description
Deactivated (Deactivated)	User with this profile cannot log in and therefore they are not able to make phone calls. Their Call Forwarding is also not activated. So it is possible to save the configuration for users, which are absent for a long time. These users will be reported separately.
Plain (Plain)	This profile only includes the basic functions, i.e. users with this profile are only allowed to place calls. ● SwyxBasicFunctionality
Minimal	This profile contains the basic functions for a telephony user: ● SwyxBasicFunctionality ● System Phone ● SwyxVoicemail
Standard	This profile contains the functions for a SwyxWare user: ● SwyxBasicFunctionality ● SwyxFax ● SwyxCTI ● System Phone ● SwyxBCR (Basic Call Routing) ● SwyxAdHocConference ● SwyxVoicemail
Advanced (Advanced)	This profile contains all available functions: ● SwyxBasicFunctionality ● SwyxCTI ● SwyxFax ● SwyxVoicemail ● SwyxRecord ● SwyxBCR (Basic Call Routing) ● SwyxECR (Extended Call Routing) ● SwyxAdHocConference* ● SystemPhone ● SwyxMonitor ● Swyx Connector for Notes ● Swyx VisualContacts ● Swyx Connector for DATEV ● Swyx VisualContacts Standard/Enhanced ● SwyxCTI+

Example:

Feature profile 'Standard' has the same scope as feature profile 'Standard Special Promotion'. The standard price is calculated for feature profile 'Standard', while the feature profile 'Standard Special Promotion' is at a reduced rate. The provider can now differentiate in the invoice between these two technically identical profiles, and charge the customer different rates.

The administrator of a customer (customer administrator) can deactivate functions that are included in a feature profile for a specific user. If a function is not included in this profile, it cannot be activated by the customer administrator.

Example:

The feature profile 'Standard' includes Call Routing Manager and SwyxFax, while the feature profile 'Minimal' includes neither of these functions. Now, the customer administrator assigns the "Standard" profile to the user, so he/she can use SwyxFax . Because of this, the customer administrator deactivates the Call Routing Manager checkbox in the field "Functional Permissions and Features overview" on the "Rights" tab. Now the user can use SwyxFax, but not edit redirection rules himself with Call Routing Manager. Rules created by the administrator with the Call Rout-

ing Manager can be activated for this user, however. The feature profile 'Standard' is entered in Reporting and charged by the provider.

Example, 'Use use of the Graphical Script Editor.':

The 'Standard' profile does not include use of the Graphical Script Editor., the 'Advanced' profile does contain the use of the Graphical Script Editor..

If the administrator chooses the 'Standard' profile for User A, he cannot permit him use of the Graphical Script Editor., since it is not included in the profile. If he assigns User B the 'Advanced' profile, the administrator can make use of the Graphical Script Editor. available for User B, by activating use of the Graphical Script Editor. in the administration. This allows User B to create or edit scripts with use of the Graphical Script Editor.. If Graphical Script Editor is not activated in the administration (e.g. if the user only has a SwyxPhone), scripts created e.g. by the administrator may still run for this user. This is not possible for User A.

The profile "Advanced" will be assigned to new users. If you want to assign automatically a different profile to new users, e.g. the profile "Minimal", you have to configure this in the properties of the profile "Minimal".

The profile "No Features" is assigned to the preconfigured users "Conference" ; the profile "Advanced" to the user "Operator".

SwyxON

Feature Profile	Description
Deactivated (Deactivated)	User with this profile cannot log in and therefore they are not able to make phone calls. Their Call Forwarding is also not activated. The usage report records the total number of users ordered, even if these users are allocated the function profile "Deactivated".

Feature Profile	Description
Feature Profile M	This profile contains the functions for a SwyxWare user: ● SwyxBasicFunctionality ● SwyxCTI ● SwyxCTI+ ● SwyxBCR (Basic Call Routing) ● SwyxAdHocConference ● SwyxVoicemail
Feature Profile L	This profile contains the functions for a SwyxWare user: ● SwyxBasicFunctionality ● SwyxCTI ● SwyxCTI+ ● SwyxFax ● SwyxBCR (Basic Call Routing) ● SwyxECR (Extended Call Routing) ● SwyxAdHocConference ● SwyxVoicemail

9.2.4 MODIFY A FEATURE PROFILE

You are not authorized to edit the defined function profiles in online licensing and in SwyxON or to create your own function profiles. For more information, please contact your provider.

This is how you create a feature profile

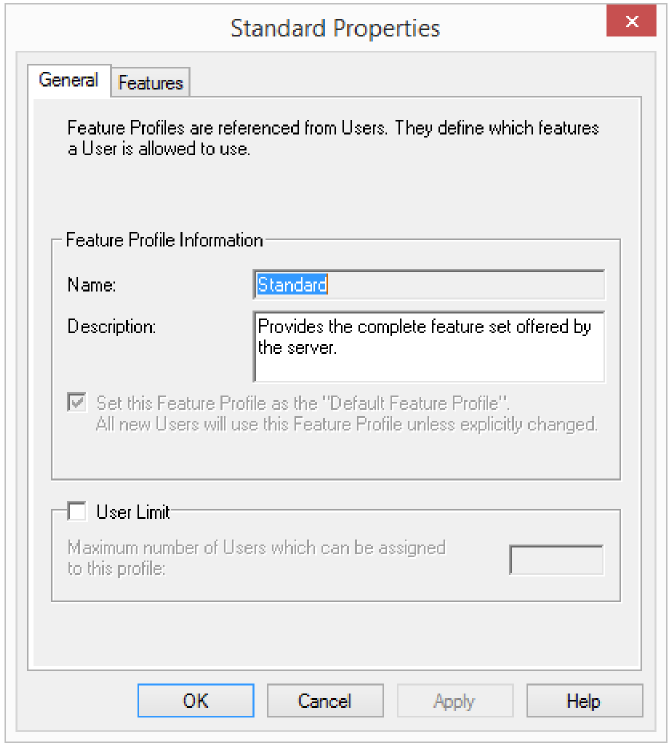
1 Right-click on "Feature Profiles" and choose the entry "Add feature profile...".
The wizard for creating a feature profile will appear.

2 Name of the feature profile
Enter a name for the new feature profile, and if necessary a description.
Specify whether this profile should be used as the standard profile for all new users.
Click on "Next>".

3 Available Functions

Activate the functions for the profile.
Click "Finish".
The new feature profile is created and is immediately available.

9.2.4.1 FEATURE PROFILE - TAB "GENERAL"



Standard Properties

General | Features

Feature Profiles are referenced from Users. They define which features a User is allowed to use.

Feature Profile Information

Name: Standard

Description: Provides the complete feature set offered by the server.

☑ Set this Feature Profile as the "Default Feature Profile". All new Users will use this Feature Profile unless explicitly changed.

☐ User Limit

Maximum number of Users which can be assigned to this profile:

On this tab you will find the name and a brief description of the feature profile.

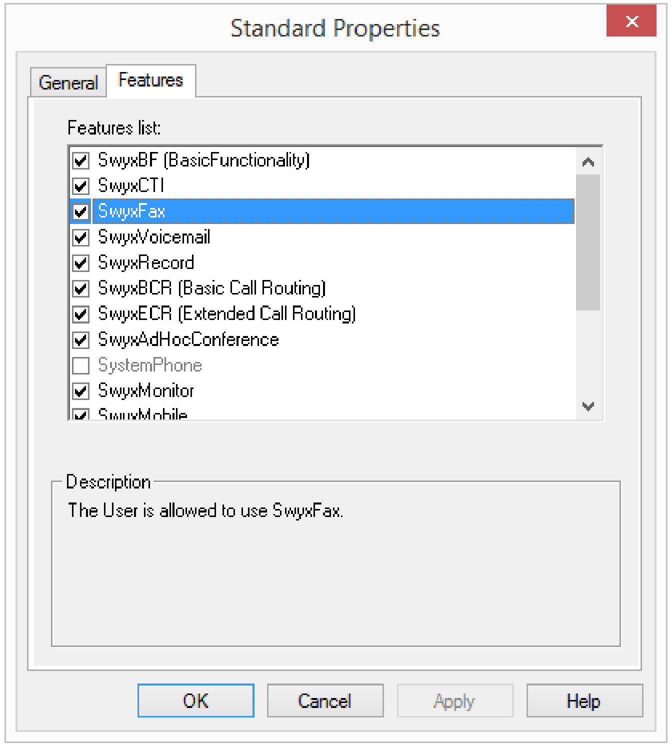
Default Feature Profile

If you want to use this profile as the standard profile for all new users, activate the relevant checkbox.

User limit

Activate the option "User limit" if only a specified number of users may use this profile. In this case, specify the maximum number of users who are allowed to have this profile.

9.2.4.2 FEATURE PROFILE - THE "FEATURES" TAB



Standard Properties

General | Features

Features list:

☑ SwyxBF (BasicFunctionality)
☑ SwyxCTI
☑ SwyxFax
☑ SwyxVoicemail
☑ SwyxRecord
☑ SwyxBCR (Basic Call Routing)
☑ SwyxECR (Extended Call Routing)
☑ SwyxAdHocConference
☐ SystemPhone
☑ SwyxMonitor
☑ SwyxMobile

Description

The User is allowed to use SwyxFax.

This tab contains the list of all available functions. You can activate and deactivate individual functions for this profile here.

This is how you edit a feature profile

1 Open the list of feature profiles.

2 Right-click on the feature profile you want to edit, or select "Properties" in the context menu.
In each case, the "Properties of..." window will appear.
On the "General" tab you can change the name and description of the profile. You can also specify whether this profile should be used as the standard profile for all new users. If you activate this checkbox, this option is unset for the previous standard profile.

3 Switch to the "Features" tab to change the functions allowed for this profile.

If you want to assign a different profile to several users, you can also highlight these in the list in Administration and use Drag & Drop to move them to the new profile.

This is how you delete a feature profile

1 Please ensure that this feature profile is not assigned to a user.

2 To do this, highlight in SwyxWare Administration the profile you want to delete.
If there are any users left using this profile (on the right side of the administration), please assign a new profile to these users.

3 Switch to the "Features" tab to change the functions allowed for this profile.

4 If this profile is no longer assigned to any users, click with the right mouse button on the profile in the tree structure, and select "Delete" in the context menu.
When you confirm the query with "Yes", the profile is deleted.

9.3 ADMINISTRATION PROFILES

In addition to the administrator with all rights, there is the option of setting up additional administrators whose rights are restricted to certain applications.

Only those parts of the administration for which the user has the appropriate rights are displayed. For example, a user administrator will not see any trunk groups in the Administration tree view and therefore cannot administrate them.

As default, the profile "Not administrator" is assigned to a user on creation. If you want to change this, open the user properties and assign a different profile to the user (*11.2.1.1 The "Administration" Tab*, Page 164).

You are already supplied with a few simple administration profiles in the standard installation.

Administration profile	Description
System Administrator	These administrators have unrestricted access to SwyxWare.
Backoffice Administrator	These administrators have all the necessary rights for configuring SwyxServer. Above all, these administrators can create or alter feature profiles.
User Administrator (User Administrator)	This administrator can undertake all configurations for users and groups. You can assign the numbers and administrator profiles and configure group parameters. The exceptions here are the trunks and trunk groups, and the feature profiles.
User Operator (User Operator)	This administrator is able to change user properties as well as create or delete users. These rights are typically needed by an administrator who is not meant to change the system configuration.
Call Status Operator (Call Status Operator)	This administrator can see the current call status in the administration, e.g. whether any calls are currently made.
Phonebook Operator (Phonebook Operator)	Users with this right can edit the global phone book, e. g. add or change important phone numbers for the whole company.
No Administrator (No Administrator)	This profile is the default profile for a new user. Therewith the user can log in via Swyx Control Center as user and change his own parameters.

9.3.1 ADMINISTRATORS IN SWYXWARE FOR DATACENTER AND SWYXON

In SwyxWare for DataCenter and SwyxON, a general distinction is made between the provider and reseller or partner level on the one hand as well as the customer's won administrators on the other hand.

Providers and Resellers/Partners

These administrators configure SwyxWare for DataCenter or SwyxON for all customers. The following specific administration levels arise:

Administration profile	Solution	Description
System Administrator	SwyxWare for DataCenter	These administrators have unrestricted access to SwyxWare for DataCenter. The target group is the administrators of the provider or the reseller. Local administrators of the Windows Server always have the rights of a SwyxWare for DataCenter administrator. Further Windows user accounts can be added. These administrators also have the right to assign administration profiles to other users.
Backoffice Administrator	SwyxWare for DataCenter	These administrators have all the necessary rights for configuring SwyxWare for DataCenter. Above all, these administrators can create or alter feature profiles. The only exception is the configuration of users and groups.
Reseller Administrator	SwyxWare for DataCenter	This administrator profile is provided specifically for resellers. It allows complete configuration of a SwyxServer. The only exception is the configuration of trunks and trunk groups.
Reseller Administrator Limited	SwyxWare for DataCenter	This administrator profile differs from the "Reseller Administrator" profile in the following aspects: ● - no permission for configuring CDRs ● - restricted permission for configuring trunk recordings ● - restricted permission for configuring trunk group profiles ● - permission for configuring trunk number signalling

For more information on provider and partner administrators in SwyxON see help.enreach.com/swyxon/1.00/Partner/Swyx/en-US/index.html#context/help/admin_profiles_$.

Customers

Customer level administrators are entered by the provider or reseller or partner, providing the customer the opportunity to administrate his telephone system himself.

The following specific options arise:

Administration profile	Solution	Description
Advanced UC Tenant Administrator	SwyxON	These administrators manage their UC tenant as well as the objects created on it, including trunk groups and trunks.
UC Tenant Administrator	SwyxON	These administrators manage their UC tenant as well as the objects created on it, excluding trunk groups and trunks.
Customer Administrator (Customer Administrator)	SwyxWare for DataCenter	This administrator has the maximum possible rights for a customer. He can undertake all necessary configurations for his front end server. The only exceptions here are the trunks and trunk groups, and the feature profiles.

Administration profile	Solution	Description
User Administrator (User Administrator)	SwyxWare for DataCenter	This administrator can change all properties of users and groups. These rights are typically needed by an administrator who is not meant to change the system configuration.
Call Status Operator (Call Status Operator)	SwyxWare for DataCenter	This administrator can see the current call status in the administration, e.g. whether any calls are currently made. This option is of interest to an administrator who e.g. wants to suspend the computer, and can thus find out whether calls are still in progress.
Phonebook Operator (Phonebook Operator: Editing the global phonebook)	● SwyxWare for DataCenter ● SwyxON	With this right, you can only edit the global phonebook, e. g. add or change important phone numbers for the whole company.

Granting of rights

Dependent on his own position within the rights hierarchy, an administrator can assign administration rights himself. Please see the following table for details:

Own administrator profile	Solution	Assignable profiles
Advanced UC Tenant Administrator	SwyxON	Advanced UC Tenant Administrator UC Tenant Administrator Phonebook Operator
UC Tenant Administrator	SwyxON	UC Tenant Administrator Phonebook Operator

Own administrator profile	Solution	Assignable profiles
System Administrator	SwyxWare for DataCenter	All profiles: System Administrator Backoffice Administrator Reseller Administrator* Customer Administrator User Administrator User Operator Call Status Operator Phonebook Operator
Backoffice Administrator	SwyxWare for DataCenter	No profile, since this administrator cannot change any users or groups
Reseller Administrator	SwyxWare for DataCenter	Reseller Administrator Reseller Administrator Limited Customer Administrator User Administrator User Operator Call Status Operator Phonebook Operator
Customer Administrator	SwyxWare for DataCenter	Customer Administrator User Administrator User Operator Call Status Operator Phonebook Operator
User Administrator	SwyxWare for DataCenter	User Administrator User Operator Call Status Operator Phonebook Operator
User Operator **Call Status Operator** **Phonebook Operator** **No Administrator**	SwyxWare for DataCenter	No profile, since this administrator cannot change any users or groups
Phonebook Operator **No Administrator**	SwyxON	No profile, since this administrator cannot change any users or groups

10 NUMBERS AND NUMBER MAPPINGS

A flexible number concept, which supports distributed locations

The number mapping explained in this chapter describes the mapping of internal numbers for a user to external call numbers. Number mapping should not be confused with the number replacement which can be defined on a trunk group. Number replacement specifies how numbers (number ranges) can be replaced by other numbers/ranges (*Special number replacement:*, Page 231).

In this context, please note the following definitions: **Forwardings** are in relation to a trunk group and establish whether a call via this trunk group can fundamentally leave the SwyxWare installation (*14 Routing*, Page 239). The call permission for a user or a trunk group defines whether a call has the right to be made via this trunk group (*9 Profiles*, Page 128).

10.1 NUMBER TYPES

SwyxWare supports three different number types:

- Internal numbers
- External numbers
- SIP-URIs

These terms are described in detail below and illustrated with examples.

10.1.1 INTERNAL NUMBERS

The numbers 110 and 112 are reserved for emergency calls in Germany, Austria and Switzerland.
As of SwyxWare version 14.00, the numbers 110 and 112 cannot be assigned to internal users.
Make sure that there are no assignments for these phone numbers in your configuration.

Tthe internal number is the user's numbers on which he can be called internally, i.e. by other users at the same location or from other networked locations. The internal number is freely definable and need not necessarily correspond to the extension of the external number, though this is the most common way of assigning internal numbers. (Example of an internal number that differs from the user's extension: External number +44 20 5666 227 -> Internal number 5227). This internal number can consist of any number of digits up to a maximum of 10 digits. It should merely be ensured that the format of the internal numbers does not conflict with other numbers or codes used in the system. For example, an internal number cannot begin with "0" if this is defined for the public line access for this location. It is also possible for a user to be assigned more than one internal number. It is not permissible for a user's internal number to begin with another user's internal number.

Example:

User1 has the internal number 12345, User2 may not be given the internal number 1234, but 1235 is permitted.

Number plan

The introduction of internal numbers enables a common number plan to be used in networked SwyxWare locations.

Example:

A company at a Liverpool location gives all employees a three-digit internal number beginning with "2" (e.g. 201, 202, 203...). The internal numbers of the company's networked SwyxWare location in Dortmund begin with "3" (e.g. 301, 302, 303, ...). When the numbers are assigned in this way and the forwarding tables are configured accordingly, it is possible for all employees to reach all other employees, even in other locations, using the internal numbers.

10.1.2 EXTERNAL NUMBERS

A user's external number defines the number on which he can be reached from an external phone. This external number must come from the public number range, which is supplied by the relevant telephone service provider. This number range must have been assigned to the SwyxServer through the number configuration of its associated trunks.

These are usually number ranges which are supplied via the SwyxServer's analog or ISDN connection to the public telephone network by the relevant service provider (e.g. Deutsche Telekom, Arcor, etc), but also by a VoIP telephony provider. It is often a contiguous number range, such as from +44 20 1234 100 to +44 20 1234 199, which differs only in the last part of the number.

Each of the numbers from this range can be assigned to exactly one user, so that he can be called on the assigned number by external subscribers.

You can also assign an external number to a user that contains less or more digits than the defined numbers range. In this case, overlaps during the call transfer may occur.
If two users have been assigned the external numbers +44 4777 28 and +44 4777 288 for example, any external calls for one of the two users are only signalized to the first user. Any longer number will not be decoded by the system, as soon as a dialed number corresponds to an assigned number.

Several external numbers for one user

It is also possible here to assign more than one external number to a user (***10.3 Mapping of numbers***, Page 149). Especially in installations with networked SwyxWare locations, this opens up the possibility of assigning a user external numbers at different locations, via which external calls can reach him.

Example:

Thus, a user working at a SwyxWare location in Germany can have, in addition to his external number at the German location, a further external number at an interconnected SwyxWare location in England. If a call comes in on this English number, this call is forwarded to the relevant user on the connected SwyxWare in Germany. For an outgoing call from the user to an external subscriber in England, the call can be forwarded via the SwyxWare installation in England into their connected public telephone network to the subscriber concerned, so that the user's external English number is signaled to the called subscriber in England. Such a configuration allows a company (in addition to saving money by using the corresponding local gateways in the interconnected SwyxWare locations) to create a much better outward impression thanks to the "local presence" of staff at different locations.

If a user should only be called internally, i.e. within the SwyxWare installation, there is no need to assign him an external number. In this case the user can only be directly reached on his internal number by other users within the SwyxWare installation (including other networked locations); he cannot be reached from the public telephone network or the Internet.

Format of the external numbers

In general, external numbers are always given in the canonical format:

```
+<country code><area code><number>
```

Example: +44 20 4777100

These are public numbers (numbers on the ISDN or analog connection). SIP providers also offer public numbers, which need to be mapped to a country or a location.

10.1.3 SIP-URIS

A special form of the external numbers is that of the SIP URI (Uniform Resource Identifier). These numbers (usual in Internet telephony) have a format like an email address. They contain a user-specific component (user ID) and a general component (realm) that may, for example, be the same throughout a company. A "number" of this type will always start with ’sip:’ and comprises:

```
sip:<user-ID>@<realm>
```

Example: sip:tom.jones@company.com

The user-specific part here can consist of

- a canonical number, often also without +, e. g. +442012345@company.com or 442012345@company.com,
- a national number e. g. 02012345@company.com
- or, as offered by some Internet telephony service providers, a character string (e. g. jones@company.com).

In the configuration of such SIP URIs, they are always prefixed with "SIP:".

SIP URI as number

A SIP URI, whether in canonical or character string form, serves in Internet telephony as the unique reference for a user, just like an external number in the public telephone network.

SwyxWare therefore allows a mapping of these SIP URIs to SwyxWare users in the same way as canonical numbers can be mapped. The SIP URIs are thus entered like the public numbers in the SwyxServer in the number/URI configuration of a trunk, and assigned to the corresponding users.

These users can then be reached by external subscribers via the SIP URI. Just as for the external numbers, one user can also be assigned several SIP URIs, under which the user can be reached from the outside world.

10.2 NUMBER CONCEPT

Every user is assigned a public number.

Conversely, each user and each trunk group is assigned one location as a property. The location property also defines information relating to the number, e.g., country code and area code, as well as the public line access number. Each source of a call (user or trunk) and each destination of a call (user or trunk) can then be related to a location and thus to information about the composition of the number (e.g. country code, local area code, public line access).

See *8 Locations*, Page 122.

Example of a number concept

The following example shows that every SwyxWare user can have several different numbers in different public networks. Each public number can be assigned to exactly one user.

User		Number
Tom	internal	**323** Tom is identified internally by his internal number
	external	**4430555 55666-323** Tom's "London" external number **44151 89 00 -99** Tom's "Liverpool" external number For outgoing calls, both numbers are signaled as CallerID, depending on which trunk is in use.
Uwe	internal	**222** Uwe is identified internally by his internal number
	external	**4430555 55666-222** Uwe's "London" external number **sip:uwe.jones@company.de** **sip:uwe.jones@company.com** **sip:jones@company.com** Uwe's further external SIP addresses
Jane	internal	**410** Jane is identified internally by her internal number
	external	**4430555 55666-410** Jane's "London" external number **44151 2 00 -99** Jane's German office

The following image shows the installed trunk groups (TG1-6) and the associated routings (WL) in diagram form.

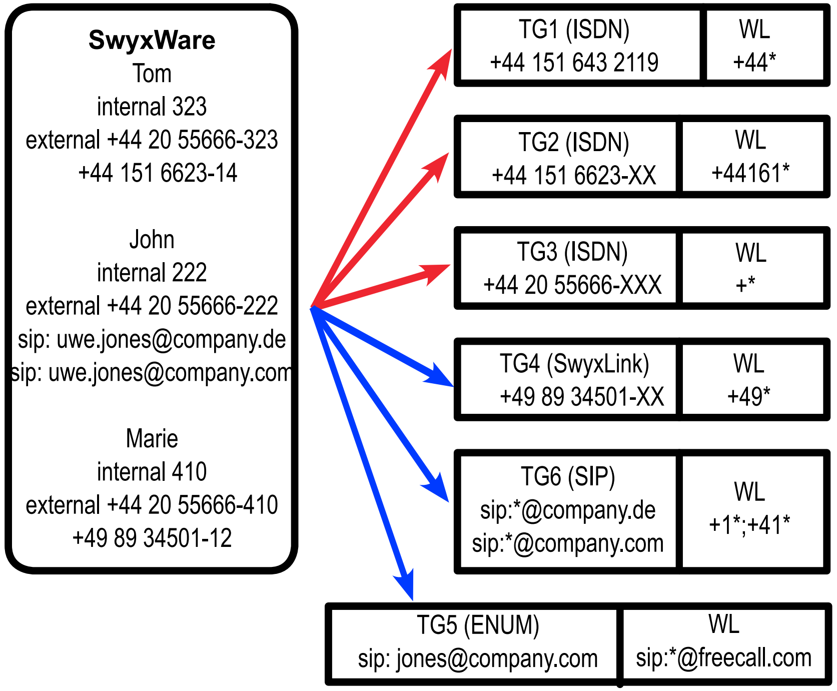


Fig. 10-1: Configuration example for a number plan, trunk groups (TG) and routing (WL)

To call another SwyxWare user, only the internal number can be dialed, even if these users are based at different locations. Calls to external numbers that cannot be routed within SwyxWare are forwarded to the outside world according to the routing records (WL) that were specified on the trunk groups.

Routing

Outgoing calls from SwyxWare are forwarded via the ISDN trunk group TG3 in London into the public network.

Calls to Germany (+49*) are also forwarded via the ISDN trunk group TG1 in Berlin into the public network. The calls going directly to Munich (+4989*) use the ISDN trunk group TG2. It is the priority or the call permission of the user (e.g. local calls only) which determines whether a call to Munich is forwarded via the trunk in Munich (TG2), the trunk in Berlin (TG1) or the trunk in Dortmund (TG3).

Calls going to England are forwarded via the SwyxLink trunk TG4 to England, and handled there according to the prevailing routing there.

Calls going to the USA (+1*) and Switzerland (+41*) are forwarded via the SIP trunk group TG6.

Calls directed to URLs, which are in the domain of a SIP provider (here freecall.com), are forwarded via the SIP trunk group TG5.

See *14 Routing*, Page 239.

10.3 MAPPING OF NUMBERS

The number mapping establishes the logical link between internal numbers (and thus users) and external numbers. This ensures that a call coming in from outside and directed to the external number of a user will be mapped to the user's internal number and will thereby reach the user.

An internal number can be mapped to users or groups as soon as these are created. Mapping to public numbers can also be configured directly (*11.2.2.1 The "Numbers" Tab*, Page 177 or for groups *12.2.2 The "Properties..." Dialog The "Numbers" Tab*, Page 218).

In general an internal number can be mapped to more than one external number, so that the user can be reached on several external numbers (see example under *10.1.2 External numbers*, Page 147).

If several internal numbers are defined for one user, each of these internal numbers can also be mapped to different external numbers.

If the user defines line properties on his SwyxPhone or SwyxIt!, he has the opportunity to configure the lines with the different internal/external numbers. This enables him to signal different external numbers to the caller by the choice of line for outgoing calls.

See *11.2.6.6 The"Line keys" Tab*, Page 190.

All mappings between internal and external numbers are listed in administration in the directory "Number Mappings". Administrators can use this list to see immediately the mappings between internal numbers and public numbers, the user or group to which these numbers belong and the trunk to which these numbers have been mapped.

One or a number of public numbers or SIP-URIs can be mapped to each internal number. In this context, it does not matter how many digits the internal number contains.

Example:

A public range of extension numbers 000-499 has been assigned to you.

For example, you can issue four-digit internal numbers from 0000-9999. However, a maximum of 500 numbers can be reached directly from the outside.

A warning occurs, when the dialed number is longer or shorter than a number of the numbers range defined in the trunk. If, for example, the numbers range is +441234777 000-999 and you assign the number +44123477755 to a user.

How to create a new number mapping

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the context menu for the "Number Mappings" directory, select "Add Number Mapping..." or "Add Range for Number Mapping".

3 The wizard for "Add Internal Number" or "Map Numbers Range" will appear.

4 Internal number:
Enter a new internal number or a numbers range.
Select "Next Unused..." to have the system assign a new number automatically. Select "Check" to ascertain whether the number entered has already been assigned.
Activate the "Show in Phonebook" option if you want the numbers mapped here to appear in the global phonebook.
Click on "Next>".

5 Map the internal number to a public number:
Enter the public number or the first number in a range in canonical format, which is to be mapped to this internal number.
Click "Select" to access a list of currently configured trunks and mapped numbers ranges/URIs.
To map a number from a range of numbers, highlight the corresponding entry and enter the number directly in the "Mapped public number" field.
If you do not wish to assign a public number, select "None" from the list.
Please note that the number cannot be dialed directly from outside (it can only be accessed via an internal connection).
Then click on "OK".

6 Select the assigned user
Select a user from the list to whom the new internal number or range, as well as the mapping you have just configured, is to be assigned.
Click "Finish".

7 The new number is mapped to the selected user.

How to edit a number mapping

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare administration window, open the directory "Number Mapping". You can now edit an existing mapping. Highlight the mapping and select "Edit..." from the context menu. The following window appears: "Edit number mapping".

3 You can edit the internal number for a user or the mapping to a public number.
Click "Finish". The new number mapping is set up for the user.

10.4 EXAMPLES OF NUMBER MAPPINGS

SwyxWare offers great flexibility for incorporating inter-location scenarios into number mapping. The following examples will show just how very flexible it is.

SwyxWare With Three Locations

There are three company locations: London (+4420), Manchester (+44161) and Germany (+49). A SwyxServer with ISDN access is installed in London; at the other locations, there is a separate gateway with ISDN connection to the public network. Furthermore, the headquarters in London is connected to a SIP provider. This means that there are four trunk groups (3*ISDN + 1*SIP) each with one trunk.

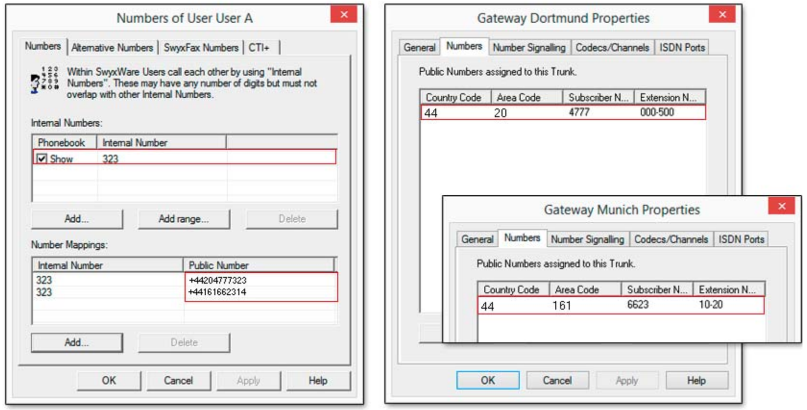
User A

has the internal number 323. Two numbers are assigned to this user. One is a London number (+44 20 1234-323) and the other is a Manchester number (+44 161 6623-14). This user can therefore always be contacted via his Manchester number, even when he is in London.

If the subscriber is in Dortmund but calls a number in Munich, his call can be routed via the gateway (trunk) in Munich and thus his number in Munich (49 89 6623-14) is signaled to the caller.

Other internal callers dialing from anywhere in the company can contact him at any time via his internal number (323).

Number Mapping



Numbers of User User A

Numbers | Alternative Numbers | SwyxFax Numbers | CTI+

Within SwyxWare Users call each other by using "Internal Numbers". These may have any number of digits but must not overlap with other Internal Numbers.

Internal Numbers:

Phonebook	Internal Number
☑ Show	323

Add... | Add range... | Delete

Number Mappings:

Internal Number	Public Number
323	+44204777323
323	+4416166231 4

Add... | Delete

OK | Cancel | Apply | Help

Gateway Dortmund Properties

General | Numbers | Number Signalling | Codecs/Channels | ISDN Ports

Public Numbers assigned to this Trunk.

Country Code	Area Code	Subscriber N...	Extension N...
44	20	4777	000-500

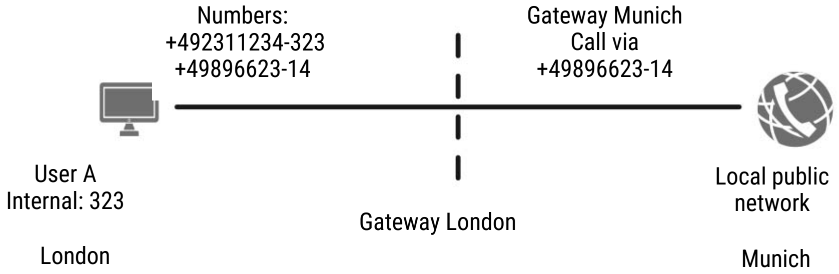
OK | Cancel | Apply | Help

Gateway Munich Properties

General | Numbers | Number Signalling | Codecs/Channels | ISDN Ports

Public Numbers assigned to this Trunk.

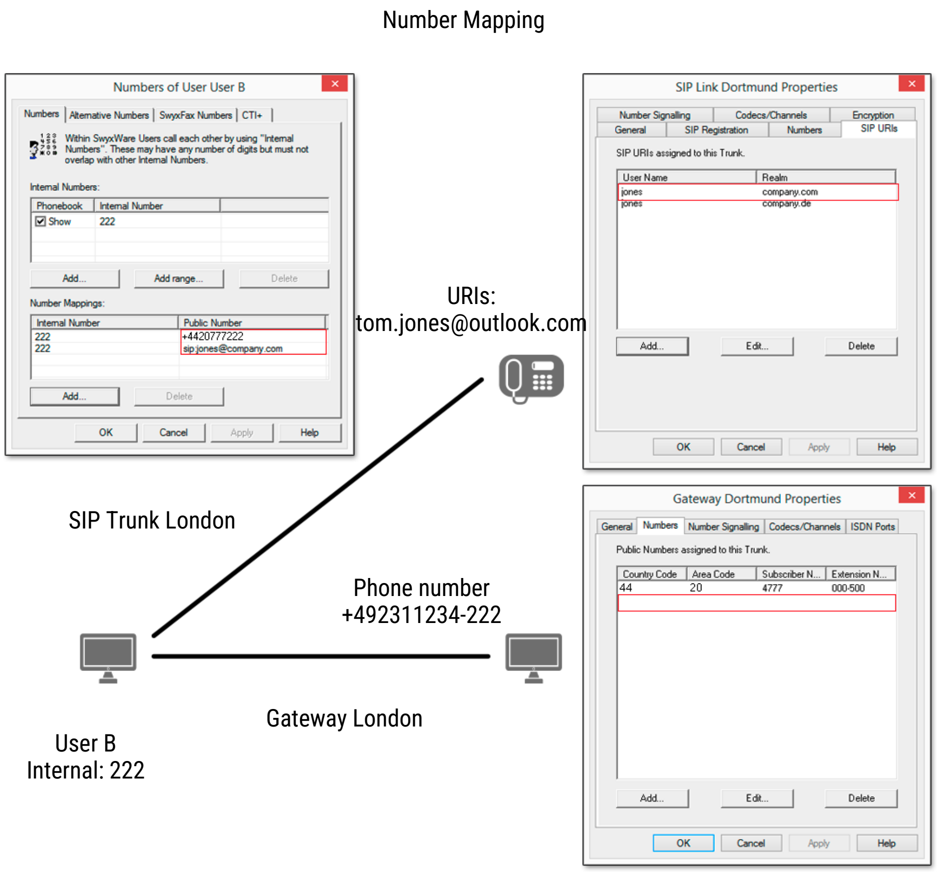
Country Code	Area Code	Subscriber N...	Extension N...
44	161	6623	10-20



User B

has the internal number 222. The London number ’+44 20 1234-222’ will be assigned to him. He also receives the URI "jones@company.com".

Other internal callers dialing from anywhere in the company can contact him at any time via his internal number (222).



Numbers of User User B

Numbers | Alternative Numbers | SwyxFax Numbers | CTI+

Within SwyxWare Users call each other by using "Internal Numbers". These may have any number of digits but must not overlap with other Internal Numbers.

Internal Numbers:

Phonebook	Internal Number
☑ Show	222

Add... | Add range... | Delete

Number Mappings:

Internal Number	Public Number
222	+4420777222
222	sip:jones@company.com

Add... | Delete

OK | Cancel | Apply | Help

SIP Link Dortmund Properties

Number Signalling | Codecs/Channels | Encryption | General | SIP Registration | Numbers | SIP URIs

SIP URIs assigned to this Trunk.

User Name	Realm
jones	company.com
jones	company.de

Add... | Edit... | Delete

OK | Cancel | Apply | Help

Gateway Dortmund Properties

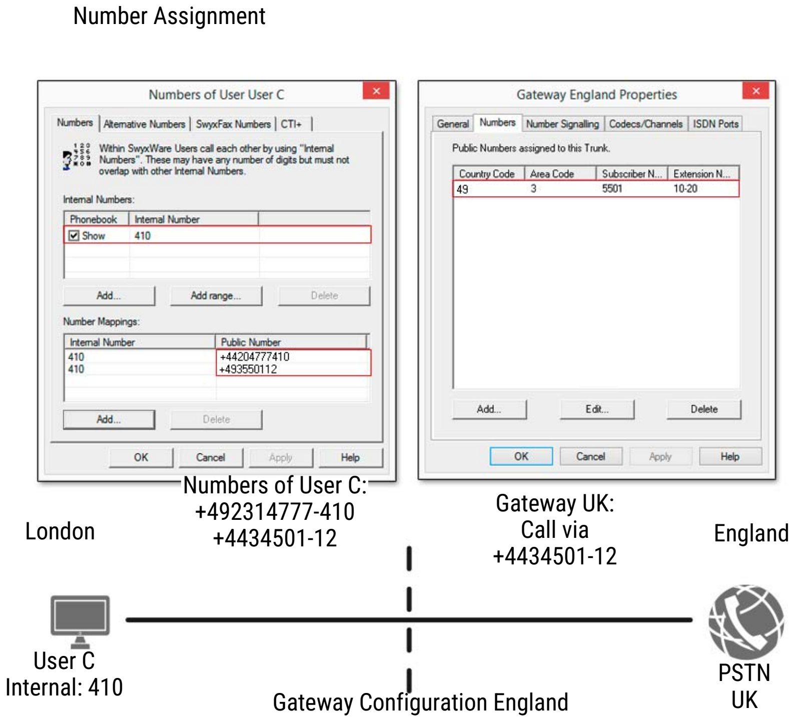
General | Numbers | Number Signalling | Codecs/Channels | ISDN Ports

Public Numbers assigned to this Trunk.

Country Code	Area Code	Subscriber N...	Extension N...
44	20	4777	000-500

Add... | Edit... | Delete

OK | Cancel | Apply | Help



Numbers of User User C

Numbers | Alternative Numbers | SwyxFax Numbers | CTI+

Within SwyxWare Users call each other by using "Internal Numbers". These may have any number of digits but must not overlap with other Internal Numbers.

Internal Numbers:

Phonebook	Internal Number
☑ Show	410

Add... | Add range... | Delete

Number Mappings:

Internal Number	Public Number
410	+44204777410
410	+493550112

Add... | Delete

OK | Cancel | Apply | Help

Gateway England Properties

General | Numbers | Number Signalling | Codecs/Channels | ISDN Ports

Public Numbers assigned to this Trunk.

Country Code	Area Code	Subscriber N...	Extension N...
49	3	5501	10-20

Add... | Edit... | Delete

OK | Cancel | Apply | Help

User C

has the internal number 410. Both a London number '+44 20 4777-410' and a German number '+49 34501-12' have been assigned to this user. This means that he can be contacted via a London number and a German number.

Other internal callers dialing from anywhere in the company can contact him at any time via his internal number (410).

If the user calls a number in Germany from London, his call can be forwarded via the gateway (trunk) in Germany and, therefore, his number in Germany (+49 34501-12) indicated to the caller.

10.5 PLACEHOLDER

Placeholders can be used when mapping numbers or SIP-URIs to a user, group or trunk. These placeholders can also be used in the Routing Table or the Calling Rights.

10.5.1 GENERAL PLACEHOLDERS

The general placeholders can be used in many places within SwyxWare, in routings, number mappings, number replacements and so on.

The following general placeholders are available:

Placeholder	Type of number	Explanation
*	Phone number	* replaces any number of characters to the right. In the case of a telephone number * can only be places at the end of the sequence. Example: +4420* indicates all numbers in London (country code 44, area code 20).
*	URI	The placeholder * replaces any number of digits. A general distinction is made between the following applications: ● Call Permissions and Routing sip:{*}[a-Z, 0-9]@[a-Z, 0-9]{*} Example: sip:*.development@company.com indicates all URIs referencing the realm 'company.com' whose user IDs end with '.development'. ● number replacement sip:[a-Z, 0-9]{*}@{*}[a-Z, 0-9] Example: sip:*@*.com stands for all URIs in English Realms. For further examples, please refer to *Examples of general placeholders*, page 153.
+	Phone number	Indicates the inter-location code for international calls. Example: +49456555 In the United Kingdom, + is replaced with '00', i. e., '0049456555' is the number dialed.

Examples of general placeholders

*@company.com	All SIP-URIs mapped to the 'company.com' realm.
.jones@company.	Configured as call authorization or forwarding: All persons named Jones who, for example, have the realm 'company.de' or 'company.com'
+44*	All numbers within the United Kingdom (+44)
+49221*	All numbers in Germany (+49) in Cologne (221)
+*	All public numbers
*	All numbers

10.5.2 SPECIAL PLACEHOLDERS

In connection with the Calling Rights (*9.1.2 Create Call Permission*, Page 134) and number replacement (*Special number replacement:*, Page 231), further special placeholders are provided. These placeholders are replaced with the location parameters of the user or trunk. It is thus possible e.g. to create a call permission that can be used independently of the location.

Example:

If you want to create a call permission that basically allows local calls via all trunk groups, but only for a specific public line access (in this case '8'), you configure the following parameters:

```
Allow call +[CC][AC]*
Trunk group "All"
Public line access 8 (private)
```

You can then use this call permission independently of the trunk group's location. In each case, the codes which were defined for the trunk group's location are used.

10.5.2.1 PLACEHOLDERS IN THE CALL PERMISSION

The following special placeholders are provided for the call permission:

Placeholder	Type of number	Explanation
[cc]	Public number	Indicates the country code. Example: +[cc]* in a call permission indicates authorization for national calls (i.e., calls within the same country). This means that this call permission can also be used for cross-national locations.

Placeholder	Type of number	Explanation
[ac]	Public number	Indicates the area code. Example: +[cc][ac]* in a call permission indicates authorization for local calls (i.e., calls within the same city). This means that this call permission can also be used for inter-location calls.

The value of this placeholder is then taken from the configuration of the trunk group or the user (*13.1.8 The "Location" Tab*, Page 237).

10.5.2.2 PLACEHOLDERS FOR NUMBER REPLACEMENT

The following special placeholders are provided for number replacement:

Placeholder	Type of number	Explanation
[cc]	Public number	Indicates the country code. Example: +[cc]* in a call permission indicates authorization for national calls (i.e., calls within the same country). This means that this call permission can also be used for cross-national locations.
[ac]	Public number	Indicates the area code. Example: +[cc][ac]* in a call permission indicates authorization for local calls (i.e., calls within the same city). This means that this call permission can also be used for inter-location calls.
[ext]	Number	Extension Example: 225
[sn]	Number	Phone number (subscriber number) Example: 4777
[ldcp]	Number	Long distance call prefix Example: 0
[icp]	Number	International call prefix Example: 00
[plap]	Number	Public Line Access Prefix Example: 0
[fplap]	Number	Public Line Access of Superior Telecommunication System (Foreign Public Line Access) Example: 9
[cbcp]	Number	Call by Call Prefix Example: 01013
[empty]	-	Has no function and can be used to improve display.
[pbxrealm]	URI	The realm that was configured. Example: company.net
[*]	-	Display of the key * (keypad), since * is already in use as a placeholder.

Further examples of number replacement

The following table lists examples of possible uses of placeholders in number replacement.

Original	Replacement	Explanation
sip:231*@*.company.com	sip:123*@*.lanphone.com	The placeholders are identified by their position in relation to @: ● before the @ Beginning at the @, all characters to the left are replaced. Here: Everything to the left of the @ up to the string "sip:231" is inserted between the string "sip:123" and the @. ● after the @ Beginning at the @, all characters to the right are replaced. Here: Everything to the right of the @ up to the string "company.com" is inserted between the @ and the string "lanphone.com". ATTENTION: It is not possible to insert more than one * before or after the @.
sip:231*@*.company.com	123*	If no @is present, the placeholder is classified as "before the @". Here: Everything to the left of the @ up to the string "sip:231" is inserted between the string "sip:123" and the @. The placeholder after the @ has no match in this example, and is not further replaced.
sip:231*@*.company.com	sip:231@*.outlook.com	Here, everything between the string "sip:231" and the @ is ignored. Everything between the @ and the string ".company.com" is inserted between the @ and the string ".outlook.com".
+4415	+44800283015	The number '+4915' is replaced by '+49800283015'
+4415*	+44800283015	All numbers beginning with '+4415' are replaced with '+44800283015'.
+4415*	+44800283015*	Any numbers starting with '+4415' will be replaced by numbers beginning with '+44800283015', i.e. +44151234567 will be replaced by +4480028301512345 67.

10.6 SUPPLIED CONFIGURATION DATA

To simplify the standard configuration of number conversion, typical installation scenarios are supplied in the two configuration files:

- NumberFormatProfiles.config
- ProviderProfiles.config

10.6.1 NUMBERFORMATPROFILES.CONFIG

In this file you will find the definition of the various number types.

The following number formats are available for selection:

Format	Explanation
CLIP no screening	Formats the numbers with ISDN type and plan information to the public line **Application:** When the function "CLIP no screening" is used on an ISDN trunk for the calling party number for outgoing calls. In this case the calling party number is defined by the server and signaled to the public line. This number is not checked for correctness (i.e. belonging to this connection) by the public line (no screening). This makes it possible, for example, to signal the caller's original number externally for forwarded calls. The function must be set up separately with the telephone service provider. **Example:** ● National numbers: <Area code><Number> Type = "National" Example: 3478, 5060). ● International numbers: <Country code><Area code><Number> Type = "International" Example: 3478, 5060).

Format	Explanation
Dial as a PBX user	Number is as an internal subscriber typically dials, i.e. at the associated location, taking into account the public line access code: or internal number or canonical number In addition, for canonical numbers a 0 is removed which is incorrectly inserted when dialing from Outlook. Transmits and interprets the number as a user of a telecommunication system does. For a connection to a subsystem, "Dial as a PBX user" should be applied for incoming calls for the called party number, and for outgoing calls for the caller number. This setting is made automatically if you select the format "Internal Lines". **Application:** ● internally for any user ● but also on a sub-telecommunication system for - the called party number for incoming calls -the calling party number for outgoing calls **Example:** ● +44 0 23147770 is converted into +442314770 ● <Public Line Access><Number> 04777555 00244777555 ● Canonical number also possible +442314777555

Format	Explanation
Extension (Extension)	For this number format, it is assumed that all dialed numbers are meant as an extension. They are correspondingly interpreted and generated, i.e. numbers of incoming calls remain unchanged. Outgoing numbers are prefixed by the public line access number of the superior telephone system. Numbers not coming from the trunk's extension range are not converted. **Application:** ISDN trunk for the called party number for incoming calls to a direct dialing-in ISDN line. **Example:** Extensions 555
Fixed Subscriber	For incoming calls, sets the number configured for this trunk. The analog connection does not supply a number, as the number is defined by the called line. In order that a called party number (inbound) is detectable for SwyxWare, the call is parameterized with the fixed line number. **Application:** This format should be set for an analog trunk. **Example:** The number on the analog connection is 475594. The destination number "Fixed Subscriber" is then configured in the profile "Standard analog lines" for the incoming call. In the number replacement on the analog trunk, all incoming destination numbers (*) are replaced by the fixed number of the analog connection (475594).

Format	Explanation
ISDN Italy	The number is formatted according to use at Italian exchange connections, with ISDN type and plan information. **Application:** ISDN trunks to Italian connections for the calling party number **Example:** ● For incoming calls, depending on the signaled number type, the signaled number is prefixed with the country code or the local area code, in order to produce the canonical format. ● For outgoing calls, the public line access number of the superior telephone system and the call-by-call prefix digits are added. ● No call-by-call numbers are added to emergency call numbers.
ISDN Netherlands CLIP	The number is formatted according to use at Dutch exchange connections, with ISDN type and plan information. **Application:** Calling party number for incoming and outgoing calls at Dutch exchange connections *Example:* *Only used for the calling party number. Outgoing numbers are converted normally according to type.* *The emergency number 112 is converted from canonical format to 112.*
Canonical without plus	This format corresponds to the canonical number format, but without leading +. **Application:** Calling party number or called party number for certain SIP providers For outgoing calls, the numbers are signaled in canonical format without the preceding +. For incoming calls, the canonical format is formed depending on the signaled number type, adding a + and the country code and area code to the signaled number as necessary. **Example:** <Country code><Area code><Number> 44204777555

Format	Explanation
Canonical with plus	Canonical number format. Emergency numbers are unchanged in the canonical format: e.g. 112. **Application:** Calling party number or called party number for certain SIP providers. The emergency numbers of known countries are correctly converted, e. g. +44 20 112 to 112. Incoming phone numbers are expected in canonical format. **Example:** +<Country code><Area code><Number> +442314777555
National	Corresponds to the format that you typically dial on the exchange connections of the respective country, but without taking into account your own local area code. This means that even if your own line belongs to the local public network (020), the dialed number must appear as 020 4777 555. **Application:** Called party number and calling party number for most SIP providers and ISDN connections. For outgoing calls, the emergency numbers of known countries are correctly converted, e.g. +44 20 112 to 112. For the normal outgoing calls, the public line access number of the superior telephone system and the long-distance call prefix are added. For incoming calls, the public line access number of the superior telephone system and the long-distance call prefix are filtered out. **Example:** <Area code><Number> 0204777555
Subscriber	Corresponds to the format that you typically dial on the exchange connections of the respective country, but taking into account your own local area code. This means that if your own line belongs to the local public network (020), the dialed number should appear as 4777 555. **Application** For calling party number and called party number for most ISDN connections without direct dialing-in. ● For incoming calls, the public line access number of the superior telephone system and the long-distance call prefix are filtered out. ● Conversely, for outgoing calls the public line access number of the superior telephone system and the long-distance call prefix are added. **Example:** <Number> 4777555
Transparent	Does not describe a format, but rather the fact that numbers remain untouched by the general replacement, so that they can be altered with the specific number configuration. **Application:** Definition of individual replacement rules based on the server's internal number format.
Type and Plan	This format sets the type and plan fields within the ISDN transmission protocol in a generic way. **Application** Very seldom used, and then only on ISDN connections

Special handling for specific numbers

In particular, the possibility of including connections at different locations in SwyxWare requires a separate consideration of special numbers and especially emergency numbers.

This special handling of the numbers is defined in the file Programme\SwyxWare\NumberFormatProfiles.config.

If you want to support special codes which are not listed in this file, you can configure these manually for the respective trunk group.

How to define the special handling for a number

1. Open the property page for the trunk group you want to use for dialing the special telephone codes.
2. Select the "Profile" tab, and click on "Configure...". Number replacement configuration opens up.
3. Beside the field "Outbound Called Party Number", click on "Add...". A window will open: "Add Number Replacement".
4. For every special telephone code you want, add the following rule:
   - Original number: +<Country code><Area code><Special number>
   - Replacement:
     Special telephone code

   Example: Directory assistance (no. 11833 in London)
     Original number +442011833
     Replacement 11833

Please inform Enreach if there is a missing special telephone code, so that we can consider this code in future versions.

10.6.2 PROVIDERPROFILE.CONFIG

The profiles for the trunk groups are specified in this file. When creating a trunk group, you can choose depending on the trunk type from various preconfigured profiles (*13.1.2 The "Profile" Tab*, Page 230).

These profiles define how SwyxWare interprets numbers for incoming calls and converts them into SwyxWare-internal formats, and how SwyxWare-internal numbers are transferred out for outgoing calls.

Example:

You select the profile "Standard DDI" for an ISDN trunk group. This is a profile for a direct dialing-in line to ISDN with the assignment:

- Outgoing call
  Calling party number Extension
  Destination number: Subscriber
- Incoming call
  Calling party number Subscriber
  Destination number: Extension

The telephone network usually delivers the numbers in the following format:

<Country code><Local area code><Subscriber number><Extension>

Depending on local circumstances, it could also be e.g.:

<Local area code><Subscriber number><Extension>

- If a SwyxWare user (+44 20 4777 225) calls a public line (e. g. 024 3456 555) over this ISDN trunk, the following interpretation arises:
  This is an outgoing call. The caller number (225) is interpreted by SwyxWare as an extension and is signaled to the ISDN line as such. The dialed destination number is recognized as a subscriber number of the public network (a subscriber, 024 3456 5555) and is passed in this form as a destination to the public network.
- If a subscriber (024 3456 555) calls from the public network and his number type is not recognized, then the called number (destination number) is interpreted as an extension, and forwarded to the internal subscriber with the extension number 225.

11 USER CONFIGURATION

How are users created and configured?

This chapter explains how to set up users, how to set up the Voice Box and remote access and how to set up conference rooms.

> ⚠ When saving and processing personal data, observe the respective applicable legal data protection regulations.

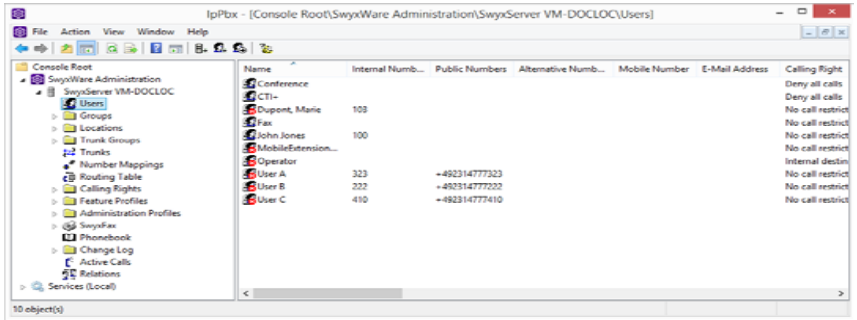
> ⚠ Personal data cannot be deleted automatically from the data base. In order to meet the valid data protection regulations, it may be necessary to delete the corresponding entries manually.

Users can be set up, and also removed, via the SwyxWare Administration (*11.1 Configuring a new User*, Page 160) as well as in Windows user administration (*11.6 Configure users in the Windows user administration*, Page 209).

11.1 CONFIGURING A NEW USER

You can view the most important settings for all configured users in the tabular detail view of the user folder:

- Name
- Name and an additional description text
- Number(s), internal and public
- E-mail address
- Forwardings (Unconditional, Busy and No Reply)
- SIP User ID
- Logon status and terminal devices used
- Assigned user accounts
- Total size of all user-specific files in the database
- Internal and public fax numbers, and fax forwardings.
- CTI+ numbers and CTI + (defines, whether CTI+ is configured for the user)



Name	Internal Numb...	Public Numbers	Alternative Numb...	Mobile Number	E-Mail Address	Calling Right
Conference						Deny all calls
CTI+						Deny all calls
Dupont, Marie	103					No call restrict
Fax						No call restrict
John Jones	100					No call restrict
MobileExtension...						No call restrict
Operator						Internal destin
User A	323	+492314777323				No call restrict
User B	222	+492314777222				No call restrict
User C	410	+492314777410				No call restrict

How to check / change a user's settings

How to deactivate a user

How to send a Welcome email

How to create a new user

1. Click with the right mouse button on the "User" directory located in the window on the left.
2. Select "Add User...".
3. Name and type of new user:
   Enter the name of the new user and, if applicable, a brief description.
   Click on "Next>".
4. Location of the new user:
   Select a location for the user from the dropdown list. The location determines site-specific parameters such as country and area code, prefixes, public line access prefix(es) and the time zone, see also *8 Locations*, Page 122.
   Click on "Next>".
5. Internal numbers of the new user:
   Enter the internal number for this user here.

The numbers 110 and 112 are reserved for emergency calls in Germany, Austria and Switzerland.
As of SwyxWare version 14.00, the numbers 110 and 112 cannot be assigned to internal users.
Make sure that there are no assignments for these phone numbers in your configuration.

Use "Verify" to immediately check whether this number has already been assigned.

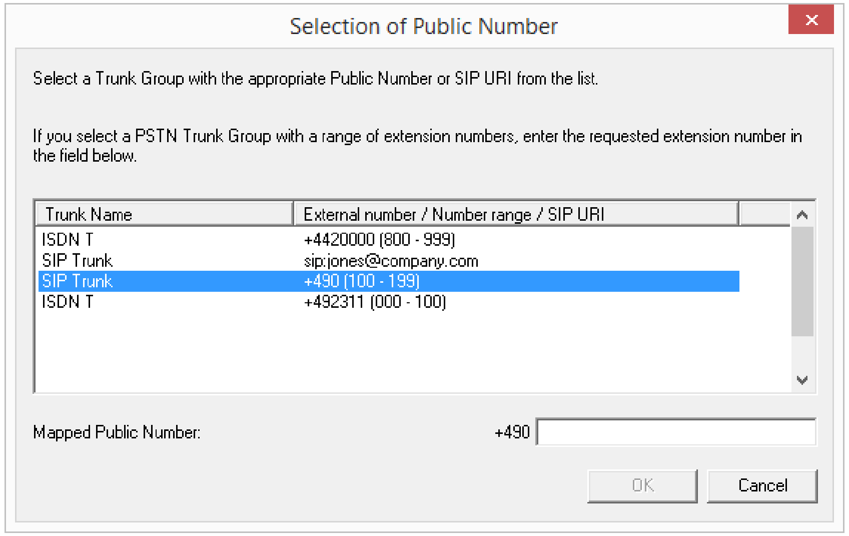
Clicking on "Next unused" will automatically assign the next unused internal number to the user. You can also enter a number, e. g. 210, in order to leave the number range below untouched. Clicking on "Next unused" will then assign the next unused internal number.

"Check" lets you check whether an entered internal number is already present.

Activate the checkbox "Show in Phonebook" if this number is to be listed in the Global Phonebook. Name resolution is always performed, regardless of whether the user is entered in the Global Phonebook.

Click on "Next>".

6 Internal number mapping:
If the internal number is to be reachable from the public telephone network, it must be mapped to an external number. You can enter this public number directly in the field or click "Select...".
The "Choose public number" window will appear.



Selection of Public Number

Select a Trunk Group with the appropriate Public Number or SIP URI from the list.

If you select a PSTN Trunk Group with a range of extension numbers, enter the requested extension number in the field below.

Trunk Name	External number / Number range / SIP URI
ISDN T	+4420000 (800 - 999)
SIP Trunk	sip:jones@company.com
SIP Trunk	+490 (100 - 199)
ISDN T	+492311 (000 - 100)

Mapped Public Number: +490

Select the SIP URI or public number here.

If the public number is to be taken from a numbers range, double-click on that range.

Assign the external number in the "Mapped Public Number:" field and click "OK".

If the number entered is shorter than the numbers range of the trunk/s, a warning signal is generated. If the numbers range is defined as +441234777 000-999, a warning occurs, if you e. g. assign the number +44123477755 to a user. See *10.1.2 External numbers*, Page 147.

Click on "Next>".

7 Terminals:
Choose the terminals with which the user will log in to SwyxServer. This selection will determine which configuration dialogs must be completed. The entries relating to the terminal equipment will later be used to authenticate the user on the SwyxServer. You have several different options:

- SwyxIt! Classic and SwyxFax Client
  Define the logon procedure. You can choose between the Windows user account, a user name or UPN and password or config-

ure both: See *11.2.1.2 The "Authentication" Tab*, Page 165.

Windows User Account

Here, it is necessary that the computer of the SwyxIt! Classic user and SwyxServer are within the same domain. For installations within one company, this is usually the case. You can enter the user account in the form "<Domain> \ <Account Name>". "Browse..." allows you to select a user from the domain.

Username and Password

When logging on SwyxServer the user enters his user name or UPN and password. He can save both in his local SwyxIt! Classic.

- SIP Devices

  Enter the following user information. Specify whether the authentication mode is chosen according to the server standard settings, or whether authentication should always or never take place. If authentication is required, enter here the necessary data for authentication, such as the user name and the password. These do not need to be identical to the SwyxWare user name and password that you may have configured for logon with a SwyxIt! Classic.

  You can make special adaptations for SIP devices from another manufacturer after creating the user, in his Properties.

  See *11.2.1.4 The "SIP Registration" Tab*, Page 169.
- SwyxPhone Lxxx

  Assign the user a PIN, with which he logs in to the SwyxServer. This PIN must contain between 1 and 16 digits.

  See *11.2.1.6 The Tab "SwyxPhone Lxxx"*, Page 171.
- Simple user for Call Routing

  This user is not allowed to log in with a terminal.

Click on "Next>".

8 E-mail address:

The user must be assigned a unique e-mail address for SwyxWare integration in Microsoft Office (SwyxIt! Classic function "Office Communication AddIn"). The e-mail address indicated must be the primary SMTP e-mail address set up for the user on the company's e-mail server (e.g. Microsoft Exchange Server).

This e-mail address is also the default setting for delivering voice messages. The e-mail address of the Voice Box can be configured by the user or in the SwyxWareadministration in the "Redirects" dialog, see *11.2.5.4 Standard Voice Box" tab*, Page 183.

Additionally you can send the user via this address welcome emails with his registration data and configurations, see *Welcome E-mail*, Page 173.

A configuration of the special Voice Box e-mail address has no influence on the existing e-mail address that was created for the integration in MS Office.

Click on "Next >".

9 Client authentication

A client's user must authenticate when logging on to SwyxServer. The following authentication types are available:

- Authentication with Windows user account
- Federated authentication via identity provider
- Authentication with user name and password

See *11.2.1.2 The "Authentication" Tab*, Page 165

Activate the "Continue without password" option if the user should set their password independently via the link in the welcome email or email to reset the password, see *Reset password:*, Page 167.

If you have set a password when creating the user, the welcome email for the user will not contain a password.

You must communicate the set password to the user by other means.

10 Call Permissions:

Call permissions and restrictions are grouped together in a profile.

See *9.1 Call Permissions*, Page 128.

Select a call permissions profile for the user from the selection list.

Click on "Next>".

11 Feature Profile:

The feature profile determines which functions are available to this user in principle.

See *9.2 Function profile*, Page 137.

12 Transfer properties to the new user:

You have the option of applying a configured user's properties to the new user you are creating. These properties include group memberships, relationships and call forwardings, and also most of

the settings for SwyxIt! Classic and the rules for the Call Routing Manager.
Select the option "Create new user account and apply the properties of an existing user", in order make use of this option. Then choose the user whose properties you would like to apply from the selection list. Alternatively, you can use the appropriate option to create an empty user account (with or without sample files for the Call Routing Manager) and manually configure the above-mentioned properties later.
Activate the "Open properties after finish" checkbox if the user properties shall be opened after the creation process.
Activate the "Send welcome E-mail" checkbox if you wish to send the user an E-mail with his registration data and configurations. You can also send the Welcome email after setting up the user at any time, e. g. due to configuration changes, see *Welcome E-mail*, Page 173.

> If you do not enable the "New users must change their password the first time they perform a login" option, the user will not receive a pre-configured password in their welcome email.

13 Complete the set up of a new user by clicking on "Finish".
A new user is created. The "Waiting for user creation" dialog window will appear. Then, possibly the newly created user's properties are displayed.

14 If you do not need the newly created user's properties, click on "Cancel".
The user is created and appears in the user list.

> Create a dummy user, which is configured as you wish and provided with a deactivated account, to be used as a template.

11.2 USER CONFIGURATION

Existing users can be changed, for example they can be assigned new rights or new terminals.

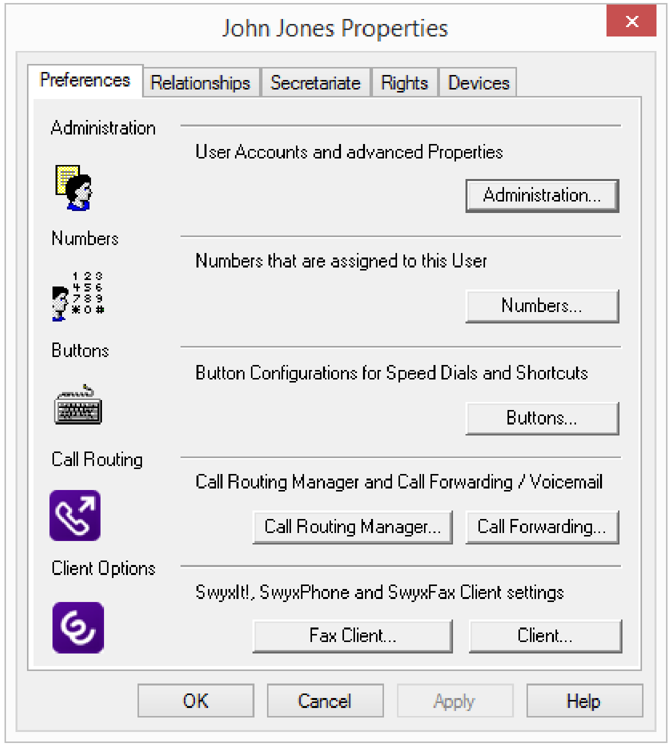
How to deactivate a user

How to check / change a user's settings

1 Click an entry in the user list with the right mouse button.

2 In the context menu, select "Properties".
You can check and change all user settings in the configuration dialog which now appears.

11.2.1 THE "ADMINISTRATOR PROPERTIES FOR USERDIALOG



In this dialog you can specify the configuration of the user, such as for example possible end devices, call intrusion and mailbox.

3 After completing your changes, click on "OK".

You will be returned to the tabular overview.

4 If you have changed the settings of a user who is logged in, select the shortcut menu once again by clicking with the right mouse button.

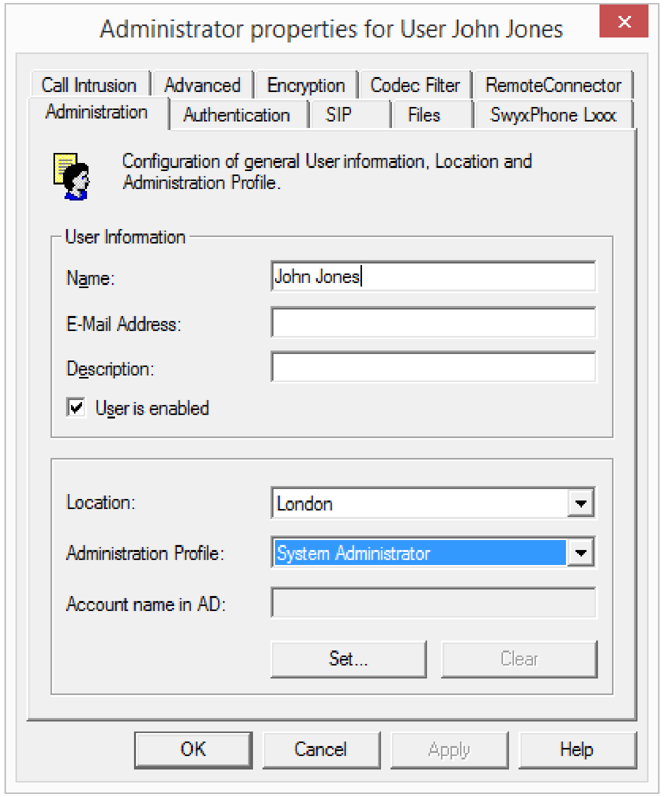
5 Click on "Logoff".
SwyxIt! Classic is thereby prompted to import the new configuration data from the SwyxServer.

> ⚠ This step will disconnect all of this user’s telephone calls currently in progress.

The user properties can be configured on the "Preferences", "Relationships", "Secretariat", "Rights" and "Terminals" tabs. Relationships will be explained in detail in the following chapter on the subject of "Groups", see *12 Configuration of Groups*, Page 215. You will find information on the secretariate configuration in the chapter titled "Secretariate", see*12.3 Secretariat*, Page 224. The preferences are set with the help of the dialogs described below.

The dialogs described below can also be called by clicking on the user with the right mouse button and then selecting the dialog you want under "Special Properties", or by clicking on the appropriate symbols in the toolbar located in the upper margin of the window.

11.2.1.1THE "ADMINISTRATION" TAB



Administrator properties for User John Jones

Configuration of general User information, Location and Administration Profile.

User Information

Name: John Jones

E-Mail Address:

Description:

☑ User is enabled

Location: London

Administration Profile: System Administrator

Account name in AD:

User Information

The display name of the SwyxWare user is defined in the field "Name". This name will be used for a variety of displays on the SwyxIt! Classic interface and the SwyxWare Administration. Furthermore, this name can be entered directly within SwyxIt! Classic to call this SwyxWare user.

Please note that the user name must be unique within SwyxWare. This means that no other user, SwyxGate, SwyxLink, group or external Phonebook entry may have this name. This is checked by the SwyxWare Administration.

In the "e-mail address" field, the e-mail address must be entered that is set up on the company's e-mail server (e.g. MS Exchange Server) for the corresponding user as the primary SMTP e-mail address.

Configuring an e-mail address in this field enables integration of the SwyxWare status information and telephony function in Microsoft Office ("Office Communication AddIn"). See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/#context/help/office_communication_$.

In the user list, check that all entries in the "e-mail address" column are correct, thereby guaranteeing integration in MS Office.

Status signalization between various SwyxWare sites requires additional configuration. See *17 SwyxLink (Server-Server Connection)*, Page 292.

More detailed information on the user can be entered in the "Description" field. However, the contents of the field are not analyzed in any way by SwyxWare.

The "User is enabled" checkbox can be used to temporarily exclude users from SwyxWare without directly having to delete them. The user will then be rejected the next time he or she attempts to log in.

Location

Each SwyxWare user is assigned a location. This location determines the country and area code, prefixes, public line access prefix(es) and the time zone.

See *8 Locations*, Page 122.

Administration profile

Each user is assigned an administrator profile (default: Not administrator). The administrator profile defines what rights this user has when he connects to a SwyxServer with the help of the SwyxWare Administration. Depending on the profile he can e. g. create or change users or edit phonebooks.

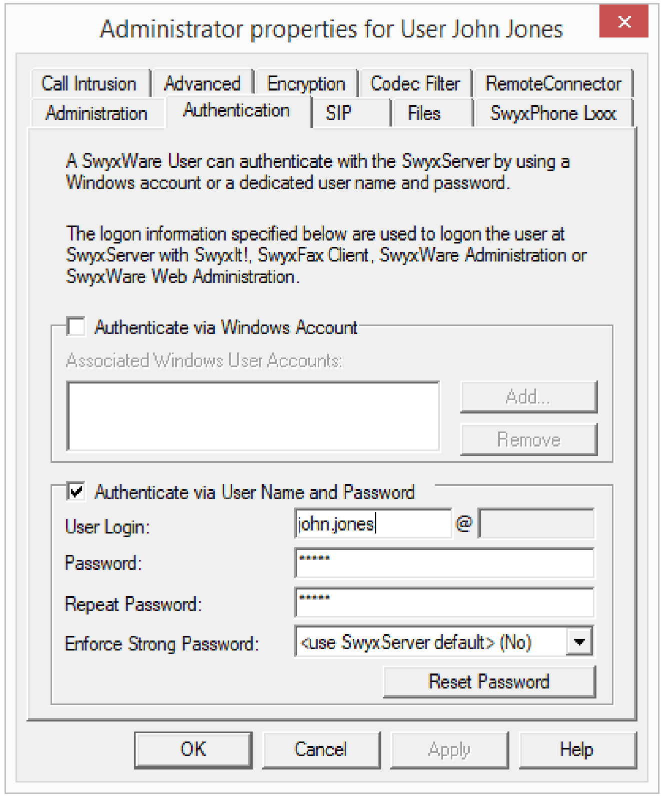
See *9.3 Administration profiles*, Page 143.

AD Account Name

Enter here the user account in the Windows user administration (Active Directory), which is assigned to this user. Click on "Set..." to select a user account. A new window opens up, in which you can search for the user and verify the entries.

See *11.6 Configure users in the Windows user administration*, Page 209.

11.2.1.2THE "AUTHENTICATION" TAB



Administrator properties for User John Jones

A SwyxWare User can authenticate with the SwyxServer by using a Windows account or a dedicated user name and password.

The logon information specified below are used to logon the user at SwyxServer with SwyxIt!, SwyxFax Client, SwyxWare Administration or SwyxWare Web Administration.

□ Authenticate via Windows Account

Associated Windows User Accounts:

☑ Authenticate via User Name and Password

User Login: john.jones @

Password: *****

Repeat Password: *****

Enforce Strong Password: <use SwyxServer default> (No)

A client's user must authenticate when logging on to SwyxServer. The following authentication types are available:

Authentication with Windows user account

Federated authentication via identity provider

Authentication with user name and password

You can specify for each user which of the three authentication types they are allowed to use.

When logging in, the user is offered two authentication types, even if one or all of them are not permitted for the user:
- Windows account- or Composite authentication
- Name/password authentication
Make sure that the user can authenticate using at least one of these options.

Authentication with Windows user account

Each SwyxWare user can be assigned one or more Windows (domain)user accounts. The SwyxWare user must be logged in using one of these Windows user accounts to be able to use SwyxIt! Classic to place calls. You can add a Windows user by clicking on "Add..." and then making a selection from the list displayed. You can remove a Windows user account from the list by highlighting it and then clicking on "Remove".

When a user logs in using a Windows user account, the user and SwyxServer need to be within the same domain.

For the telephony clients within SwyxWare for DataCenter andSwyxON, who are typically not in a domain with the SwyxServer, this authentication is then not possible.

Federated authentication via identity provider

If your organization uses identity provider services, you can use federated authentication instead of Windows authentication (federated authentication with **OAuth 2.0** and **OpenID Connect**) .

If you activate an identity provider configuration, federated authentication is offered for selection on SwyxServer instead of authentication via the Windows user account.
Deactivate all identity provider configurations to use Windows authentication again.

help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/#context/help/GeneralSettings.IdentityProvider.Configuration

Authentication with user name and password

If necessary, enter a user name and password with which a user can log in to SwyxWare Administration and the clients.

The user name must correspond to the UPN format (User Principal Name): User login name +"@" + UPN suffix. You can use the domain name or an alias as the UPN suffix.

Example: john.jones@company.com

You can set the UPN suffix in the server properties, see *7.5.18 The "Security" tab*, Page 109.

Users configured before V 11.25 do not use UPN.
To enable these users to log in via UPN, enter the appropriate UPN for each user.

The user name is used to create a SIP user ID.

See also *SIP User Name and SIP User ID; SIP password*, Page 170.

Force complex password:

As an administrator, you can force or deactivate the use of complex passwords as a general rule for SwyxServer in server configuration (*Password settings*, Page 110)

This rule can be configured individually for each user.

You can select among the following three options in the "force complex password" option field:

- Use server default settings (<current setting>): ("Yes" or "No")
  The general settings on the SwyxServer apply for the user. This option is set by default.
- Force complex password: "Yes"
  Regardless of the SwyxServer configuration, the user must set up a complex password.
  The corresponding dialog window with brief instructions is shown to the user when changing the password.
- Force complex password: "No"
  Regardless of the SwyxServer configuration, the user must set up a simple password.

Reset password:

The password reset service in Swyx Control Center allows you to reset your own password or the password of a user:

- By the administrator
  An administrator can reset a user's password by clicking on the "Reset password" button.
  The user's password is deleted and the user can no longer log in to SwyxServer. The user's existing login session is automatically terminated within one hour. The user receives an e-mail with the URL to the special Swyx Control Center dialog (SCC-URL) where he has to reset his password, help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/#context/help/PasswordReset_$

The SCC URL for resetting the password is only valid for 24 hours or until the user has changed their password.
If the user has not yet changed their password after the validity period has expired, reset the user's password to send a new email with the URL or send the generated SCC URL with the user token directly to the user, see help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/#context/help/Users-Edit-Authentication

- Initiated by the user
  The user can click on the "Forgot password" button in the login window of SwyxIt! Classic to create a new password.
  The user is redirected via the SCC URL to the special Swyx Control Center dialog where he has to reset his password, see help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/#context/help/PasswordReset_$

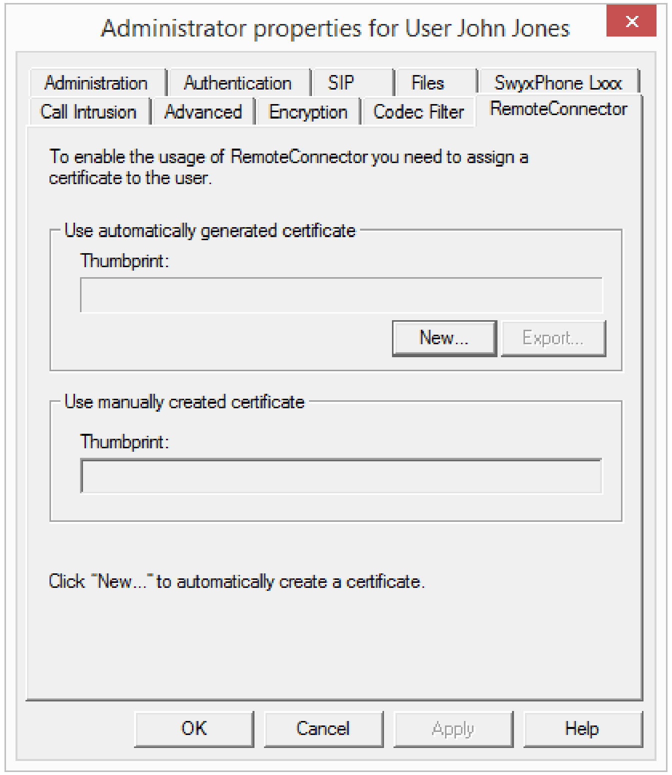
The prerequisites for resetting user passwords are the following settings for SwyxServer and the SwyxWare user:

1 E-mail server, see *7.5.9 The "Mail Server" Tab*, Page 96

2. E-mail address of the user, see *11.2.1.1 The "Administration" Tab*, Page 164

3. Configuration in Swyx Control Center: SCC-URL, see help.enreach.com/controlcenter/latest.version/web/Swyx/en-US/#context/help/GeneralSettings-System-Login

11.2.1.3THE "REMOTECONNECTOR" TAB



To enable the usage of RemoteConnector you need to assign a certificate to the user.

Click "New..." to automatically create a certificate.

This tab is used to generate the digital SwyxRemoteConnector client certificate for the user, or to assign an existing one. Via SwyxRemoteConnector, a user outside the local (LAN) or virtual private network (VPN) can log in to SwyxServer.

During a new installation or update to SwyxWare V. 13.20 you can have client certificates created automatically for all users, see *6 Swyx Connectivity Setup Tool*, Page 68

See also *26.1 Internet connection via RemoteConnector*, Page 385.

The "Use manually generated certificate" mode is supported only for compatibility with the older SwyxWare installations and is no longer recommended.

Only one of the two tab areas is active, depending on the mode selected for certificate management.

Select the desired mode via Swyx Connectivity Setup Tool.

- Generation and management of server certificates is performed automatically by SwyxWare. ("Use automatically generated certificate")

If a "404" error occurs during the connection between client and server, although all required services are running, the valid client certificate may be missing on the user's terminal device. Re-assign the client certificate to the user or generate a new one.

"Use automatically generated certificate"

"Use manually generated certificate"

"Use automatically generated certificate"

In automatic mode, the master and server certificates are generated by SwyxWare and stored in the SwyxWare database.

On the current tab, you can also have SwyxWare generate the client certificate and assign it to the user.

The certificate is automatically transferred to the user's computer on the company network after assignment.

For the generation of the client certificate, if necessary, have the password ready with which you protected the root certificate during the SwyxWare-configuration.

In SwyxON, the password for the generation of the Client certificate is not required.

How to assign an automatically generated certificate to a user

1 Click on the "New" button.
A dialog window will appear with the entry field: "Root certificate password".

2 Enter the password and confirm with"OK."
The "RemoteConnector" tab will appear in foreground.

3 Click on the "OK" button on the bottom of the tab.
The dialog window "Administrator properties for users..." is closed.
The certificate is generated.

4 Open the administrator properties and select the "RemoteConnector" tab.
The certificate's digital thumbprint is entered in the "thumbprint" field.

As soon as the user SwyxWarelogs on, or when the certificate is generated, the certificate is already logged on via RemoteConnector using an older, existing client certificate, the certificate is transferred to his computer and stored in the Windows certificate store under "Certificates - Current User | My Certificates | Certificates".

The client certificate stored only applies for the computer and the Windows user account under which is it stored in the Windows certificate storage.

In order to replace the certificate for the user, repeat steps (1) to (4).

"Use manually generated certificate"

In manual mode, the root certificate, server certificate(s) and client certificates have to be generated by you and stored in the Windows certificate storage on the corresponding computers.

In the "RemoteConnector" tab, you have to enter the thumbprint of the client certificate that you generated for the user and imported to the Windows certificate storage on the user's computer.

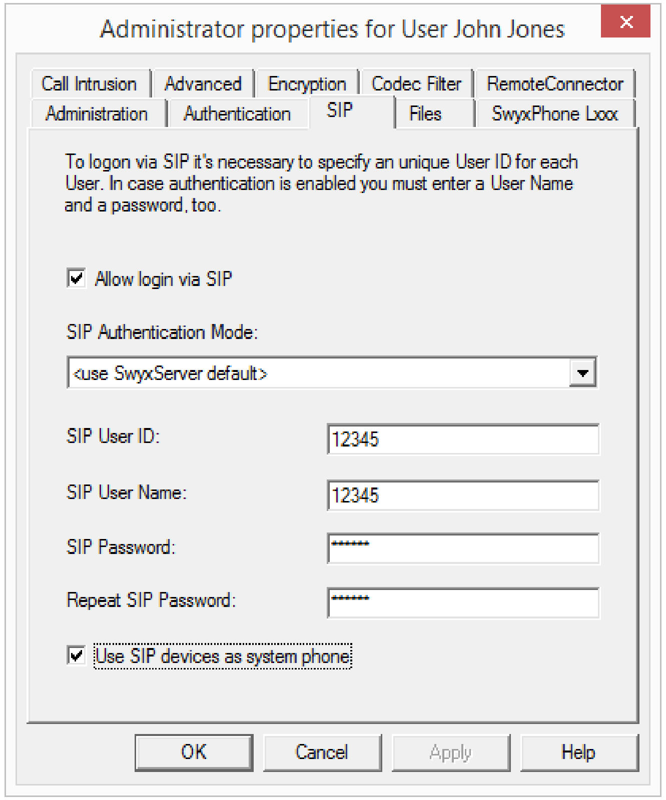
To enter the fingerprint of the client certificate

1 In SwyxWare-Administration, open "Administration Properties for Users..." and select the "RemoteConnector" tab.

2 In the area "Use manually generated certificate", enter the client certificate's thumbprint in the "thumbprint" field.

3 Confirm your entry with "OK".
The dialog window "Administrator properties for users..." is closed.
The client certificate is assigned to the user.

11.2.1.4THE "SIP REGISTRATION" TAB



To logon via SIP it's necessary to specify an unique User ID for each User. In case authentication is enabled you must enter a User Name and a password, too.

☑ Allow login via SIP

SIP Authentication Mode: <use SwyxServer default>

SIP User ID: 12345

SIP User Name: 12345

SIP Password: *******

Repeat SIP Password: *******

☑ Use SIP devices as system phone

The parameters used for authenticating SIP terminals from another manufacturer for the user are defined on this tab.

Activate the checkbox "Allow logon via SIP" if the user is generally allowed to log in to SwyxServer using a SIP device.

SIP Authentication method

Define whether the user should always or never be required to authenticate him- or herself, or required to do so in accordance with the default server settings.

SIP User Name and SIP User ID; SIP password

The data entered here are for internally logging the SIP terminal on to SwyxServer, i. e. the Administrator can freely choose a username and password here. As default, the SwyxWare user name is entered and used here as SIP user name and as SIP user ID. If a SIP terminal from another manufacturer needs other settings here, e. g. different ID and user name, you can change these defaults here. The user's password is used as password for the SIP authentication. This password is configured on the "Authentication" tab. A separate SIP password different from the SwyxWare password can also be assigned here.

See *Authentication with user name and password*, Page 166.

The logon data of the SIP provider is given directly in the configuration of the SIP trunk; the data entered here is used for internally logging the SIP terminal on to SwyxServer.

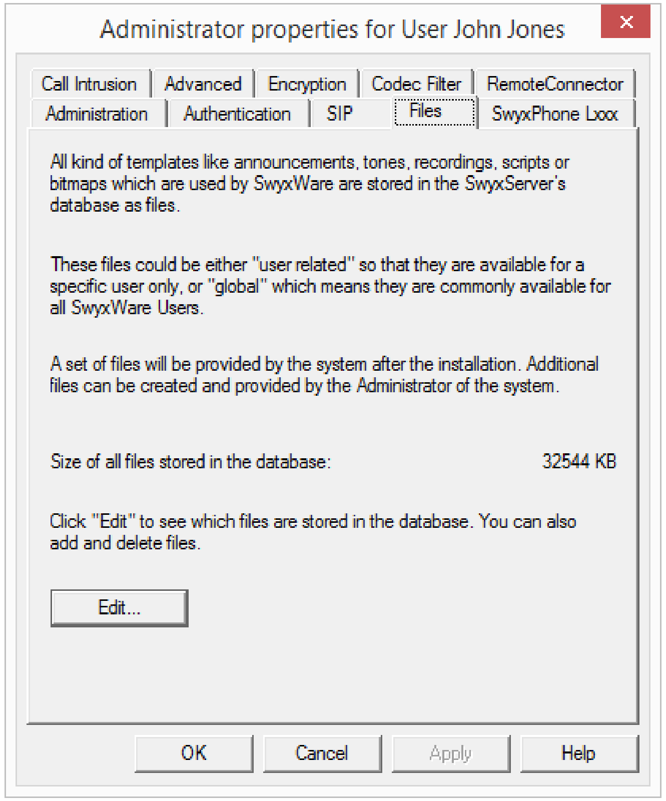
For information on how to set the SIP user ID, SIP user name and password in the SIP terminal, please see the documentation for the particular terminal.

It can happen that SIP clients (e.g. the native SIP client on a mobile device) require confirmation from the user for a passive transfer that occurs, for example, as part of scripts (voice box, remote inquiry). Since the user in this situation does not look at the device display, being on the phone at the time, this prompt is not picked up, and the connection is terminated after a short time because no confirmation is forthcoming.

Use SIP devices as system phone

Activate "Use SIP devices as system phone" to authorize SwyxCTI+ with a third party device. See *25.2.1 Configure a CTI pairing to the number of an external phone*, Page 383.

11.2.1.5THE "FILES" TAB



Administrator properties for User John Jones

All kind of templates like announcements, tones, recordings, scripts or bitmaps which are used by SwyxWare are stored in the SwyxServer's database as files.

These files could be either "user related" so that they are available for a specific user only, or "global" which means they are commonly available for all SwyxWare Users.

A set of files will be provided by the system after the installation. Additional files can be created and provided by the Administrator of the system.

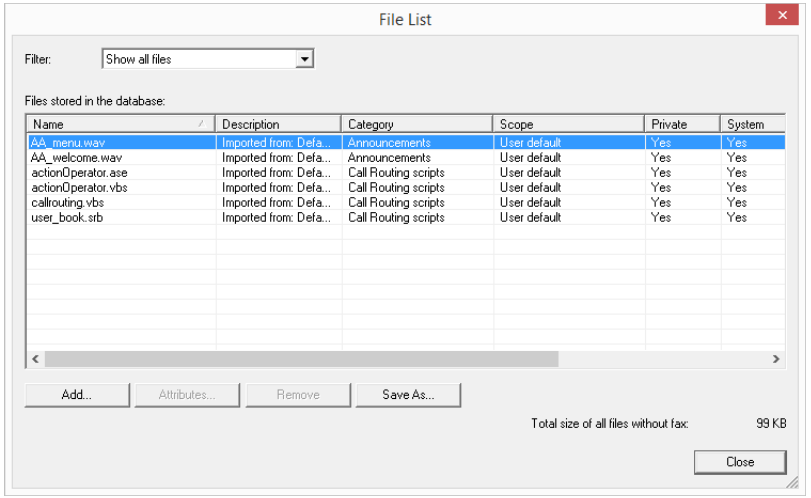
Size of all files stored in the database: 32544 KB

Click "Edit" to see which files are stored in the database. You can also add and delete files.

In the SwyxWare installation, global files such as ring tones, announcements etc. are created for all users. In addition, further files can be created specifically for this user. For example, the user can record his own announcements or generate his own scripts. These user-specific files can be edited by the administrator here.

With "Edit..." you open the list of files specifically for this user.

Here you can add or remove files, or save them under another name. The total size of all files created for this user is given.



File List

Filter: Show all files

Files stored in the database:

Name	Description	Category	Scope	Private	System
AA_menu.wav	Imported from: Defa...	Announcements	User default	Yes	Yes
AA_welcome.wav	Imported from: Defa...	Announcements	User default	Yes	Yes
actionOperator.ase	Imported from: Defa...	Call Routing scripts	User default	Yes	Yes
actionOperator.vbs	Imported from: Defa...	Call Routing scripts	User default	Yes	Yes
callrouting.vbs	Imported from: Defa...	Call Routing scripts	User default	Yes	Yes
user_book.srb	Imported from: Defa...	Call Routing scripts	User default	Yes	Yes

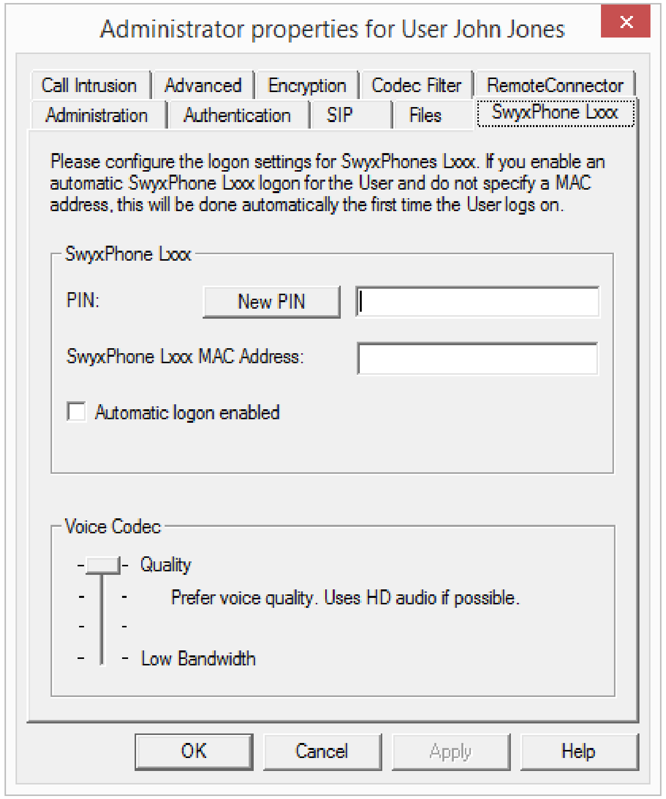
Total size of all files without fax: 99 KB

With "Attributes...", the properties of the files can be changed, so that these user-specific files (e.g. a new announcement within a script) can also be made usable for other users.

With "Add...", the administrator can make further files, such as announcements and ring tones, available for the user.

See *File Properties*, Page 100.

11.2.1.6THE TAB "SWYXPHONE LXXX"



Administrator properties for User John Jones

Please configure the logon settings for SwyxPhones Lxxx. If you enable an automatic SwyxPhone Lxxx logon for the User and do not specify a MAC address, this will be done automatically the first time the User logs on.

SwyxPhone Lxxx

PIN: New PIN

SwyxPhone Lxxx MAC Address:

☐ Automatic logon enabled

Voice Codec

Quality

Prefer voice quality. Uses HD audio if possible.

Low Bandwidth

SwyxPhone Lxxx

Here the log in of SwyxPhone Lxxx is defined.

If the user logs SwyxPhonein onSwyxServer, the user will be prompted to enter his or her PIN if the login is not automatic. SwyxServer Can identify the user based on the PIN. This means that the specific button configuration of this user (e. g. speed dials or function keys) will be transferred to any SwyxPhone the user logs on to, and the user can be reached instantly at this SwyxPhone under his or her own phone numbers. It is not possible to assign the same PIN more than once. You can enter a PIN for this user or create a PIN automatically. When you close the tab, the PIN entered will be checked to ensure it is unique.

Activate the checkbox "Automatic logon enabled" in order to log the user on without entering the PIN. In this case, after the has been SwyxPhone restarted this user is permanently logged in to this SwyxPhone. The MAC address must be configured so that SwyxServer can assign SwyxPhone to the appropriate user on automatic logon. If you do not enter any information here, the SwyxServer will note the MAC address of the SwyxPhone when the user logs in for the first time. If a user would like to exchange his/her telephone for another one, you must delete the entry field for the MAC address so that the MAC address of the new telephone can be applied.

All phones of the SwyxPhone family request entry of a PIN in the display and can therefore easily be logged in by the user.

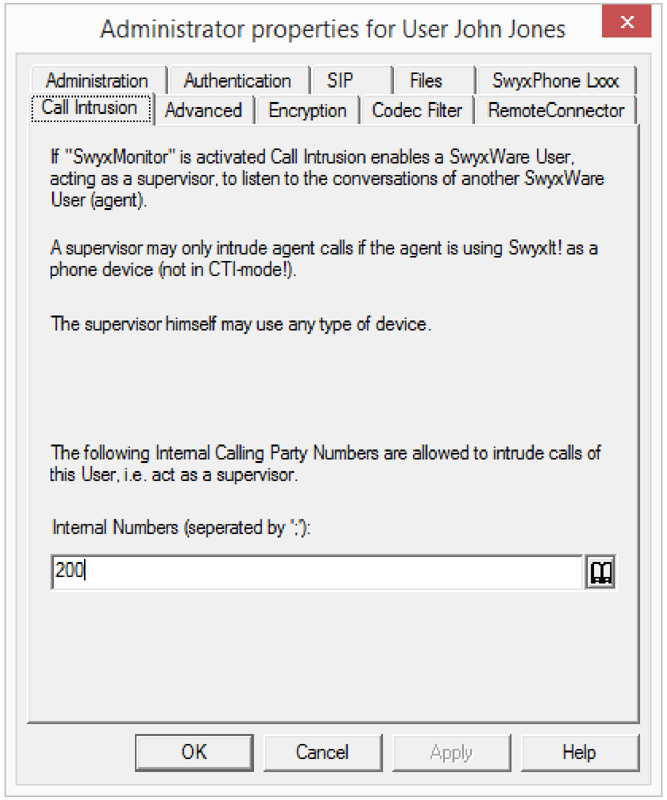
Activate the appropriate checkbox if SwyxPhone is always to compress voice data.

Speech Codec

With the help of the Codec you can specify how SwyxPhone Lxxx should compress the voice for transmission. The following options are available:

- Highest voice quality
  If possible, the voice data is transferred in HD audio quality. An attempt is made in this case to use Codecs in the order G.722/ G.711a/G.711µ/G.729.
- Prefer voice quality
  Voice data is only compressed if necessary. An attempt is made in this case to use Codecs in the order G.729/G.711a/G.711µ. The codec G.722 is never used.
- Prefer low bandwidth
  To spare bandwidth, the voice data is compressed. An attempt is made in this case to use Codecs in the order G.729/G.711a/G.711µ. The codec G.722 is never used.
- Use lowest bandwidth
  In order to use the lowest bandwidth, the voice data is always compressed. The Codec G.729 is used.
  See *26.2.1 Small Office - Connection*, Page 388.

11.2.1.7THE "CALL INTRUSION" TAB


Administrator properties for User John Jones

If "SwyxMonitor" is activated Call Intrusion enables a SwyxWare User, acting as a supervisor, to listen to the conversations of another SwyxWare User (agent).

A supervisor may only intrude agent calls if the agent is using SwyxIt! as a phone device (not in CTI-mode!).

The supervisor himself may use any type of device.

The following Internal Calling Party Numbers are allowed to intrude calls of this User, i.e. act as a supervisor.

Internal Numbers (seperated by ';'): 200

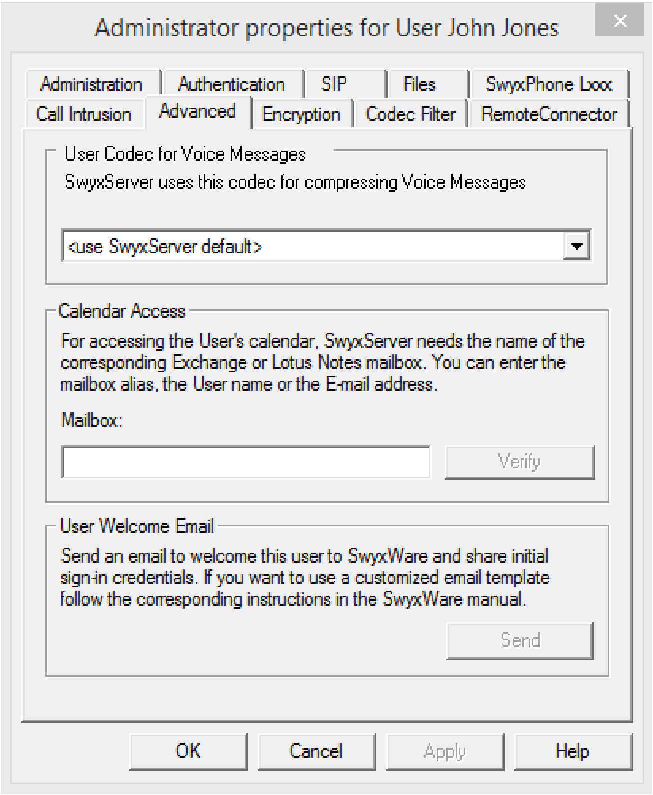
If the Option Pack SwyxMonitor is installed, a SwyxWare user (Supervisor) can intrude into an existing call of another SwyxWare user (Call Agent). A prerequisite is that the Agent is speaking via SwyxIt! Classic (not in CTI mode). The Supervisor can use any terminal.

Specify here which internal numbers may intrude into this Agent's calls. You can enter both group numbers and several numbers separated by semicolon. The permission to intrude relates to all this Agent's numbers.

See also .

help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/call_intrusion_$.

11.2.1.8THE "ADVANCED" TAB



Administrator properties for User John Jones

User Codec for Voice Messages

SwyxServer uses this codec for compressing Voice Messages

<use SwyxServer default>

Calendar Access

For accessing the User's calendar, SwyxServer needs the name of the corresponding Exchange or Lotus Notes mailbox. You can enter the mailbox alias, the User name or the E-mail address.

Mailbox:

User Welcome Email

Send an email to welcome this user to SwyxWare and share initial sign-in credentials. If you want to use a customized email template follow the corresponding instructions in the SwyxWare manual.

User codec for voice messages

Specify here whether the general server settings are used for the compression of voice messages or whether you select a user-specific compression.

Calendar Access

Enter the Mailbox alias, the name, or the email address which is assigned to this user on the Microsoft Exchange server or the Lotus/ IBM/HCL Domino Server. The necessary information (i. e. the user’s calendar) for calendar-based Call Management will then be called from this server. Click "Verify" to check whether your entries are correct.

Welcome E-mail

Send the user an Email with his registration data and most important configurations.

On Swyx clients (SwyxIt! Classic, Swyx Desktop for macOS, , Swyx Mobile) the configurations are transferred automatically by the user calling the corresponding URL in the welcome e-mail and thus being forwarded directly to his client.

Most of the configurations are linked with the template for the Welcome emails via variables. When sending, the variables are then automatically replaced by the configurations. A list of all the variables is provided as a comment at the beginning of the template.

Some configurations for Swyx clients are not SwyxWare Administration-defined in the template, but are preset by values in the template for the welcome e-mail or are automatically set by the installation, see *How to edit the template for welcome E-mails*, Page 98.

If you do not enable the "New users must change their password the first time they perform a login" option, the user will not receive a pre-configured password in their welcome email.

You have the following options for sending Welcome emails:

- Use standard email
  The standard email incorporates the most important configurations needed by the user for registration and telephoning.
- Adapt email individually
  Edit the template from which the welcome E-mails are generated before sending the mail. To add or change configurations, see *How to edit the template for welcome E-mails*, Page 98.

How to send a Welcome email

1. Edit the template for welcome E-mails as required.
2. Click on the "Send welcome E-mail" button.
   The welcome E-mail is sent to the E-mail address which you have configured for the user when setting up or editing.

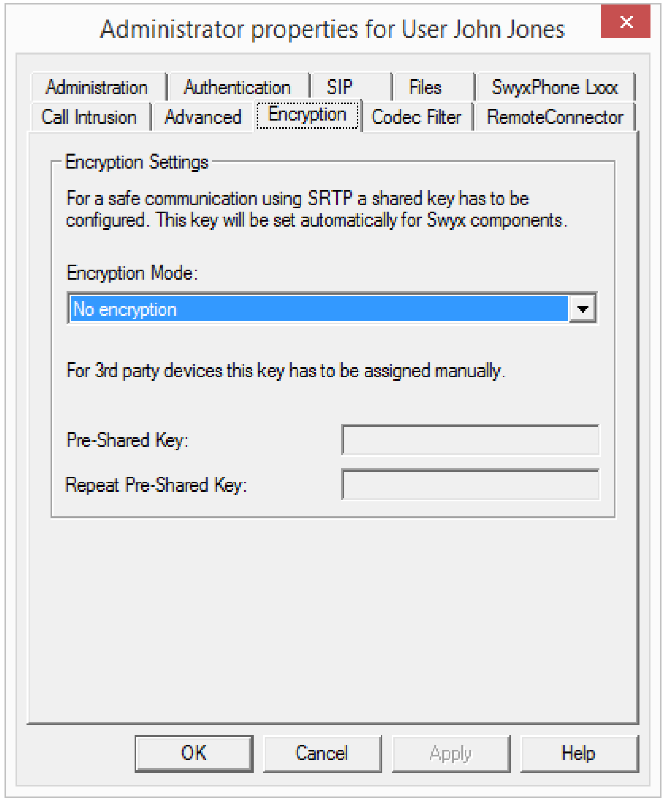
You can also, for example, use the SwyxWare PowerShell module to send Standard and individual welcome emails to selected user groups, see *E.1 PowerShell support*, Page 424.

> ⚠ Settings which have already been determined before accessing the configuration URL in Swyx Mobile apps are overwritten with the settings in the URL. Settings which are not in the URL are maintained in Swyx Mobile apps.

> ⚠ Uses of the Swyx Mobile apps can also skip the automatic configuration and therefore maintain the settings already determined in the app.

> ℹ Users of Swyx Mobile apps can use the URLs you send them several times, e. g. to restore configurations.

11.2.1.9THE "ENCRYPTION" TAB


Administrator properties for User John Jones

For a safe communication using SRTP a shared key has to be configured. This key will be set automatically for Swyx components.

Encryption Mode: No encryption

For 3rd party devices this key has to be assigned manually.

Pre-Shared Key:

Repeat Pre-Shared Key:

Encryption mode

This is where you specify the mode of encryption. The following encryption modes are available:

- No encryption
  If "No encryption" is selected, the voice data is not encrypted.
- Encryption preferred
  When "Encryption preferred" is selected, the voice data is only encrypted if the call partner has configured either "Encryption preferred" or "Encryption mandatory". If this is not the case, the voice data is not encrypted, but phoning is still possible.

- Encryption mandatory
  When "Encryption mandatory" is selected, voice data encryption is obligatory. This means that either encryption always occurs or the call is aborted with the reason "Incompatible encryption settings". This can be the case, for example, when the call partner has configured the mode "No encryption".

> If the encryption mode was set to "No encryption" within the server properties, the mode is likewise set to "No encryption" here; if "Encryption mandatory" was configured there, then the setting "Encryption mandatory" also appears here. In both cases, the mode cannot be changed. The field is then deactivated.

See *21 Encryption*, Page 342.

Key (PreSharedKey)

To ensure secure communication by SRTP, a common key (PreSharedKey) must be defined between SwyxServer and the relevant component.

For all components which use the SwyxWare database (e.g. SwyxIt! Classic, PhoneMgr, ConferenceMgr, LinkMgr, Gateway), this key is automatically generated by SwyxServer and distributed to the relevant component, once again encrypted.

> The key created automatically generated by SwyxServer serves as an example only. For security reasons, it is highly recommended to manually replace it by an individually selected key.

See *21.1 Encryption within SwyxWare*, Page 342.

However, in a few cases the key must be specified manually:

If the user uses a SIP phone (with MIKEY support) from another manufacturer, there is no automatic distribution of a key from SwyxServer to the device. It must therefore be entered manually in this case. The key must then be stored in the device as well, e.g. via the phone's web interface.

Other exceptions, which may e.g. require manual input of the key, are:

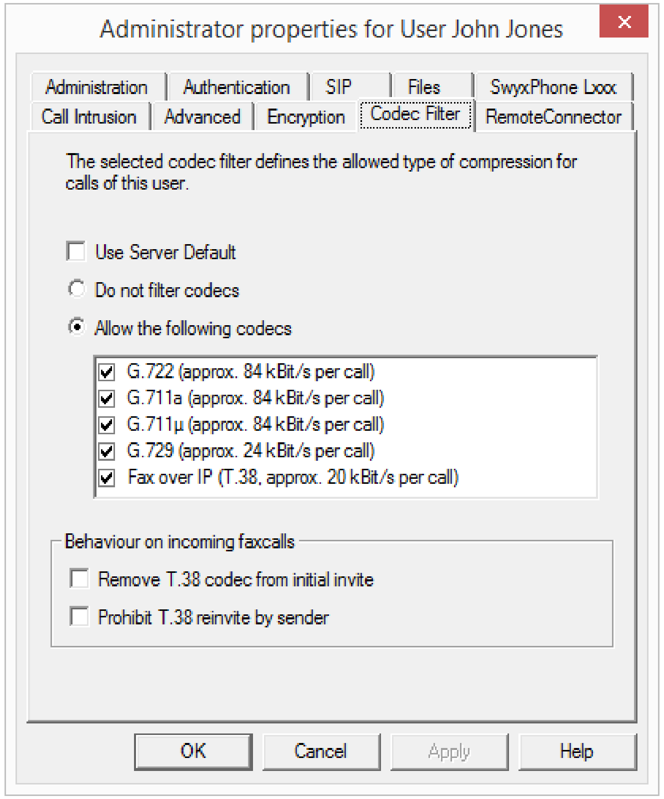
- Connection of two SwyxServers via a SwyxLink
  See *The "Encryption" tab*, Page 307.
- SIP link for the use of VoIP services of e.g. service providers

However, these must be configured within the trunk properties.

This is how you specify the encryption mode in the user properties.

1. Start the SwyxWare Administration and log in to the SwyxServer.
2. Click the user entry with the right mouse button to open the shortcut menu.
3. Select "Properties".
4. Select the "Encryption" Tab.
5. In the field "Encryption mode", choose from:
   - No encryption
   - Encryption preferred
   - Encryption mandatory
6. If the user uses a device from another manufacturer, enter the key in the "Key" field. You must then set this in the device as well (e. g. via a web interface).
7. Click on "OK".

11.2.1.10THE "CODEC FILTER" TAB



The selected codec filter defines the allowed type of compression for calls of this user.

□ Use Server Default

○ Do not filter codecs

● Allow the following codecs

- ☑ G.722 (approx. 84 kBit/s per call)
- ☑ G.711a (approx. 84 kBit/s per call)
- ☑ G.711µ (approx. 84 kBit/s per call)
- ☑ G.729 (approx. 24 kBit/s per call)
- ☑ Fax over IP (T.38, approx. 20 kBit/s per call)

Behaviour on incoming faxcalls

□ Remove T.38 codec from initial invite

□ Prohibit T.38 reinvite by sender

Here you can specify which compression type (Codecs) you want to permit for this user's calls, and filter out T.38 in the setting up of a fax connection.

You can choose from:

- Use server standard setting (default setting)
  If you want to use for this user the settings that were globally configured in the server properties, activate this option.
- Do not filter Codecs
  When "Do not filter Codecs" is selected, all media data whatever the Codec is forwarded for this user to the destination (transparent mode). This setting allows foreign Codecs unknown to SwyxServer to be used, e.g. Video. This option can only be activated when the option "use default server setting" is deactivated.
- Selection of the Codecs that should be permitted
  Here you can specify the compression type for this user's calls. The Codecs can only be selected when the option "Use server standard setting" is deactivated.
  - G.722 (around 64 kbit/s per call)
  - G.711a (around 64 kbit/s per call)
  - G.711µ (around 64 kbit/s per call)
  - G.729 (around 24 kbit/s per call)
  - Fax over IP (T.38, around 20 kbit/s per call)

If voice data is used with a Codec which is not permitted for this user, the call is aborted. An error message follows.

See *7.5.20 The "Default Codec Filter" Tab*, Page 113.

Behavior in case of fax connections

When a fax connection is set up, the T.38 protocol is negotiated between the two devices involved. Certain variants of this negotiation may not be supported by some IP adapters. Use the following filter options to establish compatibility with such devices.

Remove T.38 codec from initial invite

Some IP adapters cannot correctly interpret an initial connection request which includes T.38 as well as voice Codecs.

If this option is set, SwyxServer removes T.38 from the initial connection request. The fax devices first set up a voice connection and then switch to the fax protocol T.38 because of the fax tone (CED tone, 2100Hz).

Prohibit T.38 reinvite by sender

The receiving fax device switches to T.38 after detecting the fax tone (CED tone, 2100Hz). Alternatively, the switch to T.38 can be carried out by the sending fax device. Some IP adapters don't support switching by the sender.

If this option is set, SwyxServer suppresses a switch to T.38 by the sender.

If the receiving side involves a combined phone/fax device (fax switch), a fax data transmission is impossible when the option "Prohibit T.38 reinvite by sender" is activated.

The option "Use server standard setting" is activated as default in a new installation of SwyxWare, or in an update. The selection of the Codec filters, as of the options of the area "Action on fax receipt", is accordingly deactivated. The options cannot be selected.

11.2.2 DIALOGUE "PHONE NUMBERS..."

All numbers that should be assigned to a user are specified here.

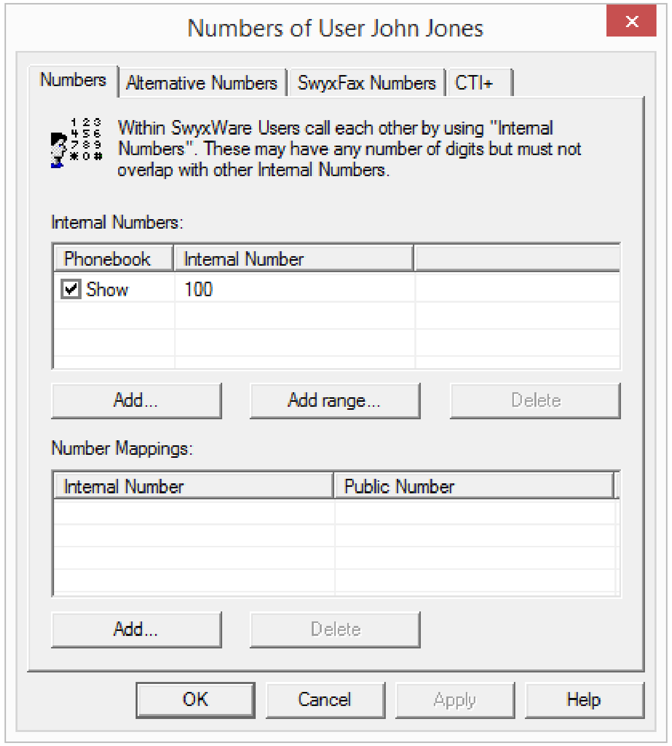
- Numbers for voice connections (telephone or computer client)
- Alternative Numbers
- SwyxFax Numbers

The "Numbers" Tab

The "Alternative Numbers" Tab

The "SwyxFax Numbers" Tab

11.2.2.1 THE "NUMBERS" TAB



Within SwyxWare Users call each other by using "Internal Numbers". These may have any number of digits but must not overlap with other Internal Numbers.

Internal Numbers:

Phonebook	Internal Number
☑ Show	100

Number Mappings:

Internal Number	Public Number

The voice numbers for the user are assigned here. It can be specified whether this number appears in the phonebook. The mapping of a public number to the user's internal number is also configured here.

Internal number

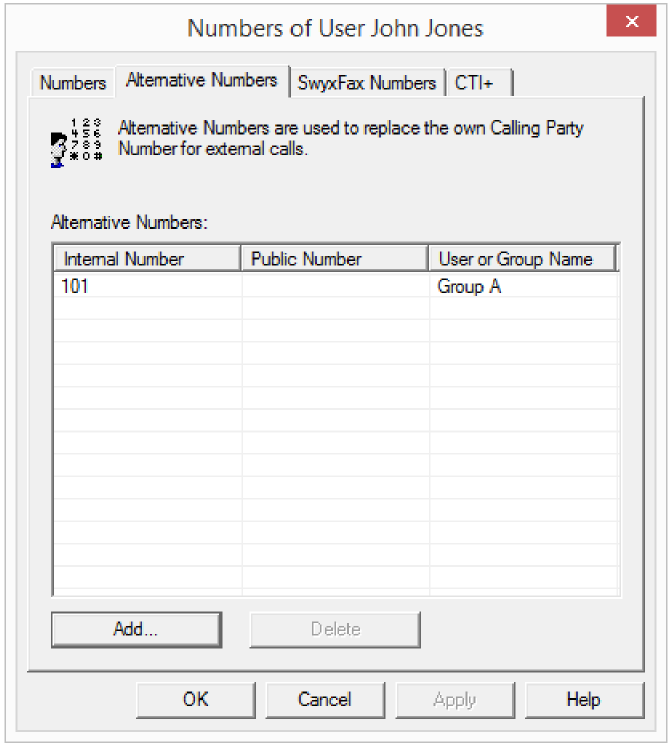
For each of these entries you can indicate whether or not the number should be shown in the SwyxWare Global Phonebook. You can delete individual entries by highlighting them and then clicking "Remove". If you would like to add more numbers, click "Add". If you would like to assign an entire number range to this user, click "Add range...". A Wizard will help to specify additional number mapping between the internal and the public number.

Number mappings

In this section you will see a list of the public numbers or SIP URIs directly assigned to this SwyxWare user.

You can delete individual entries by highlighting them and then clicking "Remove". If you would like to add more numbers, click "Add". A Wizard will help to specify additional number mapping between the internal and the public number.

11.2.2.2THE "ALTERNATIVE NUMBERS" TAB



Alternative Numbers are used to replace the own Calling Party Number for external calls.

Alternative Numbers:

Internal Number	Public Number	User or Group Name
101		Group A

Alternative numbers can be specified here, which the SwyxWare user signals to the call partner on outgoing calls.

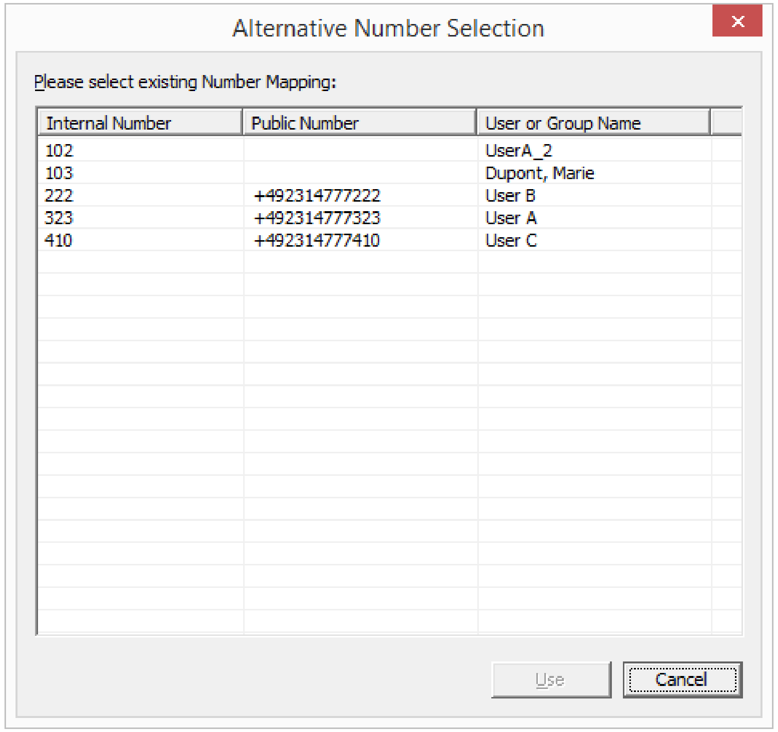
Which alternative number the user finally signals is defined on a line in the SwyxIt! Classic/SwyxPhone. Alternative numbers are marked there by the addition Alternative number. See *11.2.6.6 The"Line keys" Tab*, Page 190.

> *Example:*
>
> *The administrator can allow every SwyxWare user to signal the operator's number (+44204666100) externally, by adding this number as an alternative number to the group "Everyone". This allows every user to configure this number on the line button as outgoing number.*

To remove the assignment of the alternative number, highlight it and click on "Remove".

If the deleted number is specified within the user configuration as the number/URI for outgoing calls, then outgoing calls that should go via this number are discarded. So use another number/URI for incoming and outgoing calls.

To add an Alternative Number, which the SwyxWare user should signal on outgoing calls, click on "Add".



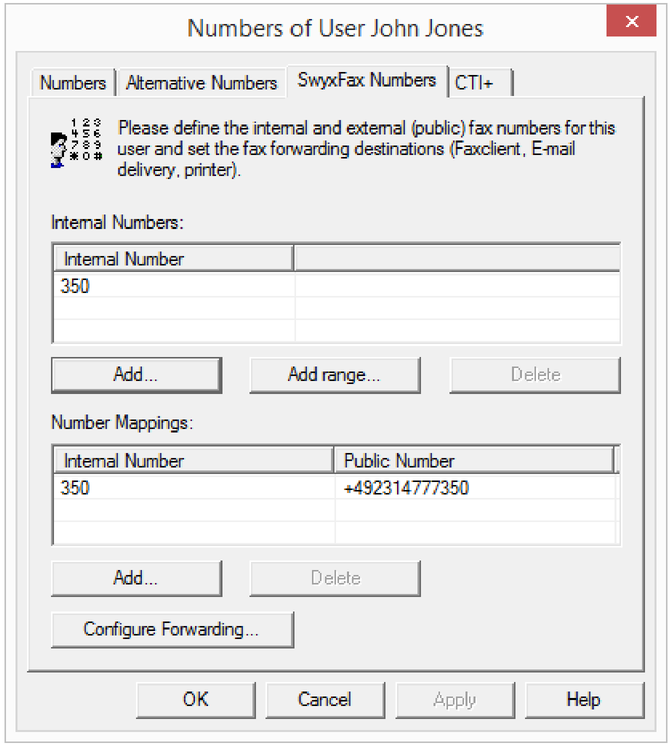
Please select existing Number Mapping:

Internal Number	Public Number	User or Group Name
102		UserA_2
103		Dupont, Marie
222	+492314777222	User B
323	+492314777323	User A
410	+492314777410	User C

Available for selection are all numbers which are assigned within SwyxWare and are not allocated to this user. Highlight the alternative number you want, and click "Use". Close the tab with "OK" to save the changes you have made.

Next, configure the number/URI for outgoing calls for the SwyxWare user on a specific line button. See *11.2.6.6 The"Line keys" Tab*, Page 190.

11.2.2.3THE "SWYXFAX NUMBERS" TAB



Please define the internal and external (public) fax numbers for this user and set the fax forwarding destinations (Faxclient, E-mail delivery, printer).

Internal Numbers:

Internal Number	
350	

Number Mappings:

Internal Number	Public Number
350	+492314777350

The fax numbers for the user are assigned here. The mapping of a public number to the user's internal number is also configured here.

"Fax Forwardings..." is used to specify how the fax documents reach the recipient: as a Faxmail with attachment (PDF and/or TIFF), in the SwyxFax Client inbox, or as a printout to a printer. Several different recipients may also be defined here.

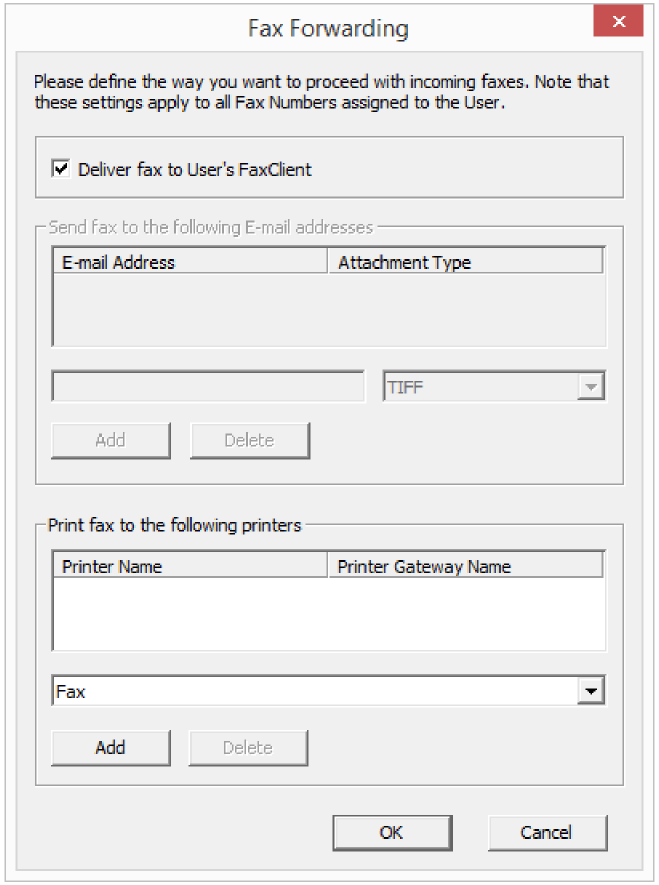
Internal numbers

You can delete individual entries by highlighting them and then clicking "Remove". If you would like to add more numbers, click "Add". If you would like to assign an entire number range to this user, click "Add range...". A Wizard will help to specify additional number mapping between the internal and the public number.

Number mappings

In this section you will see a list of the public numbers or SIP URIs directly assigned to this SwyxWare user.

You can delete individual entries by highlighting them and then clicking "Remove". If you would like to add more numbers, click "Add". A Wizard will help to specify additional number mapping between the internal and the public number.



Fax Forwarding

Please define the way you want to proceed with incoming faxes. Note that these settings apply to all Fax Numbers assigned to the User.

☑ Deliver fax to User's FaxClient

Send fax to the following E-mail addresses

E-mail Address	Attachment Type

Print fax to the following printers

Printer Name	Printer Gateway Name

Fax

Transfer

Here you can indicate whether the recipient of the forwarded fax document is a SwyxFax Client logged in under the current user, an e-mail address or a printer. You can choose from several options:

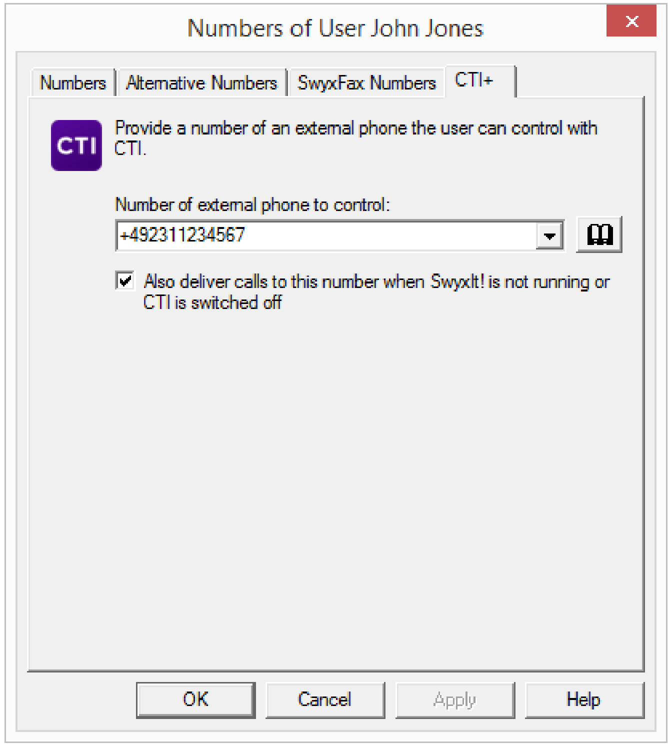
- SwyxFax Client
  Incoming fax documents will appear in the interface in the SwyxFax Client of the configured user after they are forwarded.
- E-mail with fax attachment
  In this case, enter the e-mail address, e.g. CarolJones.company.com. The forwarded fax documents are received by the addressee as an e-mail. In this case the fax is attached to the e-mail in the defined format (TIFF and/or PDF). If "TIFF and PDF" is selected, the e-mail will include two attachments.
- Printing
  In this case, select one or more installed printers in the selection list. Forwarding to a printer takes place via the SwyxFax Printer Gateway (*24.11 SwyxFax Printer Gateway*, Page 378).

If you define forwarding for one fax extension number only per e-mail, the fax will be deleted from the SwyxFax Server management after it is transferred to the e-mail server.

11.2.2.4THE "CTI+" TAB

On the CTI+ tab, you define the link to a number, with which the user can control an external phone. With the option "Also deliver calls to this number when SwyxIt! Classic is not running or CTI is switched off" you ensure that incoming calls are forwarded to the external phone independently from SwyxIt! Classic, even if the computer of the user is shut down or CTI is deactivated.

You need an appropriate license for the use of SwyxCTI+. See *25.2.1 Configure a CTI pairing to the number of an external phone*, Page 383.



Provide a number of an external phone the user can control with CTI.

Number of external phone to control:

+492311234567

☑ Also deliver calls to this number when SwyxIt! is not running or CTI is switched off

11.2.3 THE "BUTTONS..." DIALOG

In this dialog you can specifically define the button assignment, e.g. speed dials and shortcuts, line buttons and hotkeys, as well as the list settings and the configuration for the various SwyxPhone types. This tab is identical to the tab of the same name in the "Ringing and Phone Properties..." dialog which opens if you click "Client...".

See **11The "Client..." Dialog**, Page 185.

The "Speed Dials" Tab

The"Line keys" Tab

Tab "SwyxPhone"

The "Shortcuts" Tab

The "Lists" Tab

The "Keyboard" Tab

11.2.4 THE "CALL ROUTING MANAGER..." DIALOG

The Call Routing Manager will open here, together with the selected user’s Rule Book.

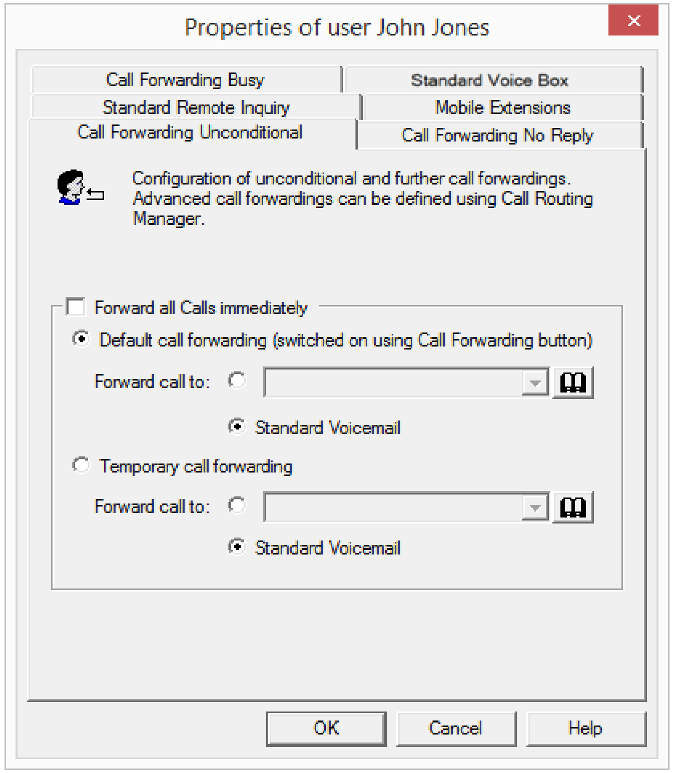
Please note that scripts created using use of the Graphical Script Editor. must be signed for your SwyxServer. Otherwise the Call Routing Manager cannot apply them in its set of rules.

See *22.1 Call Routing Manager and Graphical Script Editor*, Page 347.

11.2.5 THE "CALL FORWARDING..." DIALOG

The "Forwardings..." dialog specifies both the forwardings (unconditional, no reply, if busy) for a user, and also the standard Voice Box, standard remote inquiry and the configuration for the mobile extension (parallel calls).

11.2.5.1THE "CALL FORWARDING UNCONDITIONAL" TAB



Properties of user John Jones

Call Forwarding Busy | Standard Voice Box | Standard Remote Inquiry | Mobile Extensions | Call Forwarding Unconditional | Call Forwarding No Reply

Configuration of unconditional and further call forwardings. Advanced call forwardings can be defined using Call Routing Manager.

□ Forward all Calls immediately

● Default call forwarding (switched on using Call Forwarding button)

Forward call to: ○ [ ] ● Standard Voicemail

○ Temporary call forwarding

Forward call to: ○ [ ] ● Standard Voicemail

The properties for unconditional forwarding can be defined in this page. These settings are immediately effective when the "Redirection" button on the user interface is activated.

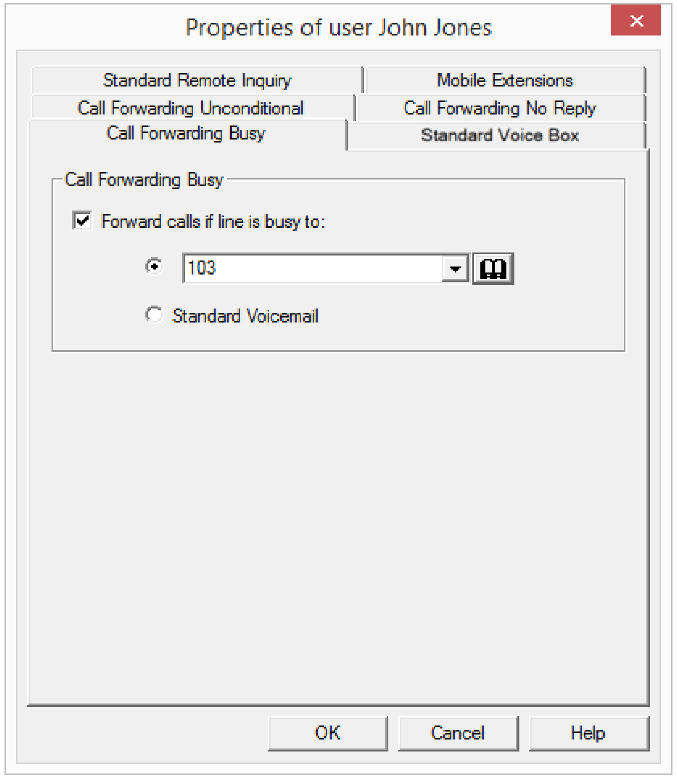
You can specify a default or temporary destination for forwarding of all calls for this user. Options here include Call Forwarding to another number or to Standard Voice Box. If the number field remains empty, no Call Forwarding is performed.

In addition, you can specify whether Call Forwarding Unconditional is to be activated as soon as the tab is closed.

If the user has not defined any rules or redirections a default call handling will be activated.

See *22.2 Default call handling*, Page 348.

11.2.5.2THE "CALL FORWARDING BUSY" TAB



Properties of user John Jones

Standard Remote Inquiry | Mobile Extensions | Call Forwarding Unconditional | Call Forwarding No Reply | Call Forwarding Busy | Standard Voice Box

Call Forwarding Busy

☑ Forward calls if line is busy to:

● 103

○ Standard Voicemail

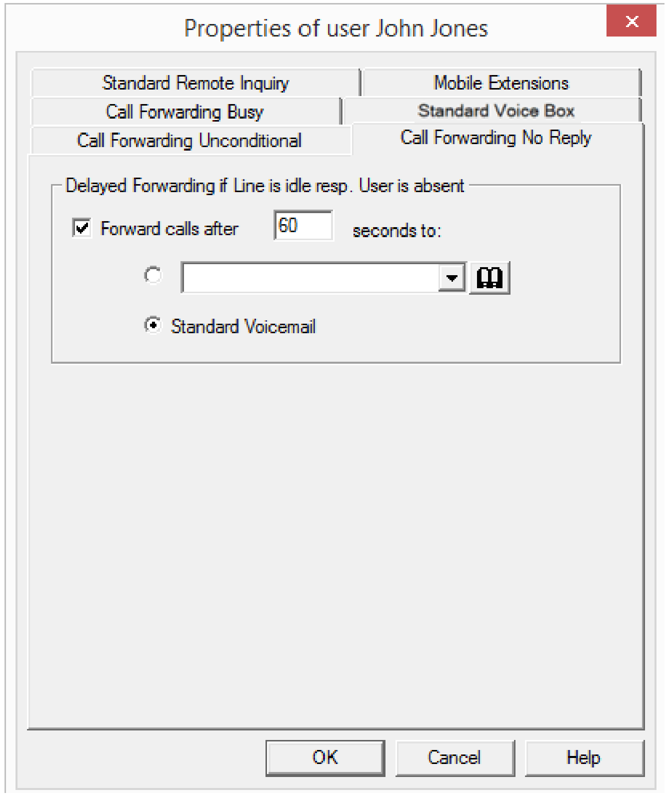
Call Forwarding Busy

Here you can define the Call Forwarding to be performed if the line is busy. You can choose Call Forwarding to your Standard Voice Box, to another phone number or user.

If the user has not defined any rules or redirections a default call handling will be activated.

See *22.2 Default call handling*, Page 348.

11.2.5.3THE "CALL FORWARDING NO REPLY" TAB



Delayed Forwarding if Line is idle resp. User is absent

☑ Forward calls after 60 seconds to:

○

● Standard Voicemail

Call Forwarding No Reply

On this page you can set up Call Forwarding after a period of your choice if the line is idle or the user is absent. Options here include Call Forwarding to another number or to Standard Voice Box.

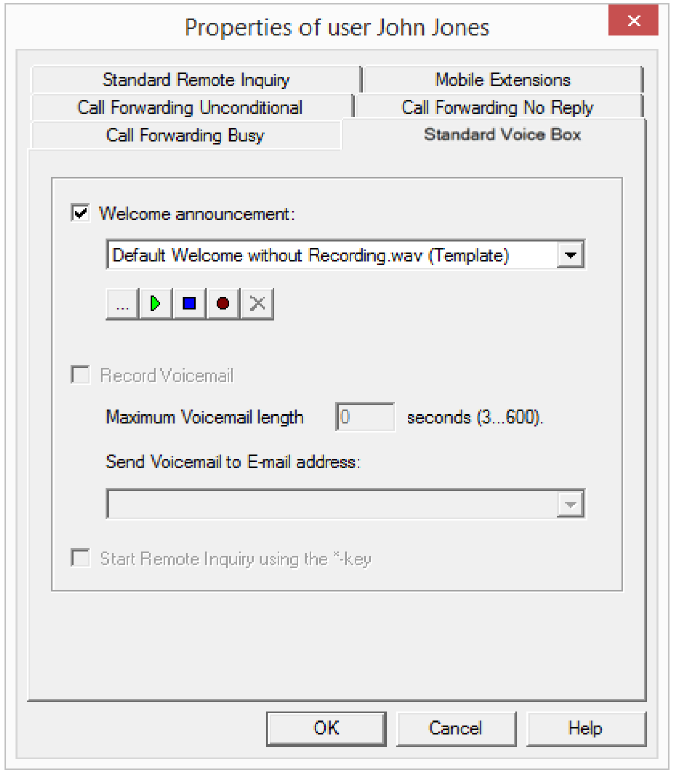
For all new users, the option "Forward calls after 60 seconds", and the checkbox "Standard" will be activated.

If a user is not logged in, any calls are directly forwarded to the Standard Voice Box by default.

If the user has not defined any rules or redirections a default call handling will be activated.

See *22.2 Default call handling*, Page 348.

11.2.5.4STANDARD VOICE BOX" TAB



☑ Welcome announcement:

Default Welcome without Recording.wav (Template)

□ Record Voicemail

Maximum Voicemail length 0 seconds (3...600).

Send Voicemail to E-mail address:

□ Start Remote Inquiry using the *-key

Here you can indicate whether a welcome announcement is to be played when a call is forwarded to the Standard Voice Box. You can also specify this text here.

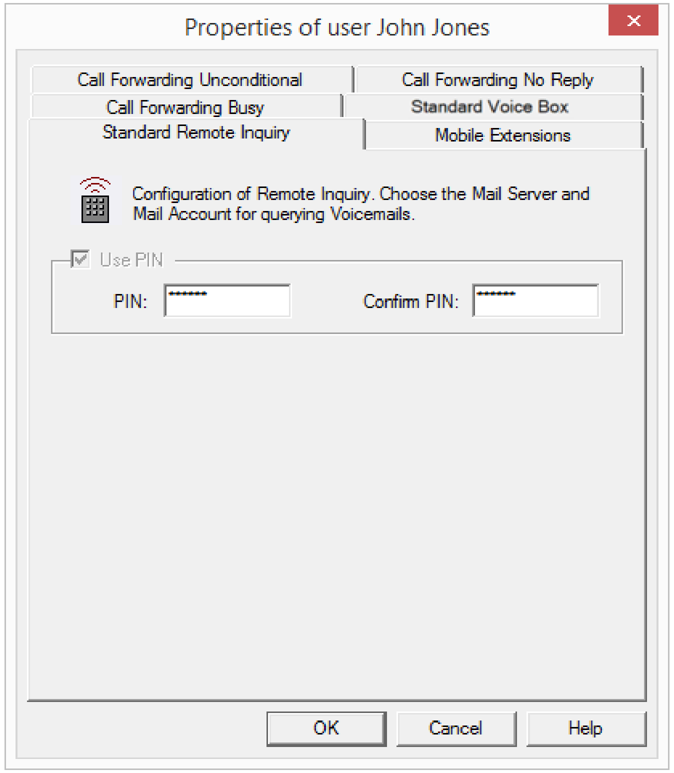
Furthermore you can specify whether voice message is to be recorded at all. In addition, you can set the maximum length of the voice message in seconds and enter the email address to which the recorded voice message should be sent.

Define here whether the user may start a remote inquiry during the standard Voice Box using the * key.

In general, a differentiation is made between the Standard and a special voice message. A special voice message is created within the Call Routing Manager for a special application. The standard voice message configured here is the message that is applied as default voice message in all rules.

See also https://help.enreach.com/cpe/latest.version/CRM/Swyx/en-US/index.html#context/help/default_voicemail_$

11.2.5.5TAB "STANDARD REMOTE INQUIRY"



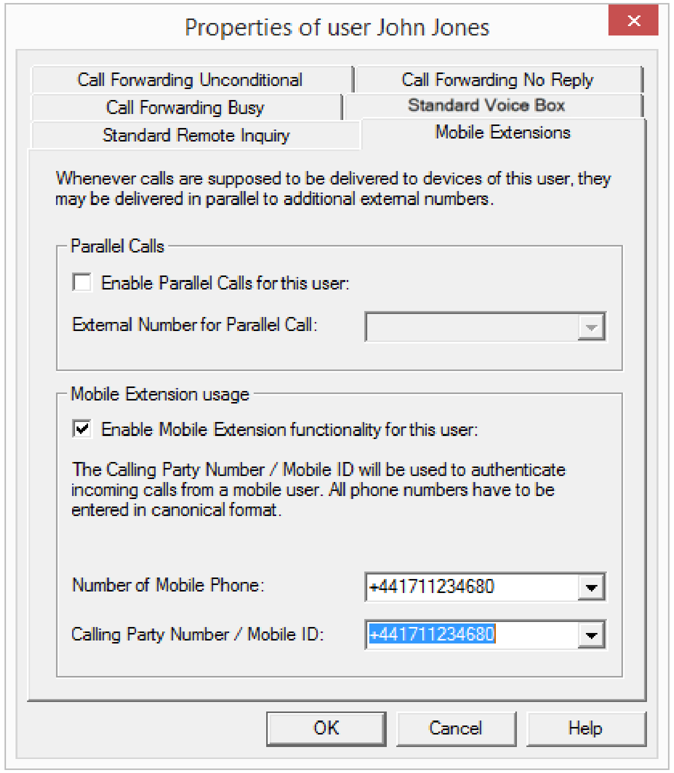
Configuration of Remote Inquiry. Choose the Mail Server and Mail Account for querying Voicemails.

☑ Use PIN

PIN: *******   Confirm PIN: *******

Remote Inquiry allows you to listen to your voice messages and to change Call Forwarding Unconditional from any telephone line. When a user is called at his or her own SwyxWare number, he or she identifies him/herself to SwyxWare with a PIN; only then can he or she listen to, repeat, or delete new voice messages and afterwards all existing voice messages.

11.2.5.6 THE "MOBILE EXTENSIONS" TAB



Whenever calls are supposed to be delivered to devices of this user, they may be delivered in parallel to additional external numbers.

Parallel Calls

□ Enable Parallel Calls for this user:

External Number for Parallel Call:

Mobile Extension usage

☑ Enable Mobile Extension functionality for this user:

The Calling Party Number / Mobile ID will be used to authenticate incoming calls from a mobile user. All phone numbers have to be entered in canonical format.

Number of Mobile Phone: +441711234680

Calling Party Number / Mobile ID: +441711234680

Parallel calls can be set up on this page.

Parallel Calls

In the event of an incoming call, not only internal terminals but also external terminals, such as for example the user's mobile phone, can ring simultaneously. The call is then handled via the terminal that first accepts the call.

If calls to this user are to be forwarded simultaneously to external terminals too, activate the checkbox "Enable Parallel Calls for this user".

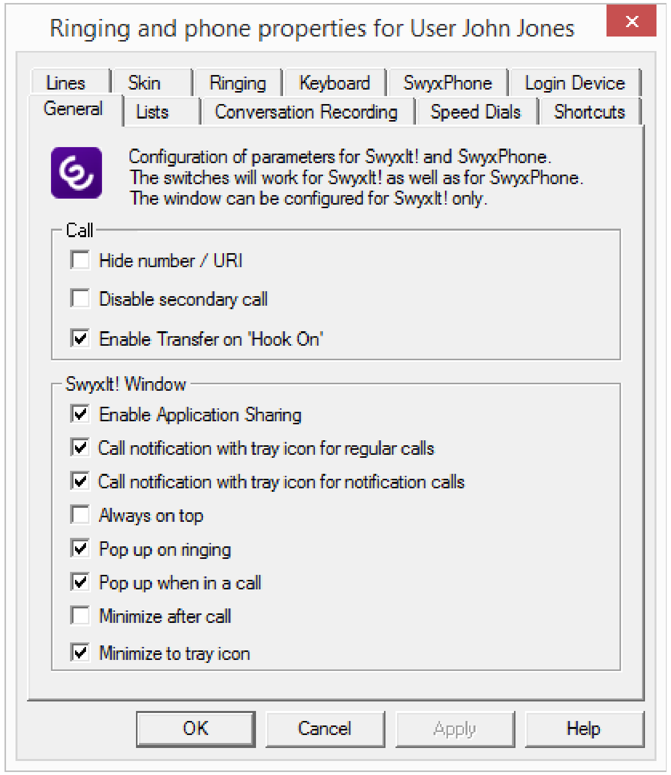
Enter the external numbers to which the call is additionally to be delivered, in canonical format (e. g. +442044455566). If you would like to deliver the call to several external terminals, separate the numbers by a semi-colon.

Please enter only **external** numbers. If you want to route parallel calls to internal Users, please create a group (parallel) to do this.

11.2.6 THE "CLIENT..." DIALOG

This dialog groups all the properties of the Telephony Client together.

11.2.6.1 THE "GENERAL" TAB



Configuration of parameters for SwyxIt! and SwyxPhone.
The switches will work for SwyxIt! as well as for SwyxPhone.
The window can be configured for SwyxIt! only.

Call

□ Hide number / URI

□ Disable secondary call

☑ Enable Transfer on 'Hook On'

SwyxIt! Window

☑ Enable Application Sharing

☑ Call notification with tray icon for regular calls

☑ Call notification with tray icon for notification calls

□ Always on top

☑ Pop up on ringing

☑ Pop up when in a call

□ Minimize after call

☑ Minimize to tray icon

Call

In this section, you can switch the Hide Number and Disable Second Call options for the selected user on or off.

This requires that you have two calls. If the call you have initiated is active, you can connect the two callers to one another by simply placing the handset on hook. Here, you can activate the "Transfer on Hookon" function. If you did not initiate the active call (i.e. you received the call), the connection will be terminated by hook on. The second call will remain on hold.

Example:

Subscriber A is called by C. Then subscriber A begins a second call on another line to subscriber B (e. g. for an Inquiry Call). If A goes on hook, subscribers B and C are then connected to one another.

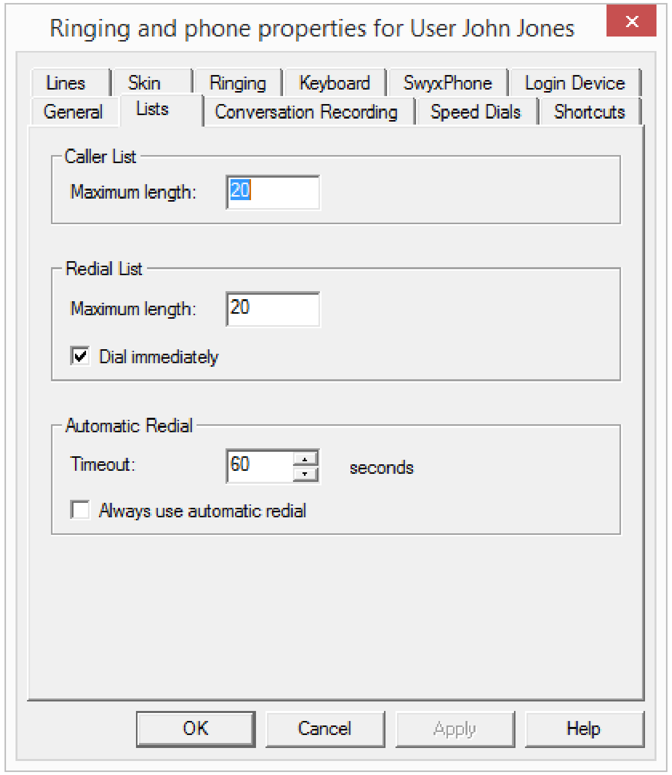
> You must place the handset of the device on hook. If you click on the SwyxIt! Classic interface to end the connection, the two lines will not be connected to one another.

SwyxIt! Classic Window

In the lower section, you can define the settings for the general behavior of SwyxIt! Classic. For example, you can define the behavior of the window during or after a call and application sharing.

See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/#context/help/office_communication_$.

11.2.6.2THE "LISTS" TAB



Caller List
Maximum length: 20

Redial List
Maximum length: 20
☑ Dial immediately

Automatic Redial
Timeout: 60 seconds
□ Always use automatic redial

You will also find this tab in the dialog "Button Configuration for User...".

> When saving and processing personal data, observe the respective applicable legal data protection regulations.

> Personal data cannot be deleted automatically. In order to meet the valid data protection regulations, it may be necessary to delete the entries manually.

Caller List, Redial List

Here you can set the maximum number of entries to be included in both the Caller List and the Redial List. The Call Journal comprises all the entries of the Caller List and of the Redial list. The maximum of list entries is 90 entries each. In the case of the Redial List, you can also indicate whether the selected entry should be dialled immediately.

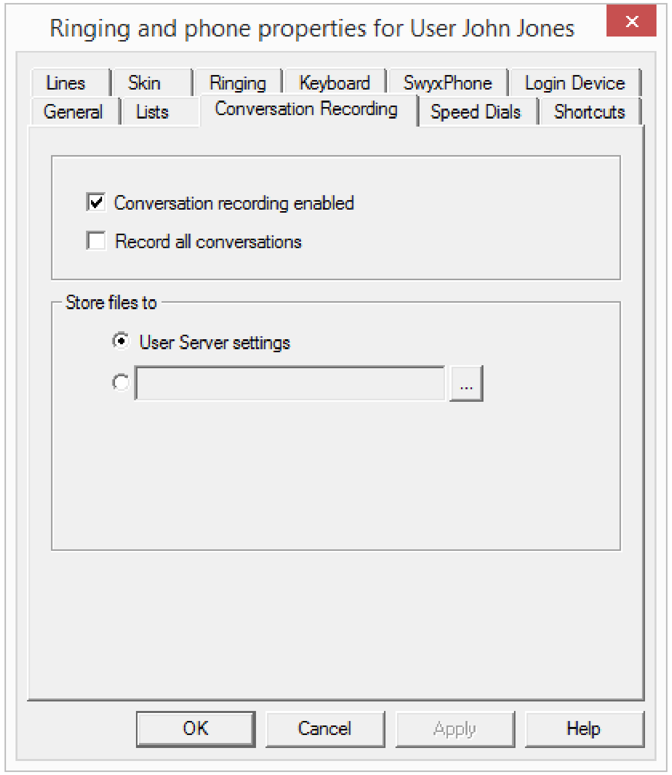
Automatic Redial

You can set the interval (0 to 3600 seconds) between two call attempts for automatic redial.

Furthermore, you can set whether or not Automatic Redial is to be used instantly when redialing is activated on the SwyxIt! Classic user interface.

Please note that the dialing process will be repeated until the selected line is free, rather than until a connection to this line is created.

11.2.6.3THE "CONVERSATION RECORDING" TAB


Ringing and phone properties for User John Jones

☑ Conversation recording enabled

□ Record all conversations

Store files to

● User Server settings

○

Here you can define

- whether the user is allowed to record conversations
- whether all conversations of this user are to be recorded.

Store files to

Here you can set the directory for saving recorded conversations. If you select "User server settings", the files will be saved to the directory set in the default server settings. (*7.5.2 The "Client Preferences" Tab*, Page 88). Alternatively you can also enter a different directory here.

If you select a different directory, please note that the user needs write permission for that directory. In order to listen to the list of recorded conversations the user also needs read access to this directory.

The file name for the recorded conversations is composed as follows:

- <Direction of the call>#
  A differentiation is made between outgoing calls (OUT) and incoming calls (IN).
- <Number of the user>#
  This is the extension called (IN) or the extension from which the call was started (OUT).
- <Name of the conversation partner>#
  The name can only be given if the number has been assigned a name.
- <Number of the conversation partner>#
  Will be displayed if one exists. Please note that the public line access will also be saved.
- <Date of the call>#
  Date in the format <yyyymmdd>
- <Time of the call>
  Start time of the call using the format hhmmss

  Example:

  The name

  Out#123#Schulz, Eva#0012345678#20050217#155844.wav

  means that an outgoing call from the number "123" to Eva Schulz with the number "0012345678" was recorded on February 17, 2005 at 15:58:44.

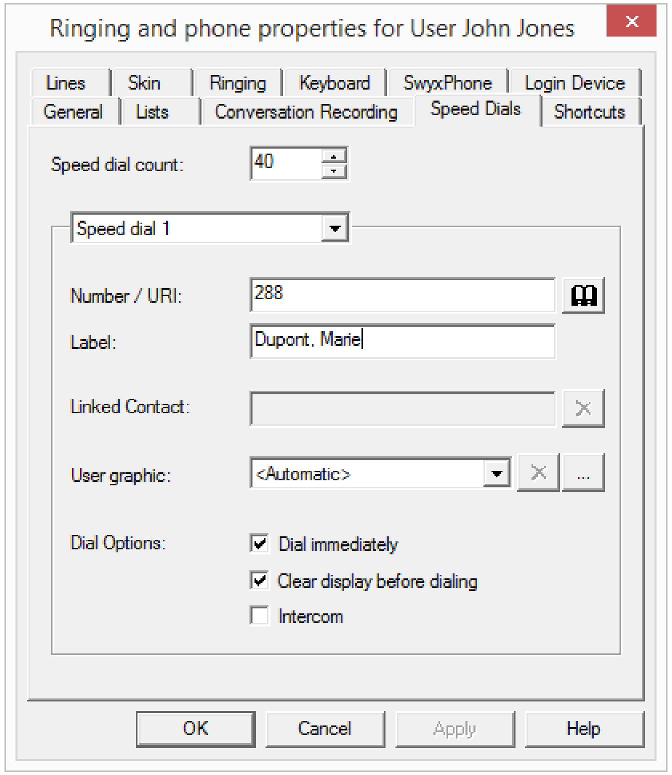
The recorded conversations can be viewed and played by the user in the Recording List. This list only contains the recorded conversations associated with the personal extensions of the corresponding user. If a group call is picked up, the conversation is associated with the same personal number as the one used for outgoing calls from this line.

If a user has the permission to record conversations him/herself, he or she will be able to delete recordings in this list – otherwise only the system administrator can delete recorded conversations.

If the user initiated the recording of the conversation, only the phone call to one conversation partner is recorded. An inquiry call made during a conversation can be recorded by recording it to a separate file.

If the recording of a conversation was specified by the Administrator, several simultaneous conversations will be saved to the same file.

11.2.6.4THE "SPEED DIALS" TAB



Ringing and phone properties for User John Jones

Speed dial count: 40

Speed dial 1

Number / URI: 288

Label: Dupont, Marie

Linked Contact:

User graphic: <Automatic>

Dial Options:

☑ Dial immediately

☑ Clear display before dialing

□ Intercom

You will also find this tab in the dialog "Button Configuration for User...".

The number of Speed Dials can be defined here. Furthermore, you can assign a number, a label and, if you want, a picture to each Speed Dial.

Users may also assign linked contacts to a speed dial button. Contact data from connected applications (e.g. Swyx VisualContacts, Microsoft

Outlook, IBM NotesIBM Notes) are being retrieved, when the user opens the context menu of the speed dial or the contact card.

The link to the connected application can be deactivated via the ✕ button. The speed dial button label and number remain saved on the speed dial button.

In addition you can define

- whether the selection of the Speed Dial results in immediate dialing
- whether the display will be deleted when the Speed Dial is selected and
- whether the Speed Dial can be used for an intercom connection.

> The intercom connection can only be used if the user who is making the call is signaled the status of the user called.

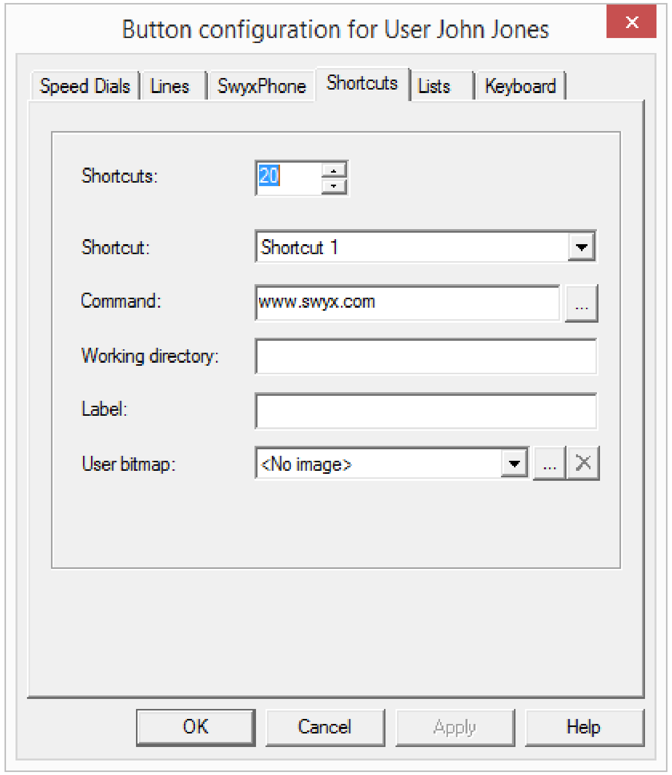
You can also configure a DTMF suffix on a speed dial. To do this, extend the number with an "x" and then add the corresponding DTMF digits. If you want to create a pause during the second dialing, please enter a colon (,) fore each two seconds.

Example:

You would like to dial the number "020 4777555"; when the connection is created, you would like to transmit the numbers "123" per DTMF. You want to dial the digits 898 after ten seconds. Assign the number "020 4777555x123,,,,,898" to the Speed Dial.

See also *Export and import of speed dials and shortcuts.*, Page 189.

11.2.6.5THE "SHORTCUTS" TAB



Button configuration for User John Jones

Shortcuts: 20

Shortcut: Shortcut 1

Command: www.swyx.com

Working directory:

Label:

User bitmap: <No image>

You will also find this tab in the dialog "Button Configuration for User...".

The number of Shortcuts can be defined in this page. You can also assign any command you want and a corresponding working folder to any defined shortcut, much like a Windows default shortcut.

As with all other buttons, you can assign a name and a bitmap to the button. Both will appear on the user interface of the telephony client SwyxIt! Classic.

Export and import of speed dials and shortcuts.

The speed dials and shortcuts of individual users can be exported and/ or imported.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

In the user list of the SwyxWare administration, select the respective menu entry in the context menu of a user:

- "Speed dials / Shortcuts | Import..."
  or
- "Speed dials / Shortcuts | Export..."

The button assignment is saved in a *.key file.

The user pictures and any linked contacts are also saved.

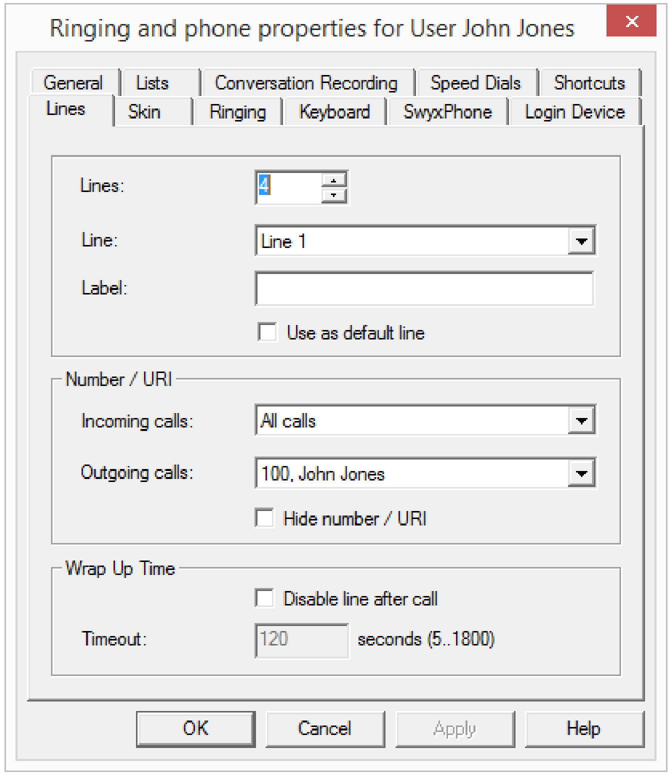
The buttons are assigned according to their label (e.g. "Speed Dial 1" is assigned to "Speed Dial 1" again).

The number of buttons on the Skin is not modified by the import.

Linked contacts are imported, regardless if the respective applications are connected to SwyxIt! Classic or not.

During the import, any speed dial and shortcut buttons are overwritten. I.e. if the *.key file only describes the assignment of one speed dial button, any other buttons will be deleted (reset).

11.2.6.6THE"LINE KEYS" TAB



Lines: 4

Line: Line 1

Label:

□ Use as default line

Number / URI

Incoming calls: All calls

Outgoing calls: 100, John Jones

□ Hide number / URI

Wrap Up Time

□ Disable line after call

Timeout: 120 seconds (5..1800)

You will also find this tab in the dialog "Button Configuration for User...".

The number of Line Buttons can be defined in this page. You can also set a label for each defined line.

The remaining parameters then apply respectively for the selected line. All spontaneously dialled numbers are dialled over the standard line (default line), provided the user does not specify any other line in advance. This setting applies both to SwyxIt! Classic and to SwyxPhone. If no line is specified as standard, then as before the last used line is selected.

Number / URI

In the "Incoming calls" field, you can define which incoming calls are signaled on the line specified above:

- All incoming Calls,
- Only group calls, or
- Calls to all internal numbers of this user, or
- Calls to a specified internal number of this user, in case there are several numbers.

In the "Outgoing calls" field, you can define the internal number used for signaling an external number.

> *Example:*
>
> *A user has the internal number "225" which is mapped to the external number "+44 20 55666225". And, the same user has the additional internal number "325" which is mapped to the external number "+44 778 88325". If you select "225" for outgoing calls, this user signals "+44 20 55666225" for external calls.*

The administrator can enter a number for each line here. This number is then used as the outgoing number. This number does not have to be the number of the user. It can be any free number or the number for the "Support" group, for example. This number is marked with "(Alternative Number)".

Please note that all Alternative numbers which are to be assigned here must have been added for the user beforehand as Alternative numbers. See *11.2.2.2 The "Alternative Numbers" Tab*, Page 178.

The display of your own number for outgoing calls can be suppressed by selecting the option "Hide Number".

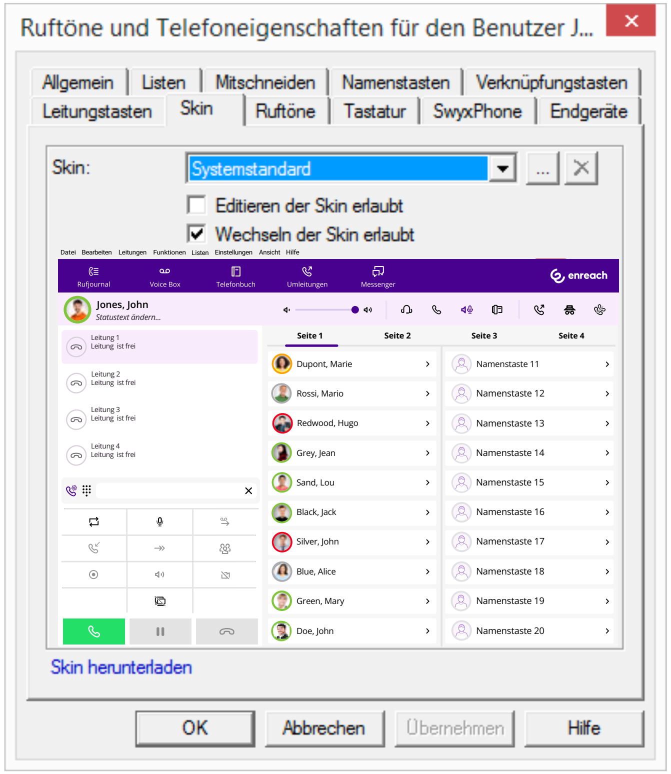
See *11.2.6.1 The "General" Tab*, Page 185.

Wrap Up Time

A wrap up time between 5 and 1800 seconds can be defined for each line here. If the checkbox is activated, the line is blocked for further calls during this time period after every incoming call.

The line is cleared if the user initiates and ends a call during the wrap up time.

11.2.6.7THE "SKIN" TAB


Ruftöne und Telefoneigenschaften für den Benutzer J...

Skin: Systemstandard

☐ Editieren der Skin erlaubt

☑ Wechseln der Skin erlaubt

This tab can be used to define the appearance of SwyxIt! Classic for the selected user. A preview of the skin selected in the drop-down list is displayed.

Furthermore, you can indicate whether the selected user is allowed to modify the appearance of SwyxIt! Classic by editing his/her own skin or by choosing another skin e. g. from the skins provided on the SwyxServer.

The skins that are provided for the user are in the SwyxWare database. Further skins are not installed directly. The administrator can add further skins e. g. from the DVD to the database, and thereby make them available to all users.

See *7.5.10 The "Files" Tab*, Page 97.

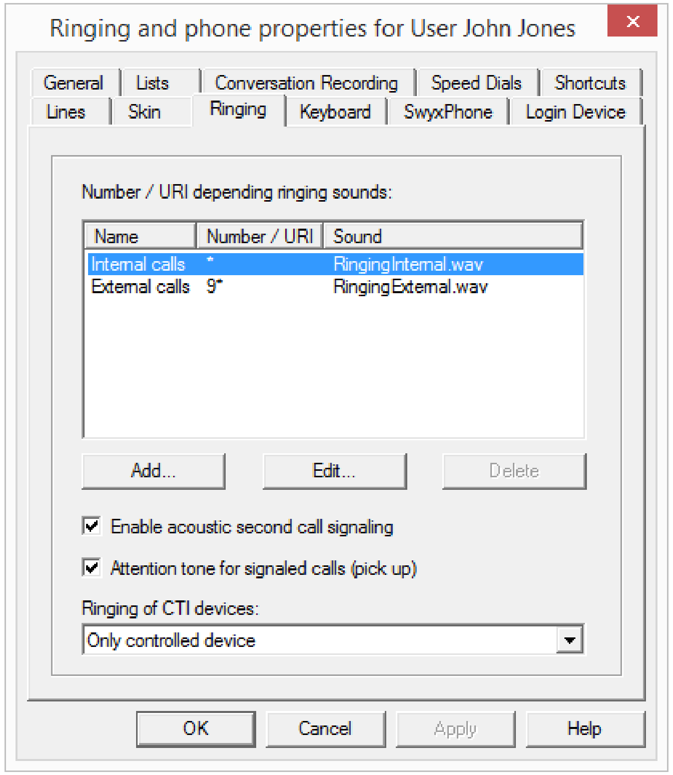
You can find more skins in the download area on the Enreachwebsite.

System-wide default skin

If you choose the system-wide Standard Skin in the drop-down list, then the skin that was specified by the administrator in the server properties will be selected (*7.5.2 The "Client Preferences" Tab*, Page 88).

If the administrator changes the system-wide Standard Skin (in the server properties), this leads to a change of skin for all users who have configured the Standard Skin here.

11.2.6.8THE "RINGING" TAB



Ringing and phone properties for User John Jones

Number / URI depending ringing sounds:

Name	Number / URI	Sound
Internal calls	*	RingingInternal.wav
External calls	9*	RingingExternal.wav

☑ Enable acoustic second call signaling

☑ Attention tone for signaled calls (pick up)

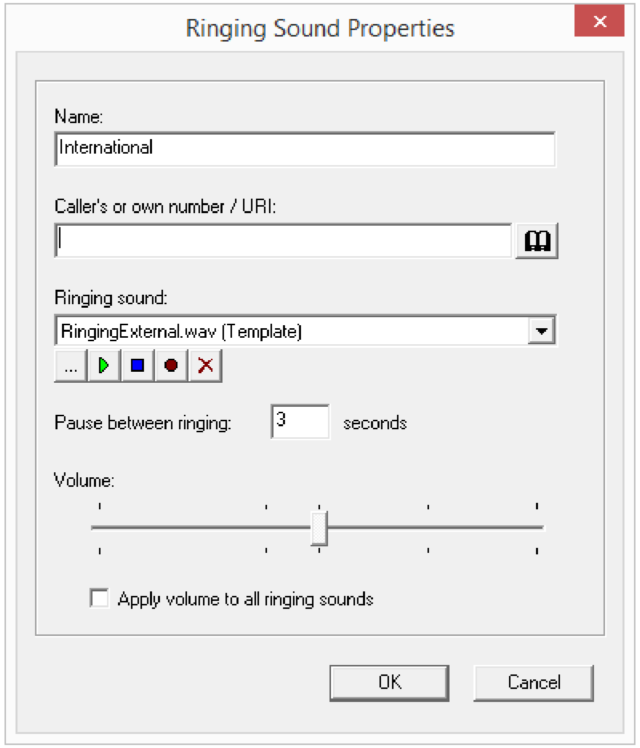
Ringing of CTI devices: Only controlled device

Number Dependent Ringing Sounds

Here you can define ringing sounds which are dependent on the number of the caller or the extension dialled. Wildcards can also be used (* for several numbers, ? for one number).

The administrator can add further ringing sounds to the database, and thereby make them available to all users.

See *7.5.10 The "Files" Tab*, Page 97.



Name: International

Caller's or own number / URI:

Ringing sound: RingingExternal.wav (Template)

Pause between ringing: 3 seconds

Volume:

□ Apply volume to all ringing sounds

You can change the definition for internal and external calls, but not delete them.

Additionally, you can specify here whether a call signaling defined by a relationship is also to be signaled acoustically.

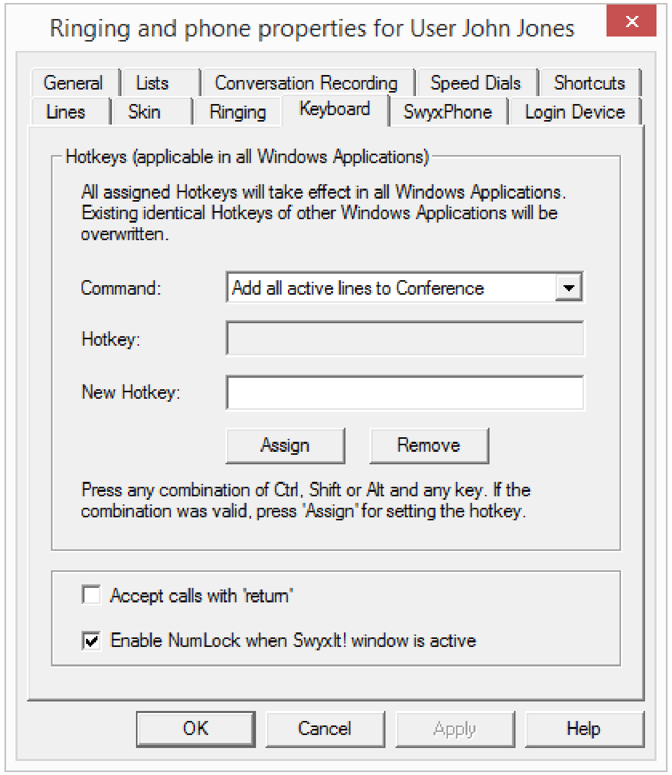
See *11.2.8 The "Properties..." Dialog: The "Relationships" Tab*, Page 202.

Activate the "Enable acoustic second call signaling" in order to hear the call-waiting tone in the headset when a second call is received.

In the drop-down list "Ringing of CTI devices" you can indicate which terminal devices should ring if SwyxIt! Classic is operating in CTI mode:

- Both devices, i. e. SwyxIt! Classic in CTI mode and the controlled device (SwyxIt! Classic or SwyxPhone)
- only CTI SwyxIt! Classic
- only the controlled device (SwyxIt! Classic or SwyxPhone)

11.2.6.9THE "KEYBOARD" TAB



All assigned Hotkeys will take effect in all Windows Applications. Existing identical Hotkeys of other Windows Applications will be overwritten.

Command: Add all active lines to Conference

Hotkey:

New Hotkey:

Press any combination of Ctrl, Shift or Alt and any key. If the combination was valid, press 'Assign' for setting the hotkey.

□ Accept calls with 'return'

☑ Enable NumLock when SwyxIt! window is active

You will also find this tab in the dialog "Button Configuration for User...".

Hotkeys

In this section of the tab you can define, edit and remove hotkeys for specific SwyxIt! Classic actions. To select a hotkey, go to the corresponding line and press the key to which you wish to assign the function specified above.

Here you can also disable the function of using the F11 key to dial from any application by removing the hotkey.

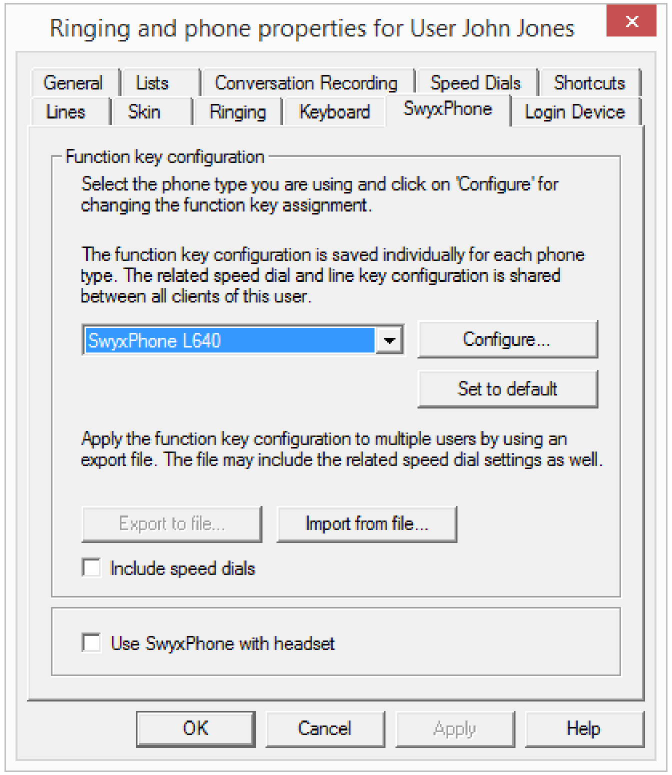
SwyxIt! Classic Hotkeys

If you activate the upper checkbox here, an incoming call can be picked up using the Return key.

If you activate the second checkbox, the NUM key of the keyboard is automatically switched on as soon as the SwyxIt! Classic window is activated. The number can then be entered directly via the numeric keypad on the keyboard. Following standard installation of SwyxIt! Classic, the NUM key is activated when the SwyxIt! Classic window is active.

The hotkeys you define here are then valid in all applications. Furthermore, no check will be carried out to determine whether the selected hotkey is already occupied on the user's system.

11.2.6.10TAB "SWYXPHONE"


Ringing and phone properties for User John Jones

Function key configuration

Select the phone type you are using and click on 'Configure' for changing the function key assignment.

The function key configuration is saved individually for each phone type. The related speed dial and line key configuration is shared between all clients of this user.

SwyxPhone L640

Apply the function key configuration to multiple users by using an export file. The file may include the related speed dial settings as well.

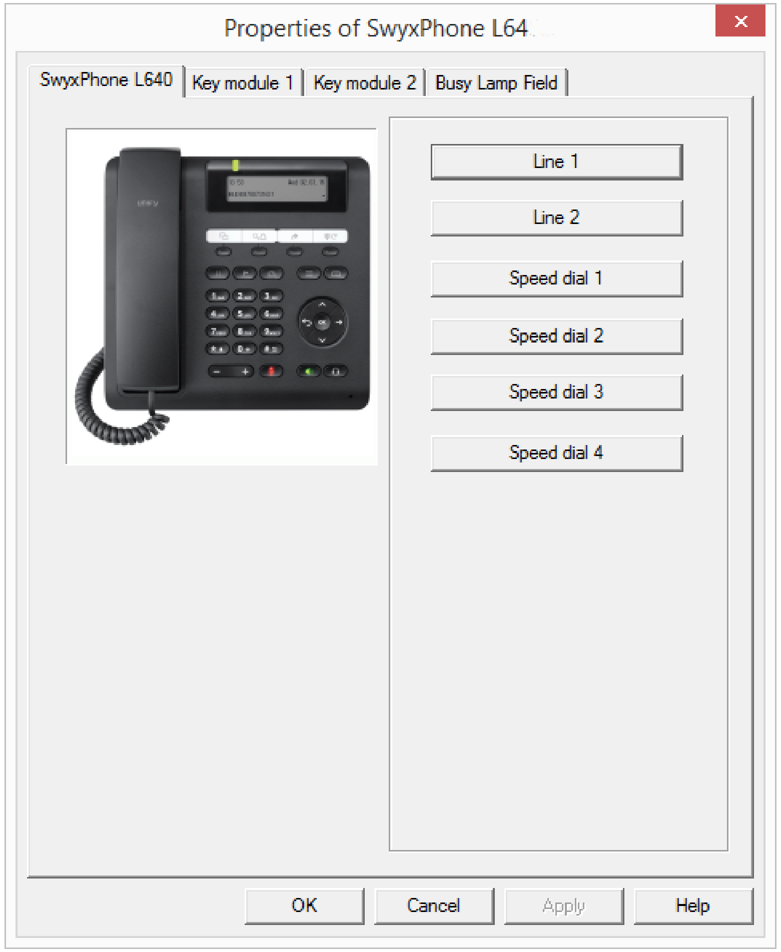
□ Include speed dials

□ Use SwyxPhone with headset

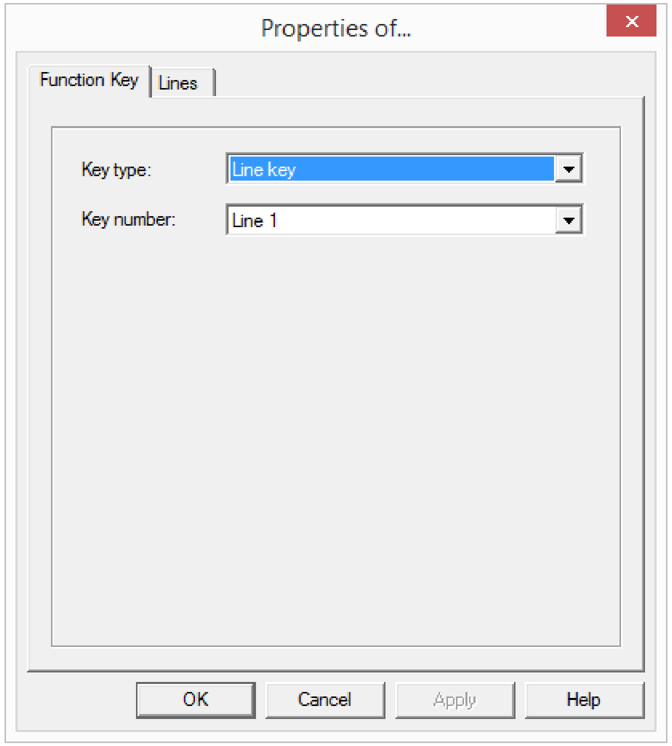
You will also find this tab in the dialog "Button Configuration for User...".

Function Key Configuration

Here you can assign the buttons of the telephone (only - SwyxPhone L 620 does not have keys to assign) and import or export this assignment. Select the type of telephone you would like to configure from the drop-down list and then click on "Configure...". A new dialog with the properties of the selected telephone will open.


Properties of SwyxPhone L64

You will see a picture of the selected phone and the buttons, which are assigned to the keys on this phone. Click on a button to configure the corresponding key. The Properties page of the key will open.



Properties of...

Key type: Line key

Key number: Line 1

Depending on the selected function of the key, there is another tab provided for defining the properties of this key in more detail.

Use this method to configure all keys of the selected phone.

If the user uses different telephone types, you can configure all keys for these telephone types here. Depending on the selected telephone type, the user is also provided with additional key modules for configuration.

Please note that the Speed Dials and the Line Buttons are indexed, i. e. that the Speed Dial 1 is the same for all telephones, for example.

The configuration of the telephone keys can be exported into or imported from a file (*.key) here. Use the checkbox to indicate whether the Speed Dials should be taken into consideration during the export or import.

On the SwyxWare DVD you'll find label templates in Word and PDF formats, which you can inscribe with personal data.

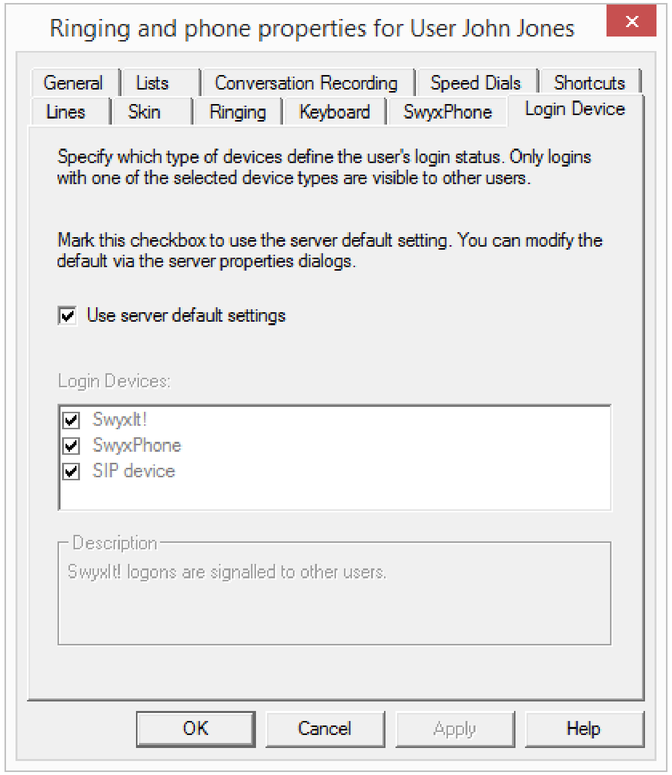
SwyxPhone use with a Headset

This option is only relevant if the user uses a SwyxPhone to which he can connect a headset.

If the handset is down, the hands-free functionality is enabled in case of an incoming call. In this case, the connected headset will not be activated until the Headset button on the phone is activated.

If this option is activated, you will hear the call via the headset connection. The handsfree phone is then activated by pressing the Speaker button on the phone.

11.2.6.11 THE "LOGIN DEVICE" TAB



Ringing and phone properties for User John Jones

Specify which type of devices define the user's login status. Only logins with one of the selected device types are visible to other users.

Mark this checkbox to use the server default setting. You can modify the default via the server properties dialogs.

☑ Use server default settings

Login Devices:

☑ SwyxIt!
☑ SwyxPhone
☑ SIP device

Description

SwyxIt! logons are signalled to other users.

Terminal types

Whether the users signal their status (logged in, speaking, is called) among each other or not, is defined in the relationships of the users or groups. Here you specify, which type of terminal signals the Log-on status of the user, if several terminal types are logged on to the same user account.

Define here which individual setting will be used for the user or apply the standard server settings by activating the checkbox.

Example:

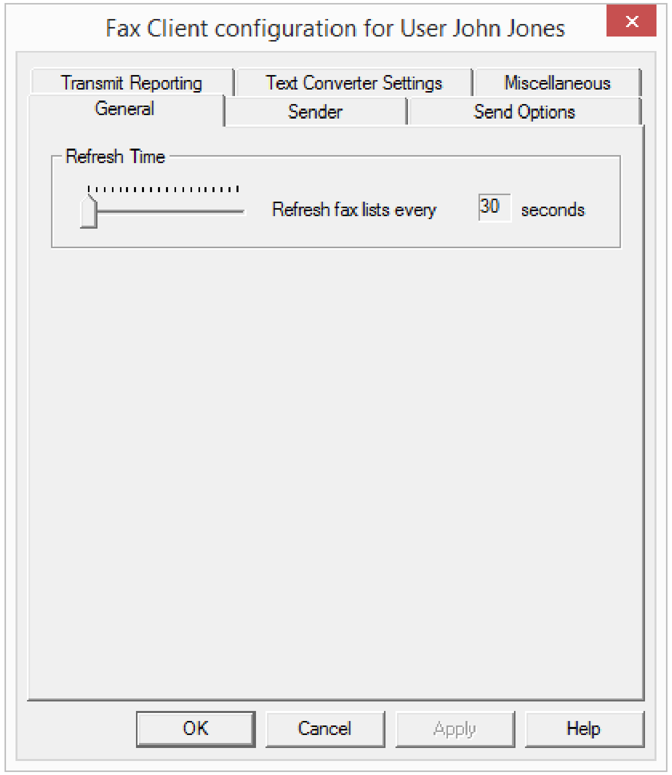
For example, if a user has a SwyxPhone on his desk and a SwyxIt! Classic installed on his computer, he can check his status by SwyxIt! Classic signal. He is then logged in when his computer is switched on and SwyxIt! Classic has started. Is SwyxIt! Classic not started, he can still use his SwyxPhone. However, the status "logged off" is signalled to internal employees and call routing. If the user speaks with SwyxPhone the status "Speaking" is signalled to the employees, for call routing his status remains "logged off".

No more than a total of four terminals of any type (SwyxIt! Classic, SIP phone) can be simultaneously logged on to one SwyxWare user account.

11.2.7 DIALOG "FAX CLIENT CONFIGURATION:"

The settings entered here are valid for the user's fax transmissions. However, the user can still change them individually for the current fax before sending it.

11.2.7.1THE "GENERAL" TAB



Fax Client configuration for User John Jones

Refresh Time

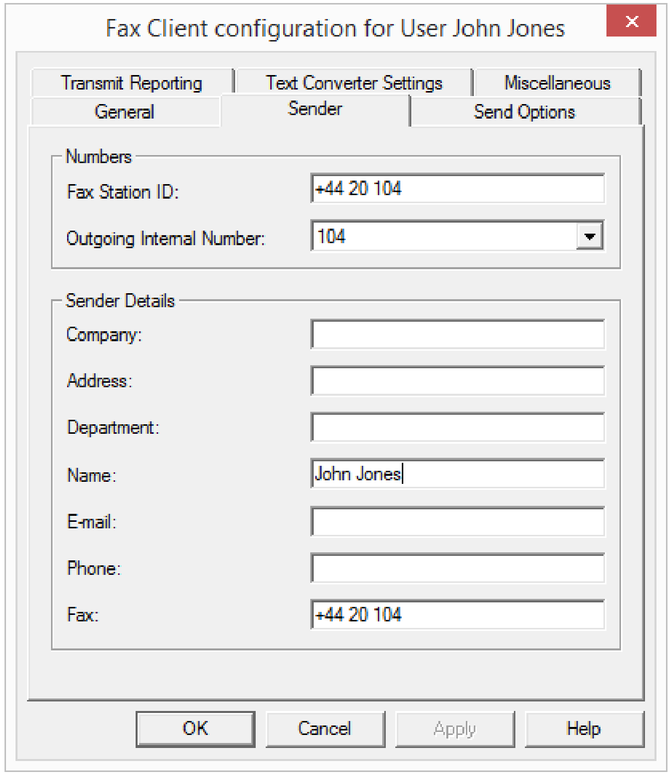
Refresh fax lists every 30 seconds

Only the refresh time for the SwyxFax Client can be changed here.

Refresh Time

"Refresh Time" is used to define the intervals at which SwyxFax Client matches its fax folder display with the server data. A range of 30 to 600 seconds is available to you here.

11.2.7.2THE "SENDER" TAB



Fax Client configuration for User John Jones

Numbers

Fax Station ID: +44 20 104

Outgoing Internal Number: 104

Sender Details

Company:

Address:

Department:

Name: John Jones

E-mail:

Phone:

Fax: +44 20 104

The user's sender information is stored on the "Sender" tab.

Numbers

In the "Numbers" field, you can enter the ID of the fax station and the internal number. The Fax Station ID is the number that SwyxFax should transmit to the remote fax machine when a fax is received.

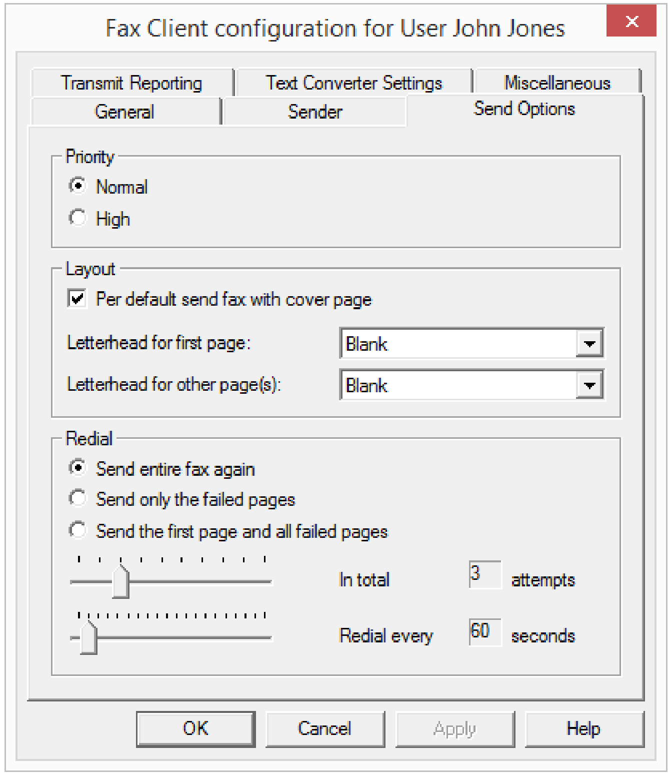
Sender Details

In the field "Sender Information" enter company, address, department, name, e-mail, telephone and fax numbers.

After a fax is sent, the send report documents are sent to the e-mail address stored here. See *11.2.7.4 The "Transmit Reporting" Tab*, Page 199.

All information entered here will be saved as the default setting, i.e. it will automatically be used as "Sender" in the window "Send Fax". If you change the sender in the "Send Fax" window and save it there as the default setting, the information will be changed accordingly on this tab. See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/#context/help/office_communication_$.

11.2.7.3THE "SEND OPTIONS" TAB



Fax Client configuration for User John Jones

Priority

● Normal

○ High

Layout

☑ Per default send fax with cover page

Letterhead for first page: Blank

Letterhead for other page(s): Blank

Redial

● Send entire fax again

○ Send only the failed pages

○ Send the first page and all failed pages

In total 3 attempts

Redial every 60 seconds

Here you can change the basic settings for fax transmission, such as Priority or the general use of a cover page or the settings for redial.

Priority

Fax documents can be prioritized. A fax document with "high" priority will be sent before every fax job with "normal" priority. This will also be the case for the fax jobs of other users that also have "normal" priority.

Layout

Activate the checkbox "Per default send fax with cover page" if you would like to send every fax with a cover page.

In the field "Layout", you can also choose which letterheads should be used for a fax to be sent to an external recipient. You can select a letterhead for the first page which is different from the letterhead used for the rest of the pages. The system administrator will make the letterheads available to all users in the database.

See *24.5.2 Tab "Cover Page"*, Page 363.

All of the settings made and applied here will automatically be applied in the Send Fax dialog (window "Send Fax") each time a fax is sent. In an individual dispatch, these settings can be modified individually for the current fax.

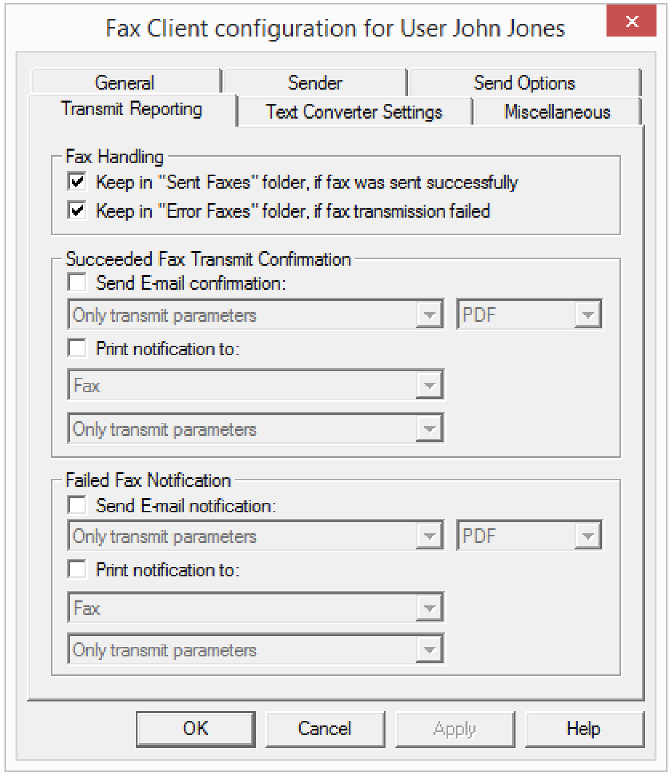
Redial

In the "Redial" field, you can define how often a transmission attempt should be repeated (1 to 10 times) after it has failed the first time. In addition, you can also define the interval at which these attempts should be made (30 to 600 seconds). In doing so you can define which pages of the fax should be sent in the renewed transmission attempt.

Select from:

- Send entire fax again,
- Send only the failed pages or
- Send first page and all failed pages

11.2.7.4THE "TRANSMIT REPORTING" TAB



Fax Handling

☑ Keep in "Sent Faxes" folder, if fax was sent successfully

☑ Keep in "Error Faxes" folder, if fax transmission failed

Succeeded Fax Transmit Confirmation

☐ Send E-mail confirmation:

Only transmit parameters | PDF

☐ Print notification to:

Fax

Only transmit parameters

Failed Fax Notification

☐ Send E-mail notification:

Only transmit parameters | PDF

☐ Print notification to:

Fax

Only transmit parameters

On the "Transmit Reporting" tab you can define the setting for the fax Send Report. If a fax is sent, the server returns a message about the success of the transmission. This may be a transmit confirmation (if the fax was transmitted successfully) or a notification (if errors occurred during fax transmission). You can define the form in which the Send Report is sent, namely per e-mail and/or in print form.

Fax Handling

In the field "Fax Handling" you can define whether successful or faulty fax transmissions should be saved in the folder "Sent Faxes" or "Error Faxes". This ensures that later access to sent faxes, sorted by transmission success, is possible.

Succeeded Fax Transmit Confirmation

Specify whether a transmit confirmation should be sent by e-mail after a successful fax transmission, and/or whether a confirmation should be printed.

Transmit Confirmation via E-mail

Activate the checkbox "Send E-mail confirmation:". Define the content of the e-mail. Decide whether just the transmission parameters, the transmission parameters and the first page of the fax or the transmission parameters and the entire fax should be sent.

Transmission parameters include:

- Sender ID
- Recipient ID
- Recipient’s name
- Send Time
- Number of Pages
- Attempts
- Duration of Transmission
- Fax Station ID
- Resolution
- Speed
- Transmission Status

If you select "Transmission parameters and the first page" or "Transmission parameters and the complete fax document", the first page or the complete fax document is attached to the e-mail as a file. You can define the format. Formats include:

- TIFF
- PDF
- TIFF and PDF (2 attachments)

The transmit confirmation will be sent to the e-mail address that you have stored in the "Sender" tab.

See *11.2.7.2 The "Sender" Tab*, Page 197.

Fax Transmit Confirmation per Print

Activate the checkbox "Print confirmation to:" and select the printer. Define the content of the printout. Decide whether just the transmission parameters, the transmission parameters and the first page of the fax or the transmission parameters and the entire fax should be printed. Confirm your selection with "OK".

A transmit confirmation can be sent by e-mail or printed.

> The parameters saved here are the default setting. These parameters will appear in the "Send Fax" window. In this window, you can adapt the parameters individually for the current fax.

Failed Fax Notification

In the field "Failed Fax Notification" you can define whether a notification of a failed fax should be sent by e-mail and/or whether it should be printed.

Notification by e-mail

Activate the checkbox "Send E-mail notification:". Define the content of the e-mail. Decide whether you would like to receive just the transmission parameters, the transmission parameters and the first page of the fax or the transmission parameters and the entire fax.

Transmission parameters include:

- Sender ID
- Recipient ID
- Recipient’s name
- Send Time
- Number of Pages
- Attempts
- Duration of Transmission
- Fax Station ID
- Resolution
- Speed
- Transmission Status

If you select "Transmission parameters and the first page" or "Transmission parameters and the complete fax document", the first page or the complete fax document is attached to the e-mail as a file. You can define the format. Formats include:

- TIFF
- PDF
- TIFF and PDF (2 attachments)

The transmit confirmation will be sent to the e-mail address that you have stored in the "Sender" tab.

See *11.2.7.2 The "Sender" Tab*, Page 197.

Notification by printout

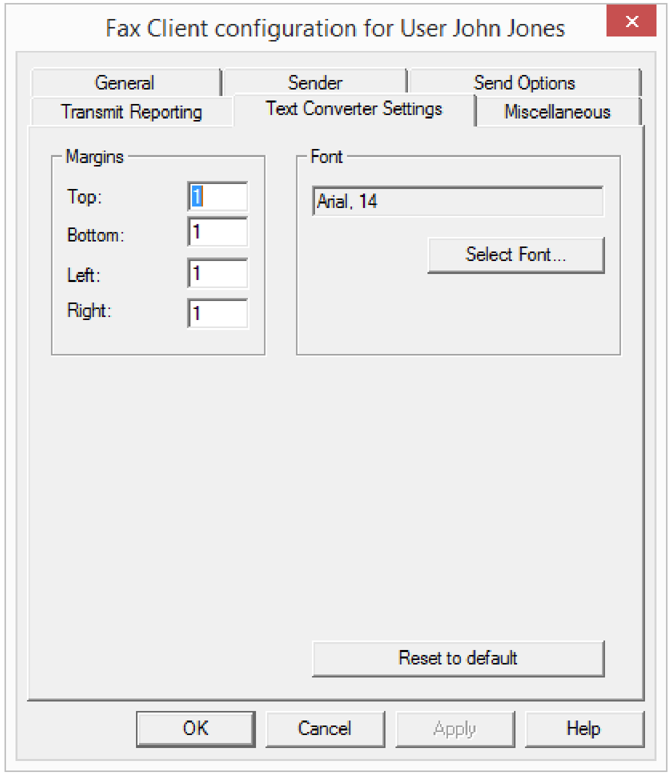
Activate the checkbox "Print confirmation to:" and select the printer. Define the content of the printout. Decide whether just the transmission parameters, the transmission parameters and the first page of the fax or the transmission parameters and the entire fax should be included. Confirm your selection with "OK".

A notification can be sent by e-mail or printed.

> Please note that the printer selected here must be a local printer which is recognized by the SwyxFax Server.

> The parameters saved here are the default setting. These parameters will appear in the "Send Fax" window. In this window, you can adapt the parameters to meet your requirements for the current fax.

11.2.7.5THE "TEXT CONVERTER" TAB



Margins
Top: 1
Bottom: 1
Left: 1
Right: 1

Font
Arial, 14

If text files are to be attached to a fax transmission, these must be converted to a suitable format (SFF) before transmission.

It is necessary to specify the layout for this. Define here the required margins and font / font size.

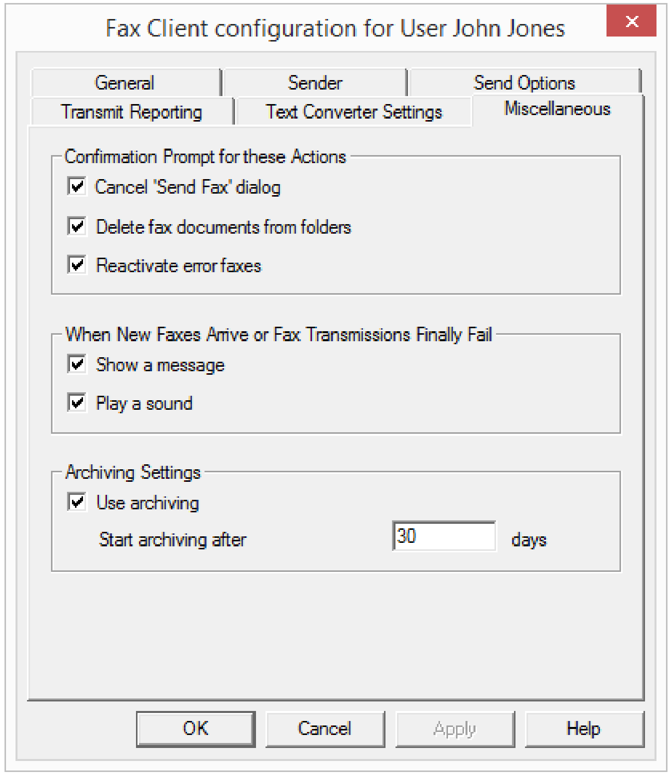
Margins

Specify here the margin widths to be applied when text is converted into a faxable format.

Font

Specify here the font and font size to which the text of an attached text file should be converted.

11.2.7.6THE "MISCELLANEOUS" TAB



Confirmation Prompt for these Actions
☑ Cancel 'Send Fax' dialog
☑ Delete fax documents from folders
☑ Reactivate error faxes

When New Faxes Arrive or Fax Transmissions Finally Fail
☑ Show a message
☑ Play a sound

Archiving Settings
☑ Use archiving
Start archiving after 30 days

The "Miscellaneous" tab is used to define additional settings for SwyxFax Client, such as security queries or notifications.

Confirmations Prompt for these Actions

Under "Confirmation Prompt for these actions", you can activate the corresponding checkboxes to indicate which actions (Cancel, Delete, or Reactivate a fax transmission) must be confirmed to be on the safe side. If confirmation is activated, a window will appear together with the corresponding action, asking for confirmation of the action. This helps to avoid accidental deletion, cancellation or reactivation.

When New Faxes Arrive or Fax Transmissions Finally Fail

Specify under "Actions when new faxes arrive, or on faulty fax transmission" whether a new fax should be signaled directly with a window and a notification tone. It is similarly reported when transmission of a document has failed. Activate the appropriate option.

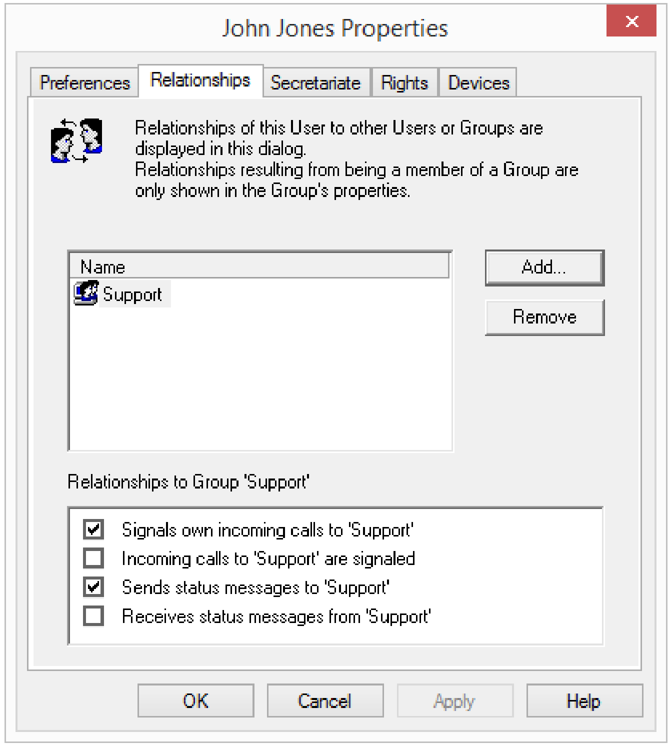
Archiving Settings

If you have faxes saved in the fax folders and these faxes are older than the number of days specified here, a window will appear when you start SwyxFax Client asking you to archive these documents. If you do not activate this option, the documents will not be archived.

Activate the archiving function here, and set the interval after which the documents should be archived (default: 30 days).

If old fax documents are present which should be archived, a prompt appears asking for a directory in which the archived documents are to be stored. The archived documents are deleted in the database.

11.2.8 THE "PROPERTIES..." DIALOG: THE "RELATIONSHIPS" TAB



Relationships of this User to other Users or Groups are displayed in this dialog.
Relationships resulting from being a member of a Group are only shown in the Group's properties.

Name
Support

Relationships to Group 'Support'

☑ Signals own incoming calls to 'Support'
☐ Incoming calls to 'Support' are signaled
☑ Sends status messages to 'Support'
☐ Receives status messages from 'Support'

Here you can display the user groups the user is associated with and the call or status signaling defined for these group relationships. Relationships will be explained in detail in the following chapter on the subject of "Groups".

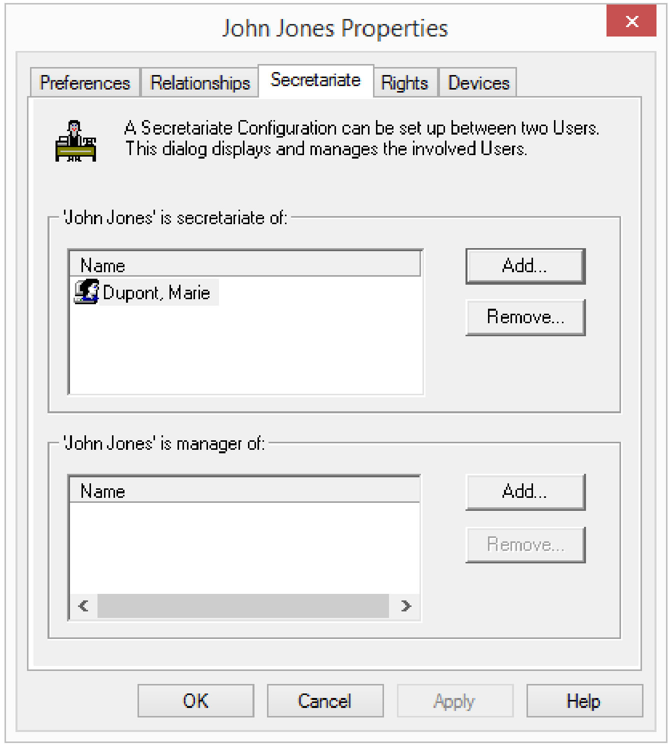
If you have used a SwyxLink trunk to configure cross-server connections to another SwyxServer (*How to configure a SwyxLink trunk*, Page 296), then you likewise specify here the recipient on the linked site to whom the selected user signals the status. This can be an individual user or a group.

See *12.2.4 The "Properties..." Dialog The "Relationships" Tab*, Page 219.

A user can only call another user per intercom connection or use the SwyxIt! Messenger if he or she is signaled the status of the other user.

In the current version the Intercom function cannot be used between different servers.

11.2.9 THE "PROPERTIES..." DIALOG: THE "SECRETARIAT" TAB



A Secretariate Configuration can be set up between two Users. This dialog displays and manages the involved Users.

'John Jones' is secretariate of:

Name
Dupont, Marie

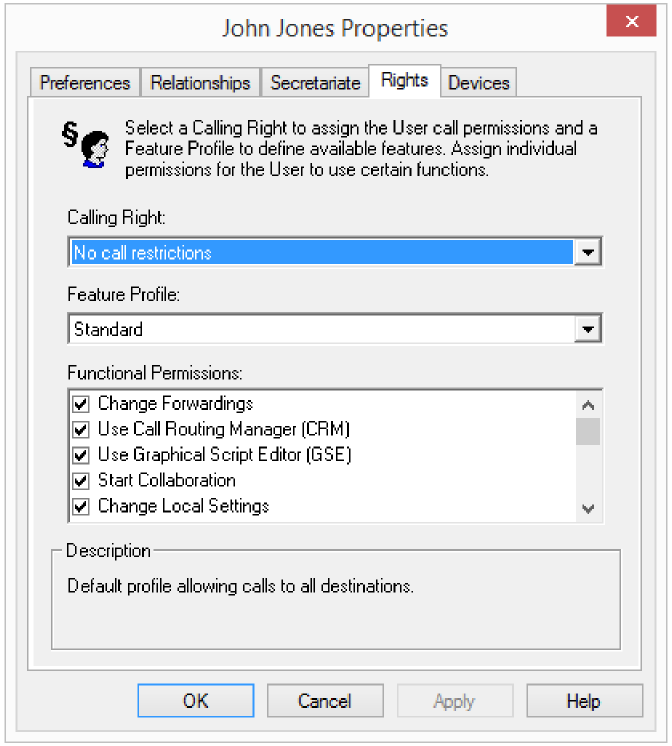
'John Jones' is manager of:

Name

Here you can see which secretariate relationships are defined for this user. You will find information on the secretariate configuration in the chapter titled "Secretariate".

See *12.3 Secretariate*, Page 224.

11.2.10THE "PROPERTIES..." DIALOG: THE "RIGHTS" TAB



Select a Calling Right to assign the User call permissions and a Feature Profile to define available features. Assign individual permissions for the User to use certain functions.

Calling Right: No call restrictions

Feature Profile: Standard

Functional Permissions:

- ☑ Change Forwardings
- ☑ Use Call Routing Manager (CRM)
- ☑ Use Graphical Script Editor (GSE)
- ☑ Start Collaboration
- ☑ Change Local Settings

Description

Default profile allowing calls to all destinations.

Different rights can be assigned to a SwyxWare user. On the one hand, it is possible to limit outgoing calls, and on the other hand the use of particular functionalities can be denied.

Call Permission

There are different levels for call restriction, which the administrator can variably organize, e. g.

e. g.

internal calls

only calls within the SwyxWare

- local calls
  only calls without prefix
- long distance calls
  calls within the country; without international prefix
- international calls
  all calls with international prefix

A user's Calling Right is defined by the assigned Call Permissions profile. You can define various call restrictions e.g. only internal calls, local calls or national calls. In addition, the administrator can also block specific numbers or prefixes (e.g. chargeable prefix numbers).

See *9.1 Call Permissions*, Page 128.

Available Functions

There are various SwyxIt! Classic functions which the administrator can allow or disable for users. These functions can be assigned via function authorizations or a specific administrator profile.

Feature Profile

The feature profile defines the selection of features which are available in principle for the user. It is possible here to grant the user rights to use advanced SwyxWare functionalities.

To change the feature profile, choose a different profile from the drop-down list. In the standard installation of SwyxWare, only the "Standard" profile is available; this provides all features for the user. Different profiles are offered in SwyxWare for DataCenter and SwyxON. See *9.2 Function profile*, Page 137.

If a different feature profile is assigned to a user, this change appears in the change log.
See *7.7 Change log*, Page 117.

Available Functions

In the field "Functional Permissions:", the administrator can define which functions are available to the user by activating corresponding checkboxes. The individual highlighted function is explained in the "Description" field.

If individual functions are not included in the feature profile, they cannot be activated in the lower field either. In this case, please choose a different feature profile.

- Change forwardings
  A user is allowed to modify the call forwardings (Unconditional, No reply, Busy), i. e. the user can either set a number, to which the call is to be forwarded or determine that all calls will be forwarded directly to the Voice Box.
  If the "Forwardings" option is deactivated, the user cannot change any of the forwarding options (immediate, delayed, if busy). The Call Routing Manager and Graphical Script Editor are then also deactivated.
- Use Call Routing Manager (CRM)
  With the help of the Rule assistants, the user himself can create a set of rules for call handling here. See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/import_export_phonebook_$.
  If a user does not have permission to start the Call Routing Manager directly, then the scripts created with the Call Routing Manager will still be available to the user. He can still change his forwardings (Unconditional, No Reply, Busy). Graphical Script Editor is likewise deactivated.
  This functionality is included for SwyxWare for DataCenter and SwyxON in the option SwyxBCR. In SwyxWare this functionality is already included in the basic version.

- Use Graphical Script Editor (GSE)

  In addition to the Rule assistants of the Call Routing Manager, a graphical representation of the rules is offered here. Graphical Script Editor is part of the option SwyxECR package.

  If scripts that the administrator has use of the Graphical Script Editor. created for a user are to be applied, the function profile must allow the use of use of the Graphical Script Editor.. In order to prevent the user from changing script, the administrator needs to deactivate the "Graphical Script Editor" check box in the user configuration.

  See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/import_export_phonebook_$.

- Start Collaboration

  The Collaboration function allows the user to share his or her desktop during a telephone conversation via SwyxIt! Classic. The share takes place on the SwyxIt! Classic user interface, in the menu "Functions | Collaboration". When the desktop is shared, the user can allow the conversation partner to access his or her computer.

  See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/collaboration_$.

The Collaboration function can only be executed between SwyxIt! Classic users. Collaboration with a SwyxPhone is not possible. Both subscribers must have SwyxIt! Meeting or TeamViewer installed on their computers and must have the right to share applications. A user can only permit one application share at a time.
The collaboration function with TeamViewer only works when the SwyxIt! Classic users are logged in to the same SwyxServer.

- Change Local Settings

  In the local configuration, users can define on which server and under which user name they log on, which email client the "Voice Box" button opens, and which voice compression is used.

  The local settings for the voice terminals are made on another tab.

  The local configuration cannot be performed in the SwyxWare Administration. For this reason it is possible to change the local configuration directly on the user's computer when SwyxIt! Classic is logged off. The altered local settings become effective as soon as SwyxIt! Classic logs in again.

  See also https://help.enreach.com/cpe/latest.version/Client/Swyx/de-DE/index.html#context/help/local_settings_$.

- Change User Profile

  Here, you can define all the settings which directly concern the user and those which the user finds on all telephony clients when he logs in to SwyxServer. These include, e.g. Speed Dials, shortcuts, ringing sounds, etc. These settings can also be made in the SwyxWare Administration under user settings.

- Video calls

  You specify here whether the user may receive and make video calls.

- Send/receive instant messages

  You specify here whether the user may send and receive instant messages with the help of SwyxIt! Messenger.

- Change own user picture

  If this option is activated, the user is allowed to exchange his/her own user picture.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

- Upload own user picture

  If this option is activated, the user is allowed to upload his/her own individually chosen user picture. This option can only be activated when the option "Change own user picture" is activated.

- Load Skin

  The user is allowed to select a different skin.

  If this option is activated, the user can change his skin, i.e. he can select another skin for the existing skins. This option is also activated when "Edit the Skin" is activated.

- Edit Skin

  The user is allowed to use and edit own skins with the Skin Editor.

  See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/skins_$.

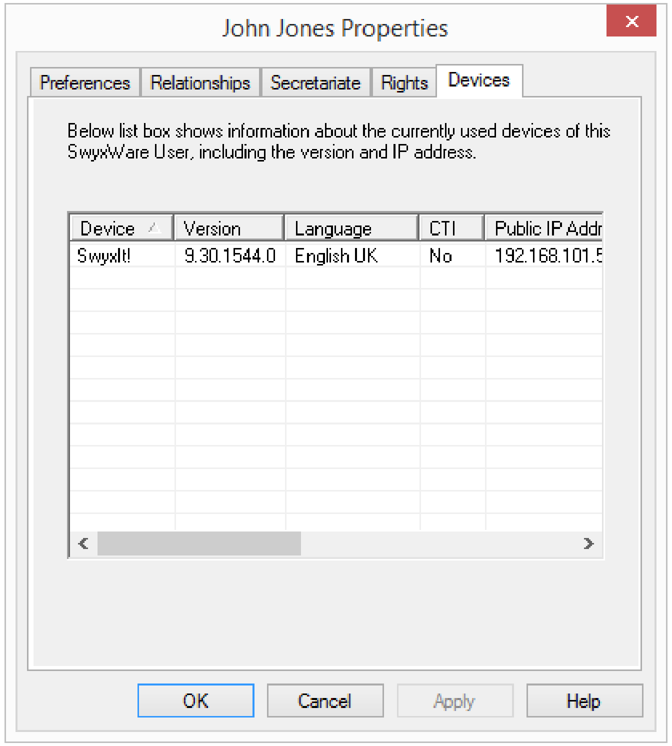
- Record Conversation in SwyxIt! Classic
  The user can record calls that he makes with SwyxIt! Classic.
  This functionality is included in the option pack SwyxRecord.
- Change number and numbers of the lines
  If this option is activated, the user can determine the number of available lines and assign certain incoming calls to the desired lines.
- Change settings for the encryption
  If this option is activated, the user can change the settings for the encryption. See *11.2.1.9 The "Encryption" Tab*, Page 174.
- CTI+ with external phone via phone number
  With SwyxCTI+, the user can control an external telephone via its phone number See *25.2.1 Configure a CTI pairing to the number of an external phone*, Page 383.

Functions on a SwyxPhone

If the user uses a SwyxPhone as a terminal, then only the authorizations for "User Profile" and "Forwardings" take effect.

- User Profile
  This affects the following functions:
  Disable Secondary Call,
  Incognito,
  Adjust Ringing,
  Call Signaling,
  Setting the function keys, speed dials and line keys
  The setting options for voice and ringing volume remain the same.
- Call Forwardings
  The user can no longer change his or her settings for the forwarding options (unconditional, if busy and no reply) or for Do not Disturb (the settings for unconditional forwarding are applied).

11.2.11 THE "PROPERTIES..." DIALOG: THE "LOGIN DEVICE" TAB


John Jones Properties

Below list box shows information about the currently used devices of this SwyxWare User, including the version and IP address.

Device	Version	Language	CTI	Public IP Addr
SwyxIt!	9.30.1544.0	English UK	No	192.168.101.5

On this page you can see which devices (telephone or computer client) are currently logged on under this SwyxWare user.

No more than a total of four terminals of any type (SwyxIt! Classic, SIP phone) can be simultaneously logged on to one SwyxWare user account.

Details for the logged on devices can be seen in the list:

Label	Explanation
Device Type	SwyxIt! Classic or telephone type
Version	Version of the software for the device

Label	Explanation
Language	for SwyxIt! Classic only: Language of the installed SwyxIt! Classic
CTI	indicates whether the device is controlled via CTI
IP-adress	IP address of the device
MAC	MAC address of the device
Operating system	for SwyxIt! Classic only: Operating system on which the SwyxIt! Classic is installed

11.3 PERSONAL PHONEBOOK FOR A USER

Personal Phonebook of a User can also be edited in the SwyxWare Administration. The administrator can, for example, export an employee's personal phone book and import the data into the phone book of his (new) colleague.

Here, the entries can be marked with a check as "personal entries", i.e. other users will be signaled the number but not the name.

See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/phonebook_$.

The administrator must have the rights of a system administrator to be able to edit another user's personal phone book.

You can:

- Open the phonebook and edit single entries.
- Import other phonebooks.
- Export the user's personal phonebook.

To edit the Personal Phonebook of a User

1. Select the user in the administration.
2. From the shortcut menu (right mouse button), select if you want to
   - open the phonebook
   - import a phonebook
   - export this phonebook

When you import or export phonebooks, a wizard will guide you through the process.

See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/import_export_phonebook_$.

The user can change the Personal Phonebook himself with his telephony client (SwyxPhone or SwyxIt! Classic). Alternatively, users of SwyxIt! Classic or SwyxPhone Lxxx can edit their Personal Phonebook with the help of the SwyxWare. This does not apply to the phonebooks of the SwyxPhoneDxxx.

11.4 ACTIVATE/DEACTIVATE OR DELETE USERS

It is possible to deactivate a user account, for example if an employee is temporarily absent. The deactivated user can then no longer log in to SwyxServer. However, the user’s call routing (Call Forwarding, etc.) will continue to function and all his or her settings will remain intact.

In a SwyxWare for DataCenter installation a deactivated user will also be counted for thr license report (Configured User). Select the feature profile 'Deactivated' for the deactivated user. Users with this profile are not included in the license data reporting.

At SwyxON, the number of users ordered is always recorded in the usage report, even if these users are assigned the function profile "Deactivated".

If the rule " lock user after failed login attempts" is activated in SwyxServer configuration, then users can be automatically deactivated by the system and any potentially terminal devices and clients logged on may be logged off. See 7Password settings, Page 110.

How to deactivate a user

1. Select the corresponding entry from the user table.
2. Select "activate (deactivate) user" in the context menu.
3. Confirm your entry by clicking on "OK".
   User status is modified. The corresponding symbol appears in the list next to the user name:

Symbol	Status
	The user is activated and logged in.
	The user is activated and logged off.
	The user is deactivated.

You can also activate or deactivate a user by opening the "Administration" tab in user settings and clicking on the checkbox "User is activated (deactivated)". See *11.2.1.1 The "Administration" Tab*, Page 164.

This is how you delete a user

1. Select the corresponding entry from the user table.
2. In the context menu, select "Delete".
3. Confirm your entry by clicking on "OK".
   All user data are removed from the database.

11.5 TO ASSIGN PROPERTIES OF A USER TO A NUMBER OF OTHER USERS

You can execute the configuration of a greater number of users faster, if you assign certain properties of an already configured user to all existing members of a group ("target group").

> You cannot undo the assignment of user properties to multiple users. Create a backup of the SwyxWare database before, *7.10 Backing up the SwyxWare Database*, Page 120.

> You cannot use the "Everyone" group as target group since the already configured user belongs to this group himself.
> To select users who are not in an existing group you can create a temporary group in advance, see *12.1 Create a group*, Page 215.

How to assign properties of a particular user to a group of users

You have configured the user as desired.

1. Right-click on the corresponding entry in the user list.
2. In the context menu, select "Clone properties...".
   You can specify the following parameters:

Name	Explanation
Client settings	Client settings should be assigned to the target group, See *11.2.6.1 The "General" Tab*, Page 185. Click on "Select" to activate the desired options.
Call Routing	Call routing settings (including rules and scripts) should be assigned to the target group, see *11.2.4 The "Call Routing Manager..." Dialog*, Page 181.
Speed dial entries from 1 to	Speed dial assignments should be assigned to the target group. Define how many speed dials (starting from the first, 160 chracters max.) should be assigned, see *11.2.6.4 The "Speed Dials" Tab*, Page 188.

Name	Explanation
Call Forwarding Busy	Settings for Call Forwarding Busy should be assigned to the target group, see *11.2.5.2 The "Call Forwarding Busy" Tab*, Page 182.
Call Forwarding No Reply	Settings for Call Forwarding No Reply should be assigned to the target group, see *11.2.5.3 The "Call Forwarding No Reply" Tab*, Page 183.
Call Forwarding Unconditional	Settings for Call Forwarding Unconditional should be assigned to the target group, see *11.2.5.1 The "Call Forwarding Unconditional" Tab*, Page 182.
Target group	Select a group for property cloning.

3 Click on "OK" to confirm the configuration changes.
The selected properties are assigned to all members of the group.

Members who are assigned to the group afterwards will not inherit the properties.
Assign the properties to the group again, if required.

11.6 CONFIGURE USERS IN THE WINDOWS USER ADMINISTRATION

This function is not available for SwyxON.

SwyxWare users can be managed in the Windows user administration. There you can

- when creating a new Windows domain user (Active Directory user and computer), directly create an associated SwyxWare user and assign him basic SwyxWare parameters such as name and number
- assign corresponding SwyxWare users to Windows users that already exist
- change basic SwyxWare parameters in the Windows user administration
- when deleting a Windows user account, remove the associated SwyxWare user directly

For information on the subsequent registration or deregistration of the Active Directory enhancement, see *E.2 Active Directory extension*, Page 425.

When users are created or edited in Windows user administration, this is usually done on an administrator's workstation computer. In order to display the corresponding SwyxWare tabs and wizard pages, please install the 'AD Integration' component of SwyxWare Administration on this workstation computer. The installation of the Active Directory enhancement with the SwyxServer simply expands the AD database with the relevant fields; it does not provide an interface. The scheme of the Active Directory won't be changed.

SwyxWare user assignment when creating a Windows user

When a new Windows user is created, additional pages appear in the wizard, querying the basic SwyxWare parameters.

This is how you create a new user in the Windows user administration.

1 In the user administration, select in the "User" context menu the entry "New". A wizard will guide you through the relevant steps. Only the steps which lead to the creation of an associated SwyxWare user are described in the following.

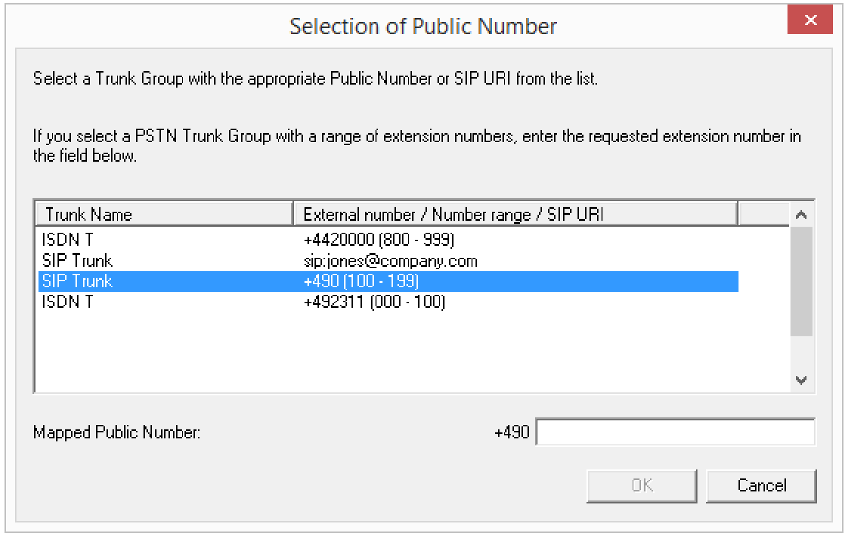
2 SwyxWare user name, and a description
Here you can also deactivate the checkbox "Create assigned SwyxWare user".
If the checkbox is activated, the SwyxServer is contacted.
In the first logon to SwyxServer, the logon parameters (Windows authentication or user name and password) are checked and stored,

so that a further logon takes place automatically. Please note that the rights for creating new users are required (*9.3 Administration profiles*, Page 143).

You can also assign an existing SwyxWare user to the new Windows user here. In this case the other parameters are not queried.

3 Internal Numbers
Enter the internal number for this user here.
Use "Verify" to immediately check whether this number has already been assigned.
Clicking on "Next unused" will automatically assign the next unused internal number to the user. You can also enter a number, e. g. 210, in order to leave the number range below untouched. Clicking on "Next unused" will then assign the next unused internal number. "Check" lets you check whether an entered internal number is already present.
Activate the checkbox "Show in Phonebook" if this number is to be listed in the Global Phonebook. Name resolution is always performed, regardless of whether the user is entered in the Global Phonebook.

4 Mapped public numbers
If the internal number is to be reachable from the public telephone network, it must be mapped to an external number. You can enter this public number directly in the field or click "Select...".
The "Choose public number" window will appear.



Selection of Public Number

Select a Trunk Group with the appropriate Public Number or SIP URI from the list.

If you select a PSTN Trunk Group with a range of extension numbers, enter the requested extension number in the field below.

Trunk Name	External number / Number range / SIP URI
ISDN T	+4420000 (800 - 999)
SIP Trunk	sip:jones@company.com
SIP Trunk	+490 (100 - 199)
ISDN T	+492311 (000 - 100)

Mapped Public Number: +490

Select the SIP URI or public number here.
If the public number is to be taken from a numbers range, double-click on that range.
Assign the external number in the "Mapped Public Number:" field and click "OK".

5 SwyxIt! Classic and SwyxFax Client are automatically assigned to the user. The logon configured here is via the associated Windows user account. See *11.2.1.1 The "Administration" Tab*, Page 164.

6 SIP Devices
Activate the checkbox, if you want to allow the registration with a SIP capable device. This option is deactivated by default.
Enter the following user information. Specify whether the authentication mode is chosen according to the server standard settings, or whether authentication should always or never take place. If authentication is required, enter here the necessary data for authentication, such as the user name and the password. These do not need to be identical to the SwyxWare user name and password that you may have configured for logon with a SwyxIt! Classic.
See *11.2.1.4 The "SIP Registration" Tab*, Page 169.

7 SwyxPhone Lxxx
Allow the logon with a SwyxPhone Lxxx.

Assign the user a PIN, with which he logs in to the SwyxServer. This PIN must contain between 1 and 16 digits.
See *11.2.1.6 The Tab "SwyxPhone Lxxx"*, Page 171.

8 Internal SwyxFax Numbers
Enter the internal fax number for this user here.
Use "Verify" to immediately check whether this fax number has already been assigned.
Clicking on "Next unused" will automatically assign the next unused internal fax number to the user.

9 Mapped public fax numbers
If the user also receives faxes from the public telephone network, an external fax number has to be assigned to the internal fax number. You can enter this public fax number directly in the field or click "Select...".

10 Mobile number
Enter the mobile number of the user in canonical number format.

11 E-mail address:
The user must be assigned a unique e-mail address for SwyxWare integration in Microsoft Office (SwyxIt! Classic function "Office Communication AddIn"). The e-mail address indicated must be the primary SMTP e-mail address set up for the user on the Microsoft Exchange Server.
This e-mail address is also the default setting for delivering voice messages. The e-mail address of the Voice Box can be configured by the user or in the SwyxWareadministration in the "Redirects" dialog, see *11.2.5.4 Standard Voice Box" tab*, Page 183.

A configuration of the special Voice Box e-mail address has no influence on the existing e-mail address that was created for the integration in MS Office.

12 Further parameters are created as standard:

- Location
  As location, the default location is assigned to the new user.
- Call Permission
  The default call permission is configured. See *Default Calling Right*, Page 136.
- Feature Profile
  The default feature profile is configured. See *Default Feature Profile*, Page 142.

13 The overview of the AD configuration wizard contains a summary of the SwyxWare parameters configured here.

Assign SwyxWare user to existing Windows users

A SwyxWare user can be assigned to existing Windows users in Windows user administration.

This is how you assign a SwyxWare user to a Windows user

1 Open the Windows user administration.

2 In the user's shortcut menu, open the properties and switch to the "SwyxWare" tab.

3 You have several different options:

- Select an existing SwyxWare user from the list. In this case the corresponding Windows user account is assigned to the SwyxWare user.

or

- Select the list entry "Create new SwyxWare user". A new SwyxWare user is created. All the necessary parameters will be queried by a wizard (*This is how you create a new user in the Windows user administration.*, Page 209 from step (3)).

SwyxWare user data amendment in Windows administration

You can also change basic parameters, such as the location or the feature profile of a SwyxWare user from the Windows user administration.

This is how you change the parameters of a SwyxWare user in the user administration

1 Open the Windows user administration.

2 In the user's shortcut menu, open the properties and switch to the "SwyxWare" tab.

3 You can change the following parameters here:
- SwyxWare user name
- Location
- Call Permission
- Feature Profile

4 Click on "SwyxWare Administration..." to open the SwyxWare Administration and enter further configurations for the user such as Call Routing scripts.

Delete an associated SwyxWare user or the link

In the Windows user administration you can delete a SwyxWare user, or just cancel the link between the Windows user and SwyxWare user.

This is how you delete a SwyxWare user in the user administration

1 Open the Windows user administration.

2 In the user's shortcut menu, open the properties and switch to the "SwyxWare" tab.

3 Remove the checkbox "Is SwyxWare user".

4 A query appears: do you want to remove the SwyxWare user altogether or cancel the link to this Windows user?

5 After confirmation with "OK", the user or link is removed.

11.7 EXPORT USER LIST

From within SwyxWare Administration you can export a list of all users directly into a file. This list can then e.g. be re-imported to the phonebooks of other SwyxServers.

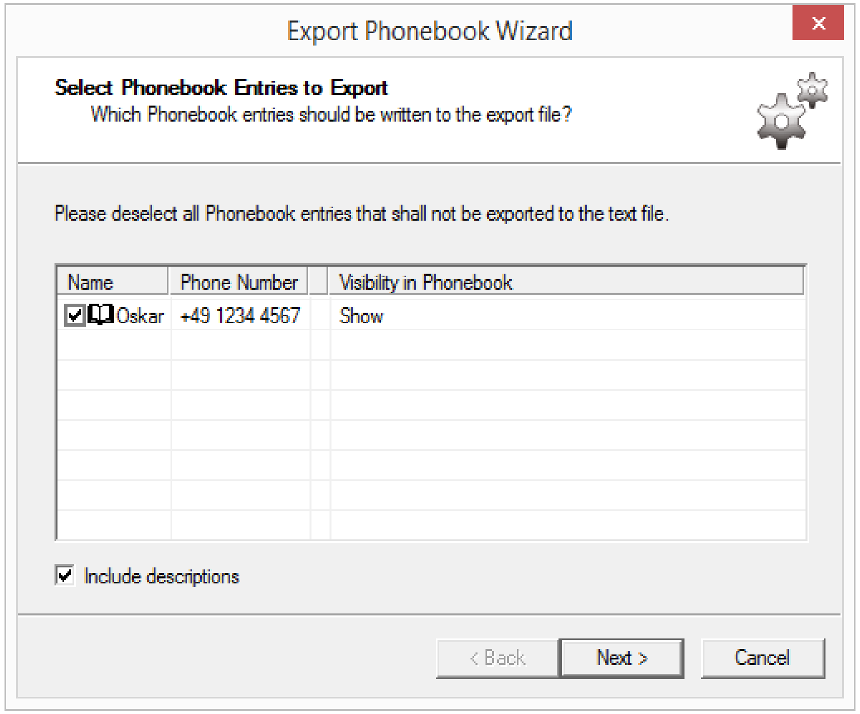
For further information on importing a user list into the phonebook of a SwyxServer, please refer to *7.6.1 The Import and Export of Phonebooks*, Page 116.

How to export the user list

1 Open the SwyxWare Administration and choose the SwyxServer.

2 Please select the "Users" folder and click with the right mouse button on the folder.

3 Select the entry "Export user list..." from the shortcut menu. The export wizard for the user list will open.


Export Phonebook Wizard

Select Phonebook Entries to Export

Which Phonebook entries should be written to the export file?

Please deselect all Phonebook entries that shall not be exported to the text file.

Name	Phone Number	Visibility in Phonebook
☑ Oskar	+49 1234 4567	Show

☑ Include descriptions

4 Activation of the corresponding checkbox will define which entries are to be exported. Furthermore, you define whether
- to export the user description
- to export the SwyxWare groups
- to export only the first entry for a user/group.

5 Click on "Next >".
Select the name and the path for the export file and define
- whether an existing file should be overwritten
- whether the first line of the file should contain the name of the

fields being exported (column name).

6 Click on "Next >".

7 Close the Export wizard with "Finish".
You will receive a CSV file in which the data fields are shown in quotation marks and separated by semicolons, whereby one line is used for each entry.

Example:

"Schmidt,Eva";"+4420123456789";"Description"

"Doe,John";"+4420999888777";"Description"

If you encounter problems when converting from databases, please refer to the corresponding articles in the Knowledge Base on our homepage.

11.8 VOICE BOX

Every SwyxWareuser has their own personal answering machine (voice box). Voice messages can be called up in the call journal and can optionally also be sent to an e-mail address. For this purpose, an e-mail system that uses SMTP (Simple Mail Transfer Protocol) as the mail transport protocol is used. Incoming calls can be forwarded to Voice Box with the Call Forwarding function.

See *22.3 Voice Box*, Page 348.

11.8.1 REMOTE INQUIRY

Remote Inquiry allows the user to listen to his voice messages and to change Call Forwarding Unconditional from any telephone line. When a user is called at the or her own SwyxWare number, he or she identifies him/herself to SwyxWare with a Remote access PIN; only then can he or she listen to, repeat, or delete new voice messages and afterwards all existing voice messages.

See *22.4 Remote Inquiry*, Page 349.

11.9 CONFERENCE

For online licensing information, see *3 Licensing via license key*, Page 28.

or

2 Online Licensing, Page 21.

The Conference function is implemented with the help of the "Swyx-ConferenceManager" service. The installation of the ConferenceManager can be carried out on SwyxServer or on an independent computer. The ConferenceManager takes over the management of the conference participants and mixes the voice data.

See *5.7.1 Installation of a SwyxWare component on an additional computer*, Page 67.

When ConferenceManager is installed, a user is set up that is specifically intended for operating this ConferenceManager. If more than one ConferenceManager is installed, a user is created for each ConferenceManager. The conferences are then distributed to the various ConferenceManagers.

If a ConferenceManager is activated, all users can use the Conference functionality, i. e. they can initiate conferences and add more than two subscribers to conferences. See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/import_export_phonebook_$.

For a user to be able to start a conference, he must have this functionality available in his feature profile (SwyxAdHocConference) and he must have the functional permission for it (*11.2.10 The "Properties..." Dialog: The "Rights" Tab*, Page 203).

11.9.1 CONFERENCE ROOMS

A conference room allows users to meet independently of each other. A Conference Room is represented by the internal number of a specific user known as "Conference". The name "Conference" can only be changed by the Administrator with the help of the configuration wizard. The Conference Room can be called by the conference participants independently of one another. The arrival of a caller in the conference room is signalled by a tone. The same is true for the departure from a conference.

A Conference Room is set up by assigning numbers to the user labelled "Conference" as you would for a normal user.

See *11.2.2.1 The "Numbers" Tab*, Page 177.

Each internal number of the user labeled "Conference" represents a different Conference Room. It is now possible to create rules for this user with the help of the Call Routing Manager in order to limit access to the Conference Rooms for example by PIN request, number of the caller or time of day.

See also https://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/import_export_phonebook_$.

In SwyxWare for DataCenter and SwyxON environment, the configured conference rooms are counted separately in the license report.

To add or remove a conference room is the same as to add or remove an internal number to the user "Conference". These changes will be written in the change log.

See *7.7 Change log*, Page 117.

Silent conference participation

Silent participants, i. e. participants who can listen to the conference call but not speak (ListenOnly), can be allowed to take part in conferences in conference rooms.

This functionality is implemented through an addition to the number of the conference room, the character sequence '#OWC'.

Please note that the complete string of digits (<number of conference room>#OWC) must be dialled as a block number.

The entry / departure of a silent conference participant is also announced by an audio signal. This signal is different from the usual entry/departure signal to indicate that this participant cannot take part in the conference call.

Example:

You set up a conference room with the internal number '219'.

With the help of you create a script that accepts calls to the number 219 and requests entry of a PIN. Depending on the entered pin, the call is branched: Callers who enter the sequence 1234 are forwarded directly into the conference (block 'Deliver'; to number '219'); callers who enter the sequence 6789 are also forwarded into the conference, but as listeners (block "Deliver'; to number '219#OWC').

12 CONFIGURATION OF GROUPS

Creation and configuration of Groups

In this chapter the creation and configuration of groups will be explained

In this context the configuration of the secretary functionality (Chese) is described.

12.1 CREATE A GROUP

Any number of groups with any number of members can be configured in a SwyxWare installation; a user can be a member of more than one group. Setting up groups makes it possible to contact members at a central group number.

How to create a group

1. Click with the right mouse button on "Groups" and select "Add Group...".
   The "Add new group..." Wizard will appear.
2. Group Properties
   Enter a name and, if required, a description for the group. The name must be unambiguous within SwyxWare.
   Indicate whether from now on all newly created users should be members of this group.

> The Checkbox "Make this group the 'Everyone Group'. All new users will be added to this group." can only be activated if you have previously deactivated this functionality in the "Everyone" group. However, new users will then no longer have access to the functionality of the pre-configured group "Everyone", e. g. Standard Call Handling.

See *The Group "Everyone"*, Page 86.

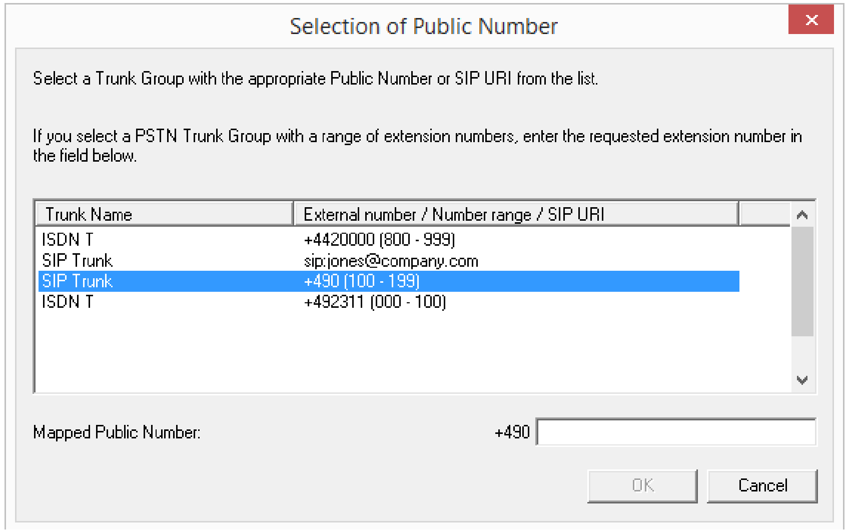
Click on "Next >".

3. Hunt group type:
   Specify how calls are to be delivered to the individual members. You have several options:
   - Parallel
     Calls to the group number are delivered simultaneously to all members. The person who accepts the call first speaks to the caller.
   - Sequential
     Calls to the group are delivered to each group member in order, always starting with the first group member.
   - Rotary
     Calls to the group are delivered to each group member in order, Always starting with the next group member, i. e. for the second call with the second member, for the third call with the third member and so on.
     Specify the maximum duration of an individual connection attempt, before the call is routed to the next member of the group.
   - Random
     Calls are distributed randomly within the group, i. e. when the specified time is over, the next member is selected randomly from the entire group.
     Specify the maximum duration of an individual connection attempt, before the call is routed to the next member of the group.

   Click on "Next>".
4. Internal number
   Assign the group an internal group number. All members of the group can be reached at this number.
   Use "Verify" to immediately check whether this number has already been assigned.
   Clicking on "Next unused" will automatically assign the next unused internal number to the user. You can also enter a number, e. g. 210, in order to leave the number range below untouched. Clicking on "Next unused" will then assign the next unused internal number. "Check" lets you check whether an entered internal number is already present.

Activate the checkbox "Show in Phonebook" if this number is to be listed in the Global Phonebook. Name resolution is always performed, regardless of whether the user is entered in the Global Phonebook.
Click on "Next>".

5 Internal number mapping:
If the internal number is to be reachable from the public telephone network, it must be mapped to an external number. You can enter this public number directly in the field or click "Select...".
The "Choose public number" window will appear.



Selection of Public Number

Select a Trunk Group with the appropriate Public Number or SIP URI from the list.

If you select a PSTN Trunk Group with a range of extension numbers, enter the requested extension number in the field below.

Trunk Name	External number / Number range / SIP URI
ISDN T	+4420000 (800 - 999)
SIP Trunk	sip:jones@company.com
SIP Trunk	+490 (100 - 199)
ISDN T	+492311 (000 - 100)

Mapped Public Number: +490

Select the SIP URI or public number here.
Assign the external number in the "Mapped Public Number:" field and click "OK".
Click on "Next>".

6 Group members
Add the users who are to be members of this group. Click "Add..." to select SwyxWare users from a list.
You can select and add several users at the same time by keeping the Ctrl button pressed.
With the sequential and rotary call Hunt Group types the order of group members is observed. Use the arrows to sort the group members so that the first member is at the top of the list.

You can also add users later by selecting the users in the user list and moving them into the group per Drag&Drop.

7 End the set up of the group by clicking on "Finish".

The users assigned to a group will be shown when you highlight the desired group in the "Groups" directory. The members will then be listed in the window on the right.

How to add a user to a group or remove a user from a group

1 Click with the right mouse button on the group in which you would like to add or remove the user and then select "Properties".

2 Select the "Members" tab.

3 Click on "Add".

4 Select the desired users in the dialog which now appears. If you would like to remove a user from a group, highlight this user and click "Remove".

Or

1 Select the user list.

2 Highlight all the users that you would like to add to or remove from the group. Hold down the CTRL key to select multiple users.

3 Move all users into the group by drag&drop.

Users newly added to the group are always inserted at the end of the group. Use the arrow keys on the right-hand side of the list to change the position of a new user within the group.

12.2 CONFIGURE GROUP

You can configure the properties of a group in the same way as you would the properties of a user.

Within the groups, calls can be distributed in different ways, e. g. to all members simultaneously, sequentially, rotary or randomly.

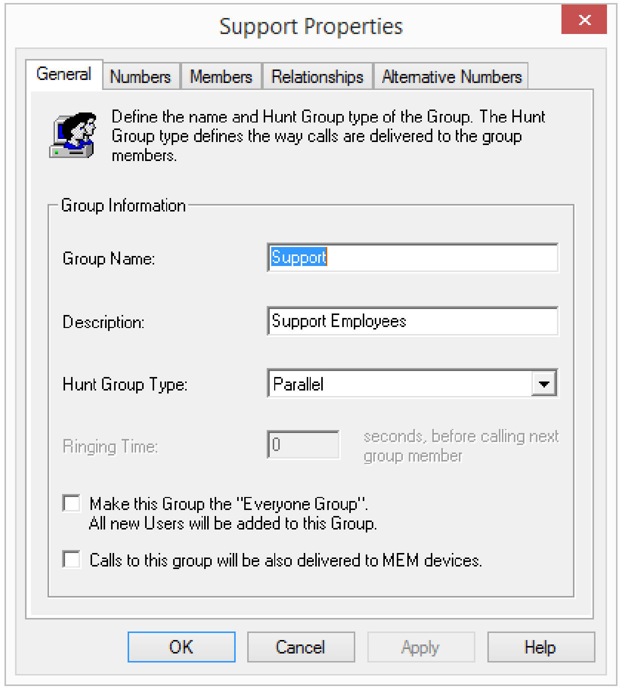
The Administrator can configure lines for the group members so that the group number is always shown for outgoing calls.

See *12.2.2 The "Properties..." Dialog The "Numbers" Tab*, Page 218.

In addition, creating groups makes it easier to assign user relationships.

See *12.2.4 The "Properties..." Dialog The "Relationships" Tab*, Page 219.

12.2.1 THE "PROPERTIES..." DIALOG THE "GENERAL" TAB


Support Properties

Define the name and Hunt Group type of the Group. The Hunt Group type defines the way calls are delivered to the group members.

Group Information

Group Name: Support

Description: Support Employees

Hunt Group Type: Parallel

Ringing Time: 0 seconds, before calling next group member

□ Make this Group the "Everyone Group". All new Users will be added to this Group.

□ Calls to this group will be also delivered to MEM devices.

You can also change the name of a group here after creating it.

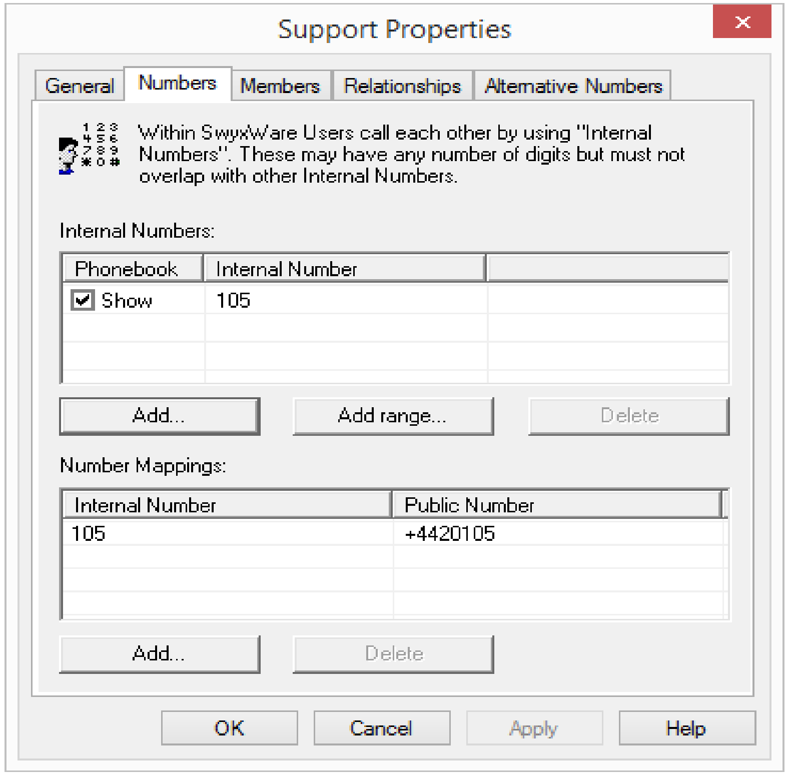
Do not change the names of the pre-configured groups "Operator", "Sales" and "Support". Otherwise the Auto Attendant will no longer function.

In the field "Hunt Group Type", define how the calls will be distributed:

- Parallel
  Calls to the group number are delivered simultaneously to all members. The person who accepts the call first speaks to the caller.
- Sequential
  Calls to the group are delivered to each group member in order, always starting with the first group member.
- Rotary
  Calls to the group are delivered to each group member in order, Always starting with the next group member, i. e. for the second call with the second member, for the third call with the third member and so on.
- Random
  Calls are distributed randomly within the group, i. e. when the specified time is over, the next member is selected randomly from the entire group.

The Checkbox "Make this group the 'Everyone Group'. All new users will be added to this group." can only be activated if you have previously deactivated this functionality in the "Everyone" group. However, new users will then no longer have access to the functionality of the pre-configured group "Everyone", e. g. Standard Call Handling.

12.2.2 THE "PROPERTIES..." DIALOG THE "NUMBERS" TAB



Within SwyxWare Users call each other by using "Internal Numbers". These may have any number of digits but must not overlap with other Internal Numbers.

Internal Numbers:

Phonebook	Internal Number	
☑ Show	105	

Number Mappings:

Internal Number	Public Number
105	+4420105

The internal numbers and their mapping to public numbers or URIs are configured on this page.

Internal numbers

You see a list of the internal numbers for this SwyxWare group.

For each of these entries you can indicate whether the number should be shown in the SwyxWare Global Phonebook. Do do this, activate the checkbox on the line with the corresponding number.

You can delete individual entries by highlighting them and then clicking "Remove". If you would like to add further numbers, click "Add..." and specify a new internal number, and - if desired - a mapped external number or URI.

If the number is not available, a warning appears.

You can insert a numbers range here with "Insert range...".

If numbers within the numbers range are already assigned, these remain mapped to their users. In that case only unused numbers within this range will be assigned to the group.

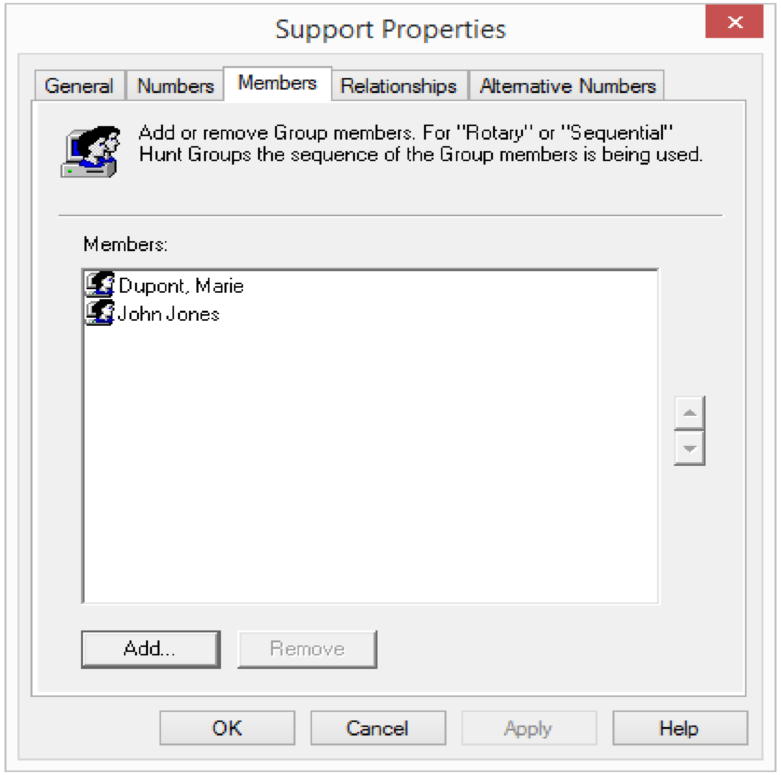
Number Mappings

In this section is a list of the internal numbers and the corresponding mappings to public numbers or URIs.

You can delete individual entries by highlighting them and then clicking "Remove". If you would like to add further numbers, click "Add..." and specify a new internal number, and - if desired - a mapped external number or URI.

If numbers within the numbers range are already assigned, these remain mapped to their users. In that case only unused numbers within this range will be assigned to the group.

12.2.3 THE "PROPERTIES..." DIALOG THE "MEMBERS"



Support Properties

Add or remove Group members. For "Rotary" or "Sequential" Hunt Groups the sequence of the Group members is being used.

Members:

Dupont, Marie
John Jones

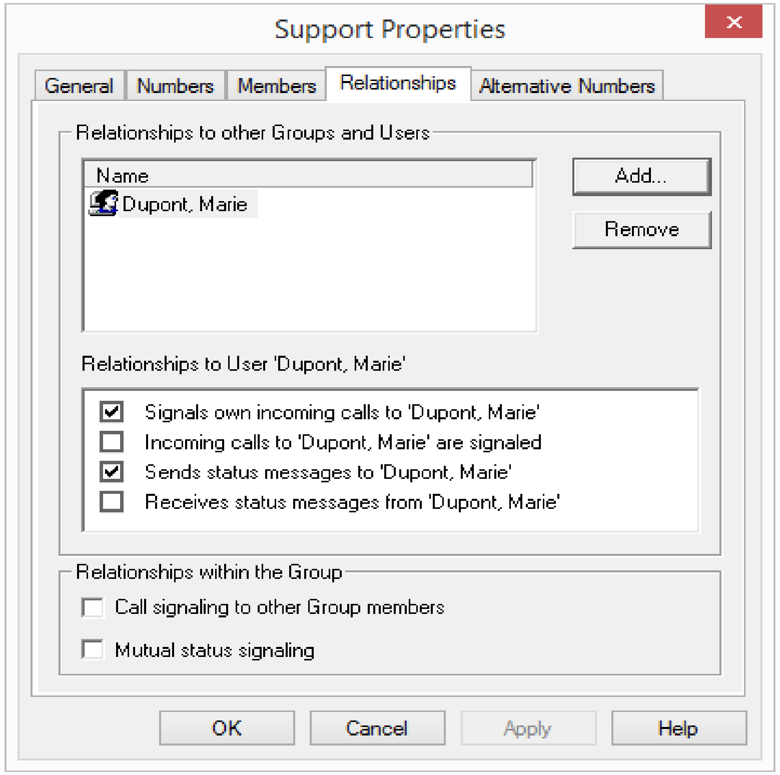
An overview of the group members is given on this page.

You can add or remove members here.

An easy method to add one or several users to a group is by moving them per drag & drop from the user list in the window on the right to the respective group in the window on the left.

You can specify the order of the group members - relevant for the Hunt Group - here by moving the highlighted group member with the arrows.

12.2.4 THE "PROPERTIES..." DIALOG THE "RELATIONSHIPS" TAB



Support Properties

Relationships to other Groups and Users

Name
Dupont, Marie

Relationships to User 'Dupont, Marie'

☑ Signals own incoming calls to 'Dupont, Marie'
☐ Incoming calls to 'Dupont, Marie' are signaled
☑ Sends status messages to 'Dupont, Marie'
☐ Receives status messages from 'Dupont, Marie'

Relationships within the Group

☐ Call signaling to other Group members
☐ Mutual status signaling

Relationships help you define whether calls for a user or that user's current status are signaled to other users or groups, even across servers. Call signalling will be shown in clients and SwyxPhones. The status, which includes "Logged off", "Available" and "Speaking", is indicated with the help of the Speed Dials and in the Phonebook. For more information on visual or acoustic signaling, see https ://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/status_signaling_$

and https ://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/call_signaling_$.

Relationships to other groups and users

Here you can define relationships to other users or groups. The page contains the respective call or status signals of the group members to the user or group selected above. If you have used a SwyxLink trunk to configure a cross-server connection to another SwyxServer, then you likewise specify here the recipient on the linked site to whom the selected user signals the status.

Relationships within the group

Here you define the call and status signalling within the group.

A user can only call another user per intercom connection or use the SwyxIt! Messenger if he or she is signaled the status of the other user.

If a user is a member of a group, the relationships defined within the group will also apply to this user. The group will not be shown in the relationships list if you define additional relationships in the properties dialog for this user. For the purpose of clarity, relationships to groups should only be entered via this user dialog if the user is not a member of this group.

Please note that call and status signaling always relates to users or users as group members and not to groups as such. This means, for example, that a group without members cannot signal any calls to other users or groups.

The following relationships can be configured for a User/Group A:

- "Signaled calls to <User/Group B>"
  When this setting is made, calls which are for User A or a member of Group A will also be signaled to User B or all members of Group B. Users to whom a call is displayed in this manner then have the option of picking up the call.
- "Incoming calls for <User/Group B> are signaled"
  If this setting is activated, all calls directed to User B or members of Group B will be signaled to User A or all members of Group A.
- "Sends status messages to <User/Group B>"
  When this setting is activated, User A or all members of Group A inform(s) User B or all members of Group B about their status. This allows User B / all members of Group B to contact User A / all members of Group A by Intercom.
- "Receives status message from User/Group B"
  With this setting User A / all members of Group A receive(s) the status messages of User B / all members of Group B. This allows User A / all members of Group A to contact User B / all members of Group B by Intercom.

When dealing with groups, the following settings will define the relationships within the group:

- "Call signaling to other group members"
  Incoming calls for one member of a group will also be signaled to all other group members. This gives the other members the opportunity to pick up the call.
- "Mutual status signaling"
  All members of the group signal their status (Logged off, Available, Speaking) to the other members. This allows all members of the Group to contact each other directly.

It is easiest to explain the use of the group functionality using a practical example:

> Five employees work in the Support department of a company (e. g. in London). These employees are defined as SwyxWare users and are all assigned to the SwyxWare group ‘Support’. The Support employees have the numbers 101-105. The Support group has been assigned the number 100.

It is now possible to cover various functionalities:

- Calls to the group number 100 are to be signaled to all Support employees.
  All calls to the group number will also be delivered to the individual Support employees, because the Support employees have been assigned to the Support group. The calls are distributed according to the Support group's Hunt Group type (parallel, sequential, rotary or random). This allows any Support employee to pick up incoming calls for the group number 100.

- Calls for Support employee A are also to be displayed to the other Support employees so that they can pick up the calls if employee A is absent.

  In order to configure for this, you must activate "Call signaling to other group members" within the relationships of the group.
- If all Support employees should receive information on the status of the other employees, "Mutual status signaling" must be activated in the group configuration. This configuration makes sense if you would like to know immediately whether you can forward the call from a customer with specific questions directly to the appropriate expert, or whether this expert is absent or already on the telephone with another customer.
- The department manager of the Support group is to receive all of the employees' status and call signaling, while he himself does not want to signal his calls or his status to the employees for confidentiality reasons.

  For this configuration, activate call and status signaling within the Support group. Do *not* add the Support department manager to the Support group, as otherwise the department manager's calls and status messages will be signaled to the group. However, in order for the department manager to receive the signaling for the Support employees, you must explicitly add the department manager to the relationships configuration of the group and activate the relationships "Signals incoming calls to 'Department Manager'" and "Sends status messages to 'Department Manager'". You can also create this configuration for the user Department Manager on the "Relationships" tab by adding the group there and activating the appropriate relationships.

How to configure relationships for groups

1 Click on the group or user to be configured with the right mouse button and select "Properties".

2 Select the "Relationships" tab. Add the users and groups you want in the section "Relationships to other Groups and Users". If an intersite connection is configured, users and groups of the linked SwyxServer are shown here as well. Now highlight a user or a group from the list and configure the appropriate relationships. If you are in the process of configuring the relationships within a group, you also have the option of configuring the relationships of the group members in the "Relationships within Group" section.

Please note that deactivating a signaling option will not cancel any other settings! This means, based on the above example, if you add the Support department manager to the Support Group, which signals calls and status messages within the group, and if you also enter a relationship between the department manager and the Support Group, in which you deactivate signaling to the group, the group will still be signaled the calls and the status messages of the department manager.

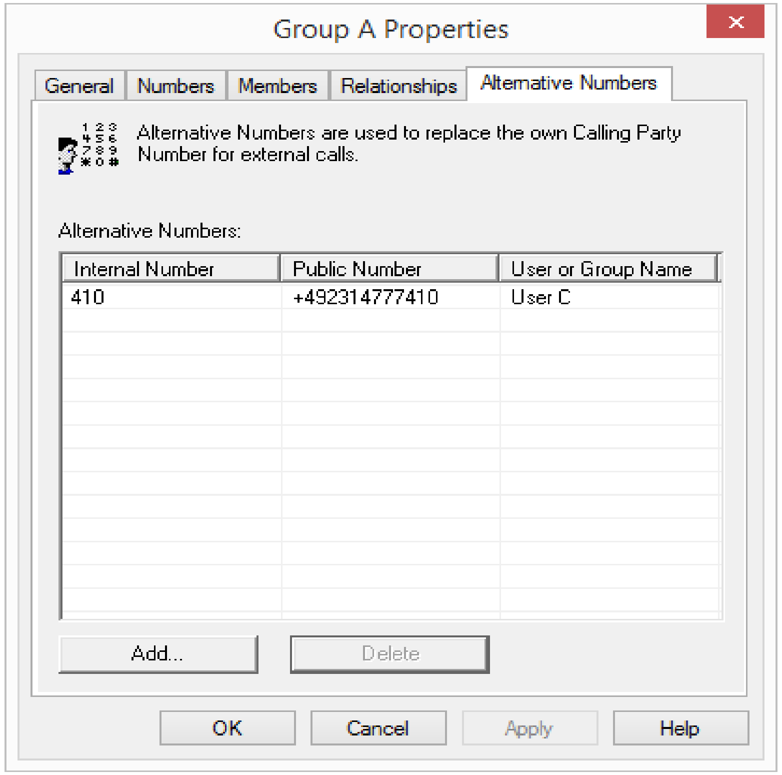
12.2.5 THE "PROPERTIES..." DIALOG THE "ALTERNATIVE NUMBERS" TAB

Alternative numbers can be specified here, which a user belonging to the group can signal to the call partner on outgoing calls.

Which alternative number users in the group finally signal is defined on a line in the SwyxIt! Classic/SwyxPhone. Alternative numbers are marked there by the addition Alternative number. See ***11.2.6.6 The"Line keys" Tab***, Page 190.

Example:

The administrator can allow every SwyxWare user to signal the operator's number (+44204666100) externally, by adding this number as an alternative number to the group "Everyone". This allows every user to configure this number on the line button as outgoing number..



Alternative Numbers are used to replace the own Calling Party Number for external calls.

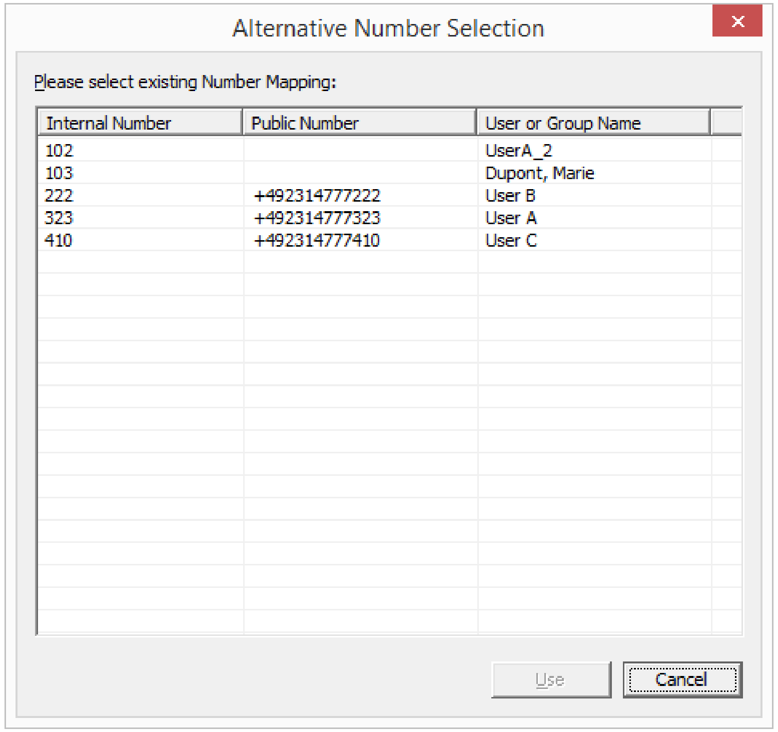
Alternative Numbers:

Internal Number	Public Number	User or Group Name
410	+492314777410	User C

To remove the assignment of the alternative number, highlight it and click on "Remove".

> If the deleted number is specified within the user configuration as the number/URI for outgoing calls, then outgoing calls that should go via this number are discarded. So use another number/URI for incoming and outgoing calls.

To add an Alternative Number, which the SwyxWare user in this group should signal on outgoing calls, click on "Add...".



Please select existing Number Mapping:

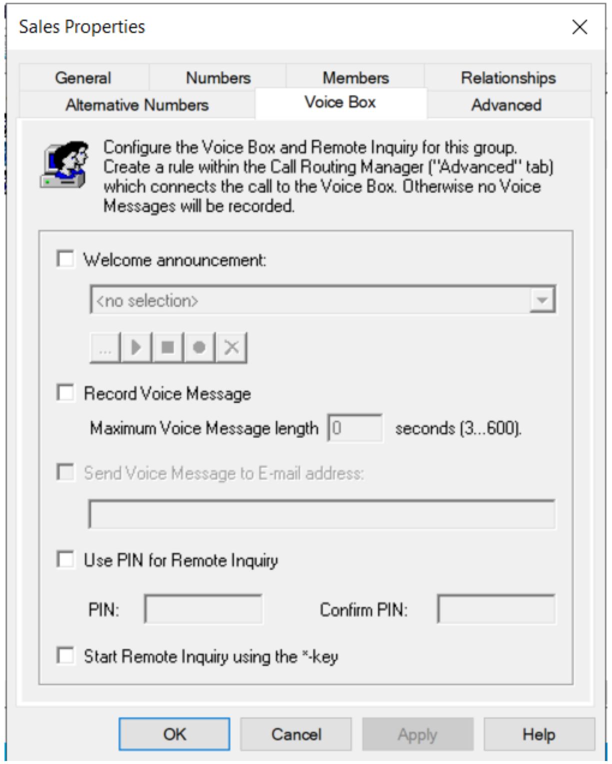
Internal Number	Public Number	User or Group Name
102		UserA_2
103		Dupont, Marie
222	+492314777222	User B
323	+492314777323	User A
410	+492314777410	User C

You can choose from all numbers which are assigned within SwyxWare and are not allocated to this group. Highlight the alternative number you want, and click "Use". Close the tab with "OK" to save the changes you have made.

> Next, configure the number/URI for outgoing calls for the group's SwyxWare users on a specific line button. See *11.2.6.6 The"Line keys" Tab*, Page 190.

12.2.6 THE "PROPERTIES..." DIALOG THE "VOICE BOX" TAB

A separate Voice Box (answering machine) can be configured for each group.



Configure the Voice Box and Remote Inquiry for this group. Create a rule within the Call Routing Manager ("Advanced" tab) which connects the call to the Voice Box. Otherwise no Voice Messages will be recorded.

□ Welcome announcement:

<no selection>

□ Record Voice Message

Maximum Voice Message length 0 seconds (3...600).

□ Send Voice Message to E-mail address:

□ Use PIN for Remote Inquiry

PIN: Confirm PIN:

□ Start Remote Inquiry using the *-key

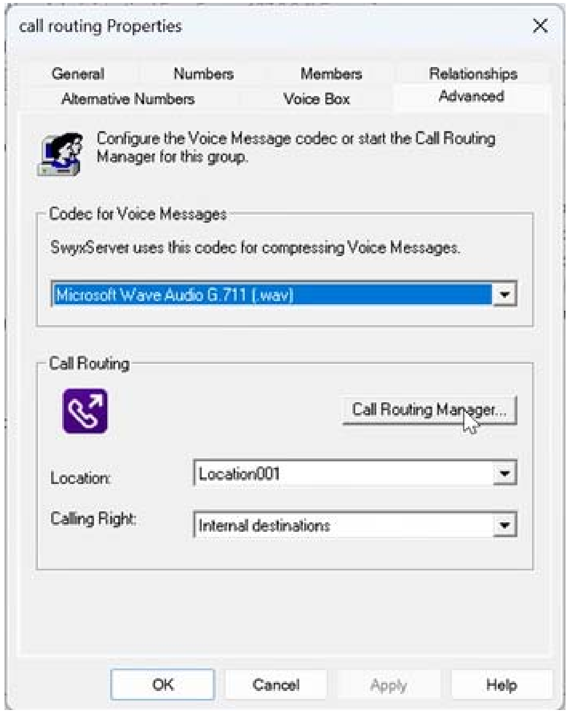
Just as with a user, a standard greeting can be played or an individual greeting can be recorded, which is then played as soon as a call is transferred to the Voice Box. The maximum length of the voice message in seconds and the e-mail address(es) to which the recorded voice message should go can also be specified.

If the * key is also to be used to retrieve the group voice announcements via remote inquiry, the function can be activated here. However, this requires a PIN configuration. When calling a SwyxWare group number, the user identifies himself to SwyxWare using his PIN and can then first listen to the new and then all existing voice messages of the group, play them repeatedly and delete them if necessary.

> In order for voice messages to be recorded, you must create a rule in the Call Routing Manager (Advanced tab) that routes the call to the Voice Box. See *Call Routing*, Page 224

12.2.7 THE "PROPERTIES..." DIALOG THE "ADVANCED" TAB

Here the Call Routing Manager opens with the rulebook of the selected user.



Configure the Voice Message codec or start the Call Routing Manager for this group.

Codec for Voice Messages

SwyxServer uses this codec for compressing Voice Messages.

Microsoft Wave Audio G.711 (.wav)

Call Routing

Location: Location001

Calling Right: Internal destinations

Codec for voice messages

The codec for compressing voice messages for the group can be set to the server default or a special codec.

Open Standard RFC 6716 (.opus)	Dynamically adjustable bit rate. Best audio quality/ storage spaceratio. (Default setting after installation.
Microsoft WAV Audio G711	WAV file, G.711 compressed

Microsoft WAV Audio GSM	WAV file, GSM compressed
Microsoft WAV Audio PCM	Standard WAV file, not compressed

Call Routing

Here the Call Routing Manager opens with the rulebook of the selected group.

Please note that scripts created using use of the Graphical Script Editor. must be signed for your SwyxServer. Otherwise the Call Routing Manager cannot apply them in its set of rules.

See *22.1 Call Routing Manager and Graphical Script Editor*, Page 347.

Location	Location of the group: Select a location for the group from the drop-down list. The location defines the location-specific parameters such as country and area code, area codes, the outside line access code(s) and the time zone, see *8 Locations*, Page 122.
Call Permission	Select a call authorization profile for the group from the drop-down list. Call permissions and restrictions are grouped together in a profile. See *9.1 Call Permissions*, Page 128.

12.3 SECRETARIATE

The manager normally does not receive any calls directly, but rather all of his/her incoming calls (i. e. incoming calls to his/her numbers) are forwarded through the defined secretariate number. As a result, the secretariate receives all calls, both those calls intended for the secretariate and those for the manager. All calls received in the secretariate are shown on the display of the manager's telephone and after a predefined time period, the calls will be signaled to the manager with an attention tone. Those calls which are received for the manager will be connected to the manager by the secretariate staff after (or without) inquiry.

The scenario described above, which is often called the manager-secretariate function, represents a combination of different parameters from the SwyxWare point of view, and these parameters must be appropriately configured by the participating users.

SwyxWare Administration Provides a wizard for this purpose to help you to set up a secretariate configuration with just a few mouse clicks.

This wizard is started on the "Secretariate" tab. This tab can be opened using the context menu in the detail view of the highlighted user or via the appropriate symbol in the toolbar. The tab offers an overview of the secretariate configuration in which the respective user is involved. The managers for which the user has accepted a secretariate function are listed in the upper section ("...is secretariate of"). If the user has a managerial function, the appropriate secretariate is listed in the lower list view ("...is manager of"). By clicking on the correspondingly labeled button next to the list views, you can create a new secretariate configuration for the user or clear existing configurations.

A user can take on the secretariate function for several managers. Each manager, however, is assigned exactly one secretariate. Therefore, after creating a secretariate configuration in which the user functions as a manager, the "Add" button for the lower list view is deactivated.

This is how you set up a new secretariate configuration

1 Depending on whether the user should be defined as a secretariate or a manager, click on "Add" in the upper or the lower list view. The wizard for setting up the secretariate configuration will open.

2 On the start page, select the second user for the secretariate configuration from the list. If the wizard was opened via "Add" in the upper list view, the user selected here will be assigned the chosen functionality.

3 On the next page, indicate which SwyxWare parameters are to be adjusted for the secretariate configuration. On the one hand, these

parameters include the call forwarding functions that are useful in connection with a CheSe functionality, such as the immediate and delayed forwarding of calls for the supervisor to the secretary and the delayed forwarding of calls for the secretary to the Standard Voice Box. On the other hand, you can also define whether mutual call and status signaling should be activated for both users and whether a Speed Dial is set up for each of the configuration partners in SwyxPhone and SwyxIt! Classic. All of the options described up to this point are automatically preselected. If you would also like both users to use the same SwyxIt! Classic skin, please activate the appropriate checkbox. The number of following dialogs within the wizard depends on the selection made on this page:

4. If you have activated the option "Configuration of the manager's first speed dial with the secretariate's number and vice versa", the corresponding configuration dialog will now appear. If both of the users involved already have Speed Dials set up, you can indicate here whether the existing Speed Dial should be overwritten or whether a new Speed Dial should be added. If a user has several numbers, you can choose the number to be assigned to the Speed Dial from a list.
5. If you have activated the option "Use of the same SwyxIt! Classic Skin for manager and secretariate", a dialog will appear in which you can choose whether the manager's or the secretariate's skin will be used as the common skin.
6. On the last page of the wizard, you will be shown an overview of those user properties which will be changed as a consequence of the new secretariate configuration. Click on "Finish" to start the configuration process. This process may take a moment to complete. After confirming the successful creation of a new secretariate configuration you will automatically be returned to the "Secretariate" tab. The user for whom a new secretariate relationship has been created should now appear in the appropriate list view.

Any changes made to the SwyxIt! Classic skin will not take effect until the user in question has logged in to the SwyxServer again!

This is how you remove an existing secretariate configuration.

1. Open the "Secretariate" tab for one of the involved users.
2. In the "Secetariate" tab, select the user for which you want to remove the secretariate configuration.
3. Click on the "Remove" button next to the corresponding list view in which the user was selected.
   The wizard for clearing a secretariate configuration will now open.
4. On the start page, you will once again see both users for whom the secretariate configuration is to be removed. Click on "Next" if you are sure you want to remove the configuration.
5. The dialog which follows allows you to select the individual SwyxWare parameters that are to be reset when removing the secretariate relationship between the two users. Parameters which you or one of the users have changed manually since the creation of the secretariate configuration appear grayed out and cannot be selected.
6. Click "Finish".
   The parameters you selected are reconfigured. After successful removal of the secretariate configuration, you will automatically return to the "Secretariate" tab.

13 TRUNKS AND TRUNK GROUPS

Trunks and trunk groups as connections from a SwyxWare installation to the outside world

Configure trunk groups

Activating and deactivating a trunk

"Trunk" denotes a connection to another network, e.g. the public telephone network. A connection to another network can be e.g. an "ISDN trunk", a connection to the Internet an "SIP trunk". Connections or trunks of the same type are combined to form groups. The trunks of a trunk group then have the same properties (such as the same connection protocol or the same rights parameters). The trunks of a trunk group are thus primarily "capacity expansions" from the user's point of view, with no further differences for their use. A trunk must always be a member of a trunk group.

We distinguish between various trunk types:

- ISDN Trunk (SwyxGate lines)
- SIP Trunk
- SIP Gateway Trunk
- ENUM Trunk
- SwyxLink Trunk (Server-server coupling)

ISDN Trunk (SwyxGate lines)

ISDN trunks are all ISDN lines, - whether for the S0 Basic Rate Interface Connection or the S2m Primary Rate Interface - with which a gateway (SwyxGate) is connected via ISDN cards to the public telephone network or a superior or subordinate telecommunication system.

Installation of the ISDN Cards *15.2 Installation of the ISDN Cards*, Page 246

To configure a ISDN Trunk, see*15.4 Creation of an ISDN trunk*, Page 267.

SIP Trunk

SIP trunks enable the use of VoIP services that are provided by carriers or service providers. The service provider provides you with a phone number or a number range. Alternatively the SwyxWare users can be assigned SIP addresses (SIP-URIs, e. g. "tom.jones@.com") or entire ranges (e. g. *@company.com) by the provider, which can be used as an "email address for a telephone". By this means, SwyxWare users can globally reach other SIP-URIs, and be reached themselves. If this service provider also offers gateway services, it will also be possible to reach any phone in the public telephone network via an SIP trunk and the underlying gateway of the provider.

See also *16 SIP Links*, Page 278.

SIP Gateway Trunk

SIP gateway trunks are used for activating gateways which are themselves reached by SwyxServer via an SIP connection. Thus e.g. SwyxConnect is addressed within SwyxWare as a SIP gateway trunk. This allows e.g. telephones in small branch offices to be operated with a local gateway in each case and with a local direct connection to the PSTN. In this way, sophisticated requirements of a company network can also be met when there are numerous small sites (e.g. many shops in a chain of stores).

Only gateways for which profiles are included in the delivery are supported at present.

To configure a SIP Gateway Trunk, see*19 SIP Gateway Links*, Page 321.

ENUM Trunk

An ENUM link enables you to make SIP calls with ENUM number resolution via the Internet.

A user of a SIP phone is thus able to investigate the SIP address automatically using only the telephone number of the called party, and to convert the number into the SIP address. The called party can then be reached over the IP network in spite of using a 'normal' phone number. This postulate that the called party is registered at ENUM.

See also *18 ENUM Links*, Page 309.

SwyxLink Trunk (Server-server coupling)

SwyxServers at different sites are interconnected via a SwyxLink trunk via an IP route. The SwyxLinkManager assumes control of the connection. You can configure a connection to further SwyxLink sites within the configuration of a SwyxWare trunk, so that status information (logged off, free, speaking) can also be exchanged between users who are logged in to different servers.

It is also possible to use the Collaboration, Video and Instant Messaging features (only SwyxIt! Messenger, not Swyx Messenger) across different servers via the SwyxLink trunk.

See also *17 SwyxLink (Server-Server Connection)*, Page 292.

Setting up trunks and trunk groups

Set up trunk groups first. Parameters such as the location are assigned to these trunk groups. All trunks belonging to a trunk group then have common parameters, e.g. a common location.

Then set up individual trunks, specifying the corresponding trunk group to which each individual trunk belongs. If there is not yet a trunk group with the appropriate parameters, then while setting up a trunk you can also set up a further trunk group.

For details of which group parameters you need for which trunk type, please see the chapter on the relevant trunk type.

Once you have set up a trunk group, you can set up the individual trunks. An individual trunk can be e.g. an ISDN line with two B channels, or an SIP connection to a provider.

For details of which parameters you need for which trunk type, please see the chapter on the relevant trunk type.

Editing trunks and trunk groups

If parameters of a trunk or trunk group are changed, you can update the new parameters in the properties of this trunk or the trunk group.

This is how you edit a trunk or a trunk group

1. Open the SwyxWare Administration.
   Open the trunks or trunk groups.
2. Highlight the trunk or trunk group that you want to edit.
3. In the context menu (right mouse button) of the trunk or trunk group, select "Properties".
   The window labeled "Properties of ...." will open.
   You will now see different tabs depending on the type of trunk or trunk group.
   See also *13.1 Configure trunk groups*, Page 227.
4. Make the necessary changes, then click on "OK".

The trunk or trunk group adopts the changed parameters at once.

Deleting a trunk or a trunk group

You can remove a trunk or a trunk group in the SwyxWare Administration.

This is how you remove a trunk or a trunk group

1. Open the SwyxWare Administration.
   Open the trunks or trunk groups.
2. Highlight the trunk or trunk group that you want to remove.
3. In the context menu (right mouse button) of the trunk or trunk group, select "Delete...".
   The trunk or trunk group is removed. The connection is subsequently no longer available.

13.1 CONFIGURE TRUNK GROUPS

A trunk group represents all the trunks of the same type which are grouped together in it. The properties that are the same for all trunks of this group (such as the connection protocol and the permissions) are specified by the properties of the trunk group. The group properties can still be changed after the creation of a trunk group.

When parameters of a trunk group are changed, this change takes effect at once. There is no need to halt and restart any services for this.

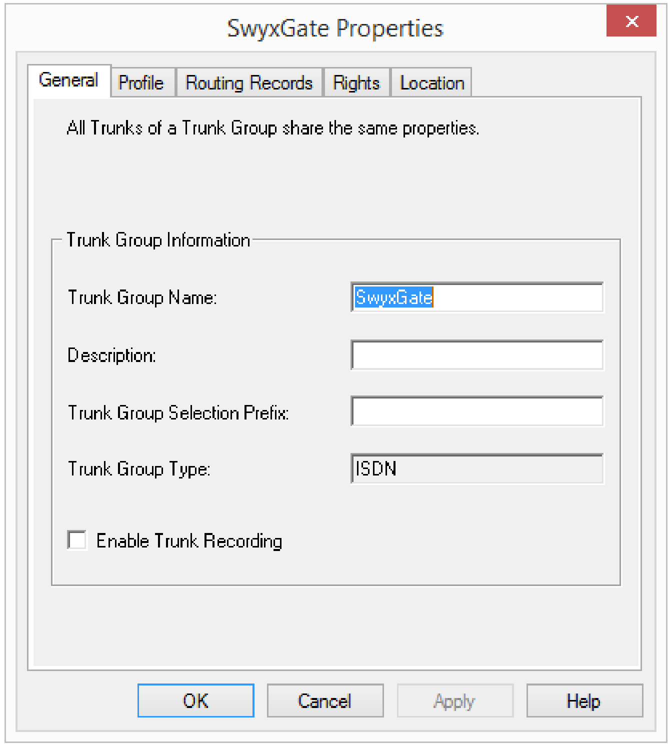
This is how you configure a trunk group

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click on "Trunk groups", and in the right-hand window select the trunk group you want to configure.

3 In the context menu, select "Properties".
In each case, the "Properties of..." window will appear.

13.1.1 THE "GENERAL" TAB



All Trunks of a Trunk Group share the same properties.

Trunk Group Information

Trunk Group Name: SwyxGate

Description:

Trunk Group Selection Prefix:

Trunk Group Type: ISDN

□ Enable Trunk Recording

In this tab you can modify the name and description of the trunk.

This tab appears for all trunk groups.

Trunk Group Information

In the fields "Trunk Group name" and "Description" you will find the descriptive information that is displayed in Administration. The name must be unambiguous within SwyxWare; the description is optional.

In the field "Trunk Group Selection Prefix", a prefix can be specified to allow a user to route a call specifically via this trunk group. This character string can have up to 10 characters, and can consist of the characters "0123456789*#". The selection prefix must be uniquely assigned to one trunk group; it cannot be multiply assigned.

Please note that the character string for the Trunk Group prefix may not begin with the public line access, nor with an existing internal number. We also recommend having the trunk group prefix begin / end with * or #, so as to achieve a better delimitation for the destination numbers.

If a user defines which trunk group should be used for the next call by using the assigned selection prefix, no further routing records are applied.

If a project code is used in addition to the trunk group prefix, please enter this first. The project code always begins with * and ends with #.

Examples:

In the following, the project code is *1234# and the trunk group prefix is **34#

- <*Project code#><Trunk Groups prefix><Canonical number>

  *1234#**34#+44123555777
- or if using a public line access
  <*Project code#><Trunk Groups prefix><Public line access><National number>

  *1234#**34#00123555777
- or if using an internal number
  <*Project code#><Trunk Groups prefix><Internal number>

  *1234#**34#123555777
- or if using an SIP URI (always beginning with sip:)
  <*Project code#><Trunk Groups prefix><SIP:URI>

  *1234#**34#sip:han.solo@millenium-falcon.com

If the user enters a Trunk Group prefix, only trunks of this trunk group are selected and no further attempt is made to make the call via different trunks.

The "Trunk Group Type" field provides information about the type of Trunk Group.

Record all Trunk Calls

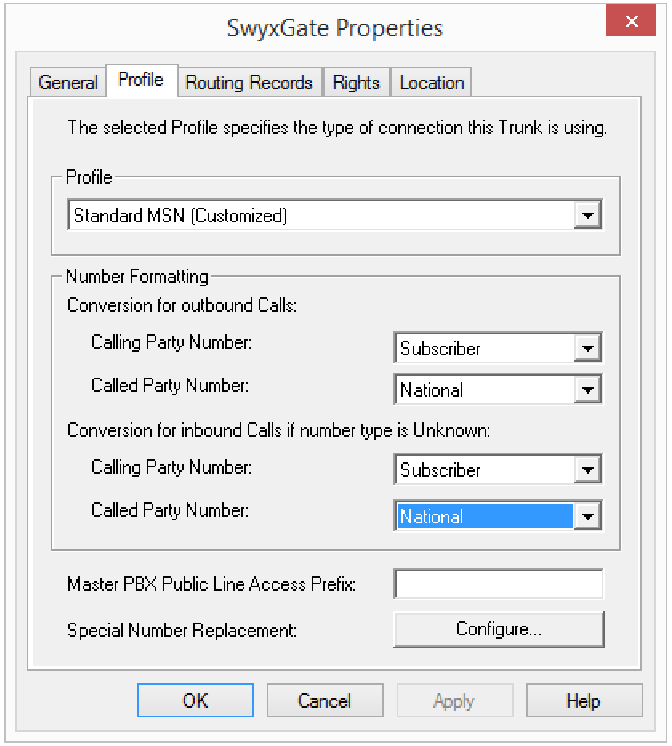
If you activate the checkbox "Enable Trunk recording", all calls that are made via this trunk group will be permanently recorded, provided this is activated in the SwyxServer settings, see *7.5.7 The "Trunk Recording" Tab*, Page 94

There are different options for recording the call:

- Record all trunk calls
- All calls to a particular number are always recorded
- Record call only if a particular DTMF string is entered

See also *7.5.7 The "Trunk Recording" Tab*, Page 94.

13.1.2 THE "PROFILE" TAB



The selected Profile specifies the type of connection this Trunk is using.

Profile: Standard MSN (Customized)

Number Formatting

Conversion for outbound Calls:

Calling Party Number: Subscriber

Called Party Number: National

Conversion for inbound Calls if number type is Unknown:

Calling Party Number: Subscriber

Called Party Number: National

Master PBX Public Line Access Prefix:

Special Number Replacement:

On this tab the profile for all Trunks of this group is specified, along with the conversion of numbers for outgoing calls and the display of the numbers of incoming calls.

You can input the public line access of a superior telecommunication system, and configure automatic number replacement.

This tab appears for all trunk groups.

Profile

A trunk group profile specifies how the trunk interprets and handles the call numbers. Depending on the trunk type, a number of predefined profiles are available. For each of these profiles, the number format is specified. For SIP trunks in particular, the profile specifies the provider and the necessary SIP parameters.

For details of the available profiles, please refer to the respective sections:

- *15.3.1 Profile of an ISDN trunk group*, Page 266
- *16.3.1 Profile of a SIP Trunk Group*, Page 281
- *19.4 Creating a SIP Gateway Trunk*, Page 322

For the trunk types SwyxLink and ENUM, only one profile is available at the moment in each case.

Number formats predefined by the profile can be changed by choosing other parameters for the number formats in the field below. After making the change, close the tab with "OK", and a new profile is then created with the name of the provider (e.g. "Freenet (customized)").

The profile that was originally supplied remains available for selection in the selection list.

> If you have created a changed profile and switch back to the predefined original profile, the customized profile will be deleted. It is not possible to create multiple customized profiles based on one predefined profile.

Number Format of a Trunk Group

Procedures for converting outgoing numbers and interpreting incoming numbers are defined within a trunk group. In the properties of a trunk group, the selected protocol contains a detailed definition of which numbers (outgoing/incoming and calling/called number) are converted into which formats. This mapping of formats can be modified subsequently by administrators.

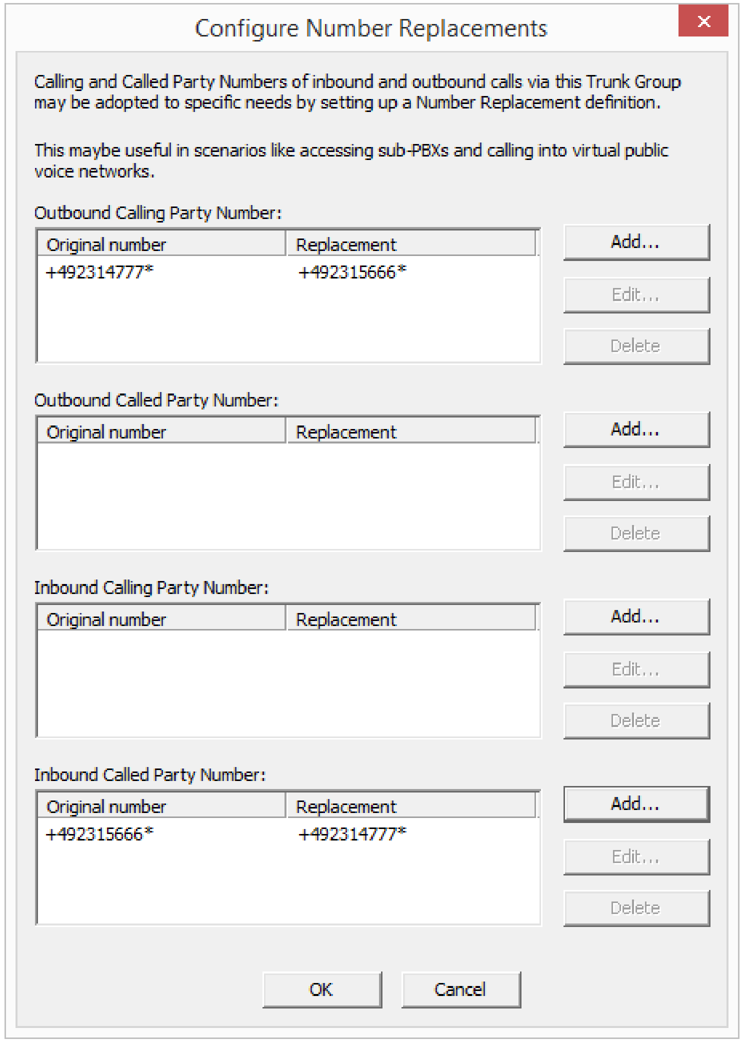
You will find the available number format in *10.6.1 NumberFormatProfiles.config*, Page 155

Public line access of the superior PBX

If SwyxWare is configured as a sub-telecommunication system, please specify here the public line access of the superior telecommunication system.

Special number replacement:

You can specify a special automatic number replacement here for individual call numbers.



Configure Number Replacements

Calling and Called Party Numbers of inbound and outbound calls via this Trunk Group may be adopted to specific needs by setting up a Number Replacement definition.

This maybe useful in scenarios like accessing sub-PBXs and calling into virtual public voice networks.

Outbound Calling Party Number:

Original number	Replacement
+492314777*	+492315666*

Outbound Called Party Number:

Original number	Replacement

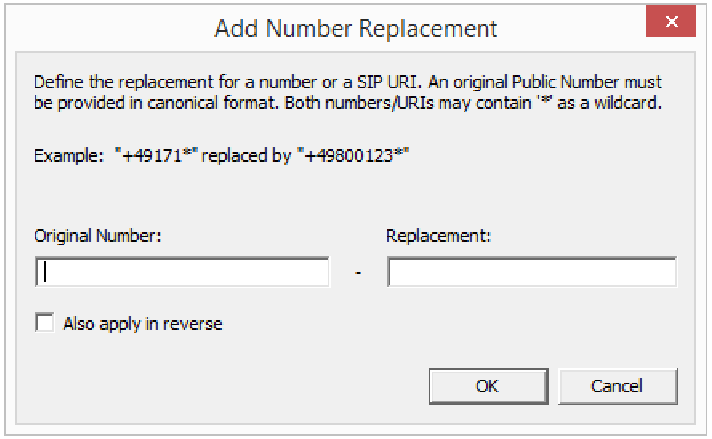
Inbound Calling Party Number:

Original number	Replacement

Inbound Called Party Number:

Original number	Replacement
+492315666*	+492314777*

If you want to add or edit an automatic number replacement, a further window opens.



Add Number Replacement

Define the replacement for a number or a SIP URI. An original Public Number must be provided in canonical format. Both numbers/URIs may contain '*' as a wildcard.

Example: "+49171*" replaced by "+49800123*"

Original Number: - Replacement:

□ Also apply in reverse

You can specify the replacement of a number or SIP URI here. You can also use placeholders in the definition (*10.5 Placeholder*, Page 152).

Please note that numbers which go into the public network must be specified in canonical format.

If you activate the checkbox "Apply in reverse", this replacement applies in both directions, i.e. the incoming caller number is replaced and conversely the outgoing destination number, as well as the incoming destination number and the outgoing caller number.

Replacement configured for	"Apply in reverse" affects
Outgoing caller number	Incoming destination number
Outgoing destination number	Incoming caller number
Incoming caller number	Outgoing destination number
Incoming destination number	Outgoing caller number

Example 1:

In the table, the replacement of the destination number is configured for outgoing calls:

Original +44 is replaced by 0044**

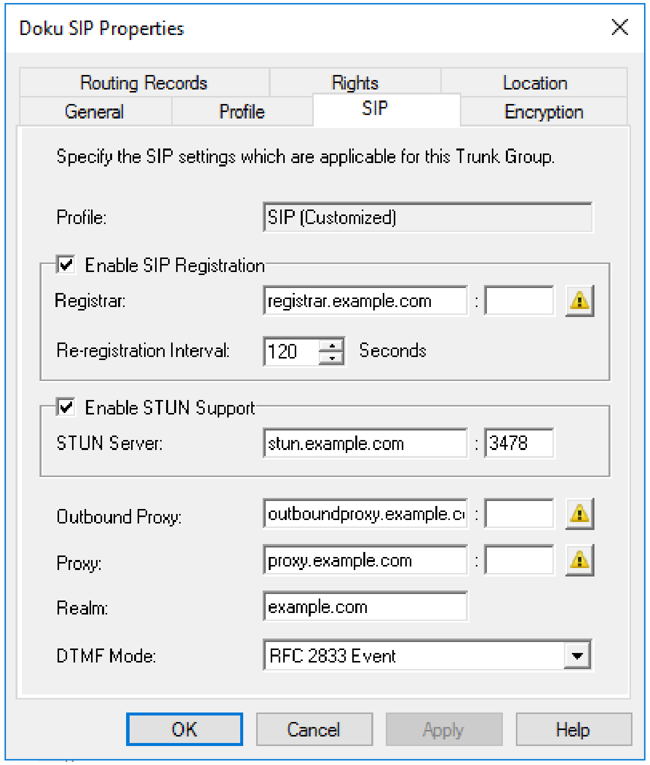
If "Apply in reverse" is activated, then for incoming calls the 0044 in the caller number is replaced by +44.

Example 2:

The number '+442012345' is replaced by '12345'

If using a profile that has the setting "national" for the destination number, then without this entry 023112345 would be dialed. However, certain special phone codes can be reached only with 12345, and not with a prefixed local area code.

13.1.3 THE "SIP" TAB OF THE SIP TRUNK GROUP



Doku SIP Properties

Specify the SIP settings which are applicable for this Trunk Group.

Profile: SIP (Customized)

☑ Enable SIP Registration

Registrar: registrar.example.com :

Re-registration Interval: 120 Seconds

☑ Enable STUN Support

STUN Server: stun.example.com : 3478

Outbound Proxy: outboundproxy.example.c :

Proxy: proxy.example.com :

Realm: example.com

DTMF Mode: RFC 2833 Event

The SIP settings for this trunk group are specified on this tab, dependent on the trunk type. You can allow both SIP registration and STUN support here, and set the corresponding parameters. The default setting occurs in the profile selected on the "Profile" tab.

The profile that was selected on the "Profile" tab is displayed here for information. If you change settings of a predefined profile, the profile will be saved as a customized profile.

Activate SIP registration

Activate the checkbox to permit SIP registration.

Define the registrar. REGISTER messages are sent to this address. If no value is entered here, the value configured under proxy will be applied.

The "Re-Registration Interval" defines how often the registration must be updated. A small value will allow you to quickly recognize the loss of the SIP connection to the provider. A high value results in lower network burden in standby.

In the "Port" field you define the port on which the configured registrar receives the registration request.

The port must match the selected transport protocol. Leave the filed empty if you did not receive information on the port by your provider. The port is determined via DNS query.

Activate STUN Support

STUN is a network protocol that recognizes the existence and type of firewalls and NAT routers and takes this information into consideration. It enables the uncomplicated use of devices (e.g. SIP telephones) and programs in networks that should receive information from the Internet.

STUN helps to identify the current public IP address of the line. This is necessary in order for the opposite terminal to correctly address and return your call data.

For more information on the STUN protocol, please see the corresponding RFC standard (RFC 3489).

Activate the checkbox to permit STUN support. See also *STUN*, Page 279.

A STUN server can be used to identify the IP address of the line. Supports your provider STUN, so please enter the name or the IP address of the STUN server of your provider and the appropriate port. If you would like to use STUN, although you have not received any STUN server information from the provider, you can use the free STUN server "stunserver.org" with port "3478"..

Configure the general SIP parameters in the lower section:

Outbound Proxy

Some providers have an outbound proxy before the SIP proxy. Configure this parameter according to the settings of your provider.

Proxy

Defines the SIP proxy for outgoing calls.

The SIP proxy server takes over the connection setup to the appropriate subscriber, first checking which SIP registrar the relevant subscriber is logged in with. From this it requests and receives the current IP address of the subscriber, and can thus deliver the call to this address.

Realm

Defines the SIP realm of the provider.

An SIP URI (userId@realm) is derived from the user ID (userId), the configuration of the SIP account, and the realm of the provider (realm). If this field is left blank, the value registrar or proxy will be used.

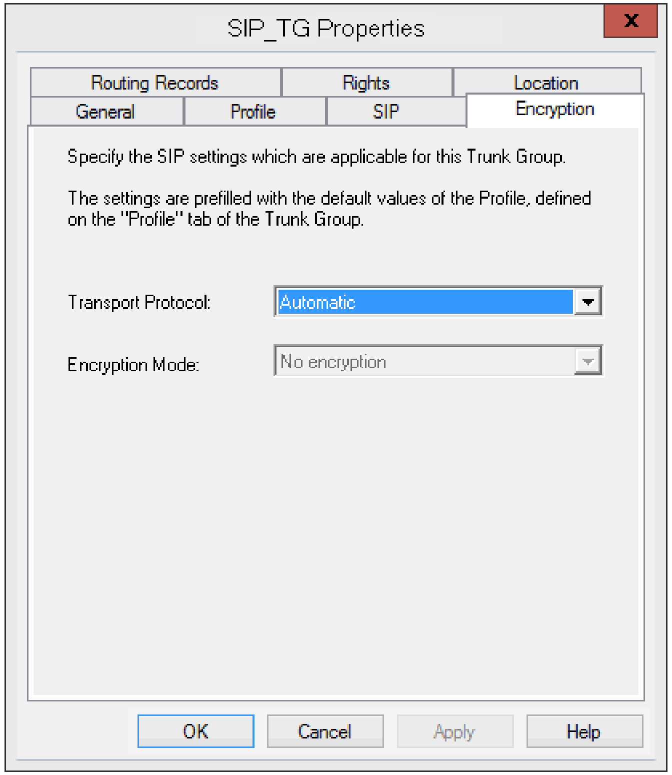
DTMF method

This mode defines how the provider proceed with the keyboard input of a user during a call (DTMF signaling).

You can choose from a variety of options:

- None. DTMF signalization is deactivated
- RFC2833_Event: RFC2833_Event: DTMF signalization, based on the event mechanism described in RFC2833, will be used.
- Info Method DTMF Relay DTMF signalling as recommended by Cisco (applicationtype DtmfRelay) will be used.

13.1.4 THE "ENCRYPTION" TAB OF THE SIP TRUNK GROUP



SIP_TG Properties

Specify the SIP settings which are applicable for this Trunk Group.

The settings are prefilled with the default values of the Profile, defined on the "Profile" tab of the Trunk Group.

Transport Protocol: Automatic

Encryption Mode: No encryption

On this tab you can select transport protocol and encryption mode for the Trunk Group.

Transport protocol

Make sure that the selected transport protocol is supported by your provider.

From the dropdown list select the transport protocol that you want to assign to the Trunk Group.

- Automatic (Standard)
  The transport protocol is determined automatically by DNS lookup.
- UDP
  This transport protocol is supported by most SIP providers. It requires the lowest bandwidth, however, it carries a higher risk of data loss.
- TCP
  This transport protocol is known to be reliable, however, it requires higher bandwidths.
- TLS
  This transport protocol has TCP characteristics and supports encryption. When selecting this protocol SIP packet are transmitted encrypted.

Encryption mode

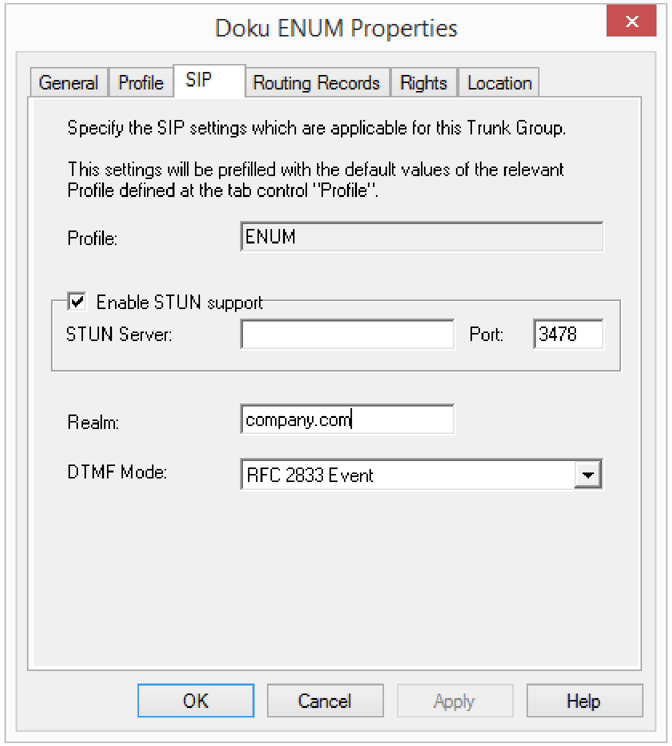
This option will only be activated if you have selected the TLS transport protocol. You can define if voice data will also be encrypted when using the secure TLS connection.

- no encryption
  The voice data is not encrypted.
- Encryption mandatory
  Voice data is encrypted between SIP provider and SwyxLinkManager.

> When "Encryption mandatory" is selected, voice data encryption is obligatory. This means that either encryption always occurs or the call is aborted with the reason "Incompatible encryption settings".

> A SIP Trunk Group's encryption mode does not affect the SRTP encryption settings for SwyxServer, see*21 Encryption*, Page 342

13.1.5 TAB "SIP" OF THE ENUM TRUNK GROUP


Doku ENUM Properties

Specify the SIP settings which are applicable for this Trunk Group.

This settings will be prefilled with the default values of the relevant Profile defined at the tab control "Profile".

Profile: ENUM

☑ Enable STUN support

STUN Server: Port: 3478

Realm: company.com

DTMF Mode: RFC 2833 Event

Only one profile is currently available for the ENUM Trunk.

Activate STUN Support

Activate the checkbox to permit STUN support. See *STUN*, Page 279.

A STUN server can be used to identify the IP address of the line. Supports your provider STUN, so please enter the name or the IP address of the STUN server of your provider and the appropriate port. If you would like to use STUN, although you have not received any STUN server information from the provider, you can use the free STUN server "stunserver.org" with port "3478"..

Realm

Defines the SIP realm of the provider.

An SIP URI (userId@realm) is derived from the user ID (userId), the configuration of the SIP account, and the realm of the provider (realm). If this field is left blank, the value registrar or proxy will be used.

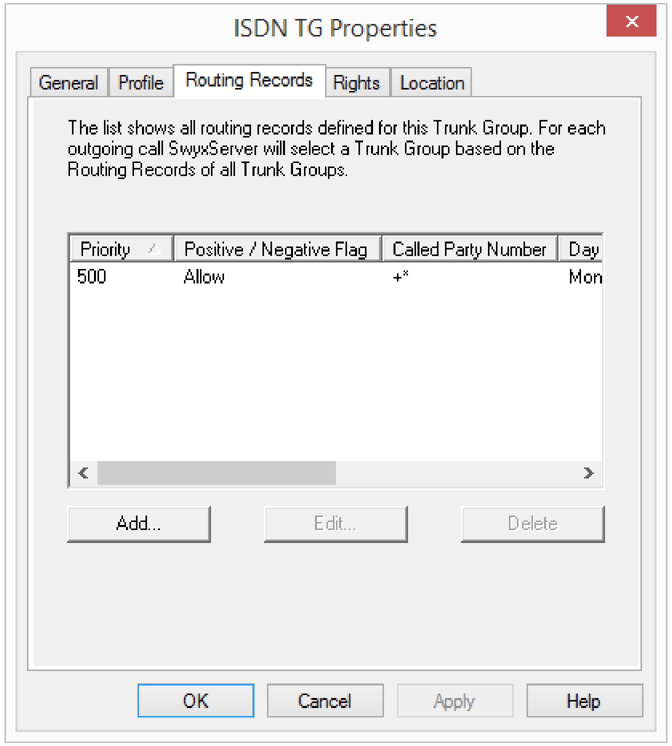
DTMF method

This mode defines how the provider proceed with the keyboard input of a user during a call (DTMF signaling).

You can choose from a variety of options:

- None. DTMF signalization is deactivated
- RFC2833_Event: RFC2833_Event: DTMF signalization, based on the event mechanism described in RFC2833, will be used.
- Info Method DTMF Relay DTMF signalling as recommended by Cisco (applicationtype DtmfRelay) will be used

13.1.6 TAB "ROUTING RECORDS"



The list shows all routing records defined for this Trunk Group. For each outgoing call SwyxServer will select a Trunk Group based on the Routing Records of all Trunk Groups.

Priority	Positive / Negative Flag	Called Party Number	Day
500	Allow	+*	Mon

The forwarding options for this Trunk Group are defined on this tab.

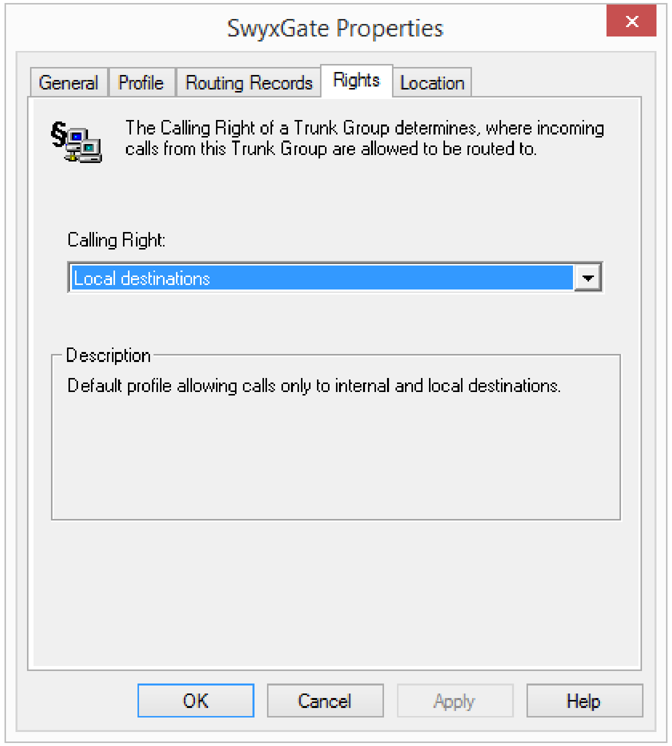
This tab appears for all trunk groups.

All routes defined for this trunk group are listed here. You can generate new entries here, or edit or delete existing ones.

You will find an overview of all forwarding entries for this server in the administration in the "Forwarding table" directory.

See *14 Routing*, Page 239.

13.1.7 THE "RIGHTS" TAB



The Calling Right of a Trunk Group determines, where incoming calls from this Trunk Group are allowed to be routed to.

Calling Right: Local destinations

Description
Default profile allowing calls only to internal and local destinations.

Specify what rights a call has when coming in via this trunk. By doing so you specify whether it may use other trunk groups (and which ones) to leave this SwyxWare installation, if its destination is not a user of this SwyxServer.

The permission 'inherited' from the trunk group is used if the received call is not addressed to a user on this SwyxServer. If a user on this SwyxServer was addressed and the call is forwarded by his call routing, then the call 'inherits' the permissions of the called user.

This tab appears for all trunk groups.

All available profiles are offered for selection; see the "Description" field for details. Select a rights profile from the list here. In the default setting, the Calling Right profile "Internal Calls" is selected.

STOP

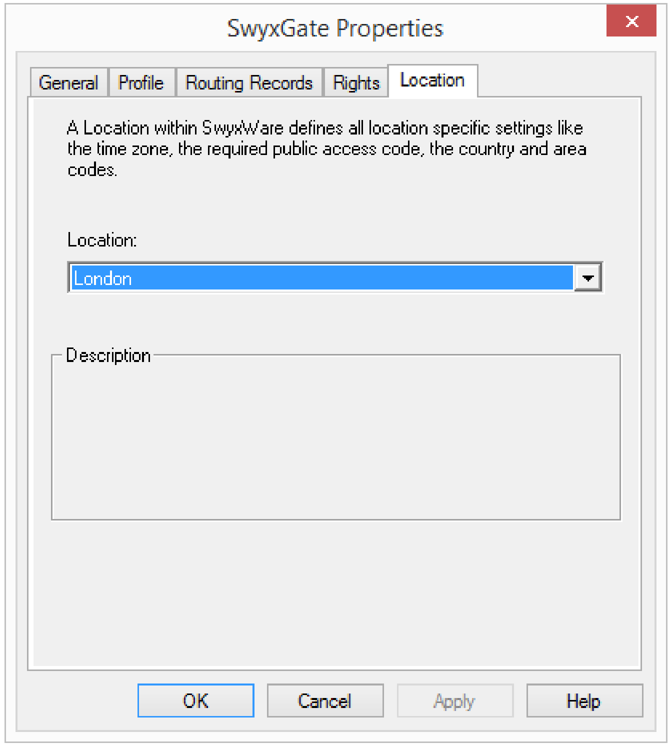
Call permissions of a trunk group only apply to incoming calls!
The advanced call permissions (more than "internal calls") could, depending on the configured forwarding entries, be misused by external callers. Protect your SwyxServer by only allowing external forwarding of incoming calls in exceptional cases.

After installation, you have a variety of available options:

- International connections
- European destinations
- National connections
- Local calls
- Internal calls only
- Deny all calls

To define right profiles, see *9 Profiles*, Page 128.

13.1.8 THE "LOCATION" TAB



A Location within SwyxWare defines all location specific settings like the time zone, the required public access code, the country and area codes.

Location: London

Description

By specifying the location, you specify both the corresponding prefixes and also the time zone relating to this location.

This tab appears for all trunk groups.

You can select a location here from the previously defined locations. In the default setting, only the location "DefaultLocation" is available.

If you would like to specify or change a location, please refer to *8 Locations*, Page 122.

13.2 ACTIVATING AND DEACTIVATING A TRUNK

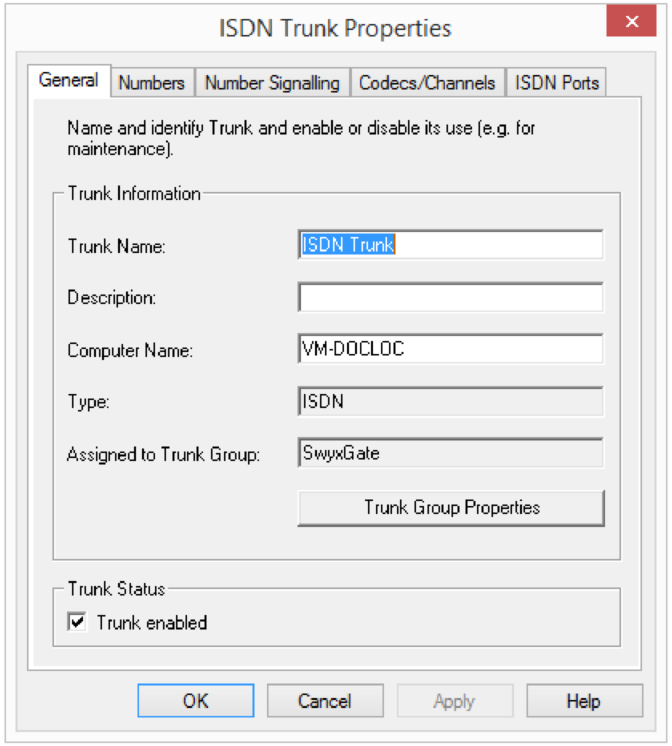
In order to be able to carry out maintenance work on a line, for example, it may be necessary to temporarily deactivate one or more trunks within SwyxWare.

It won't be written in the change log, if a trunk was activated or deactivated.

This is how you deactivate / activate a trunk

1 In the SwyxWare Administration, open the directory "Trunks".
In the list of trunks, highlight the trunk that is to be deactivated/ activated.

2 In the context menu, select "Properties".
In each case, the "Properties of..." window will appear.



Name and identify Trunk and enable or disable its use (e.g. for maintenance).

Trunk Information

Trunk Name: ISDN Trunk

Description:

Computer Name: VM-DOCLOC

Type: ISDN

Assigned to Trunk Group: SwyxGate

Trunk Status

☑ Trunk enabled

3 Deactivate the checkbox "Trunk enabled" on the "General" tab to block this trunk for further incoming or outgoing calls.

4 Click on "OK".

5 Select "Active calls" in the left side of the SwyxWare Administration window, and check whether telephone calls are still being made via this trunk. Under "Origination Device" or "Destination Device" this trunk is listed as long as it is being used for an existing connection.

6 If there are no active connections via the trunk, you can stop the associated SwyxGate service via the Service Manager.
To reactivate the trunk, use the Service Manager to start the service and then activate the trunk with the checkbox.

If you have deactivated a service (e.g. SwyxGate) on another computer, you must then start the service locally on the remote computer in the Service Manager.

14 ROUTING

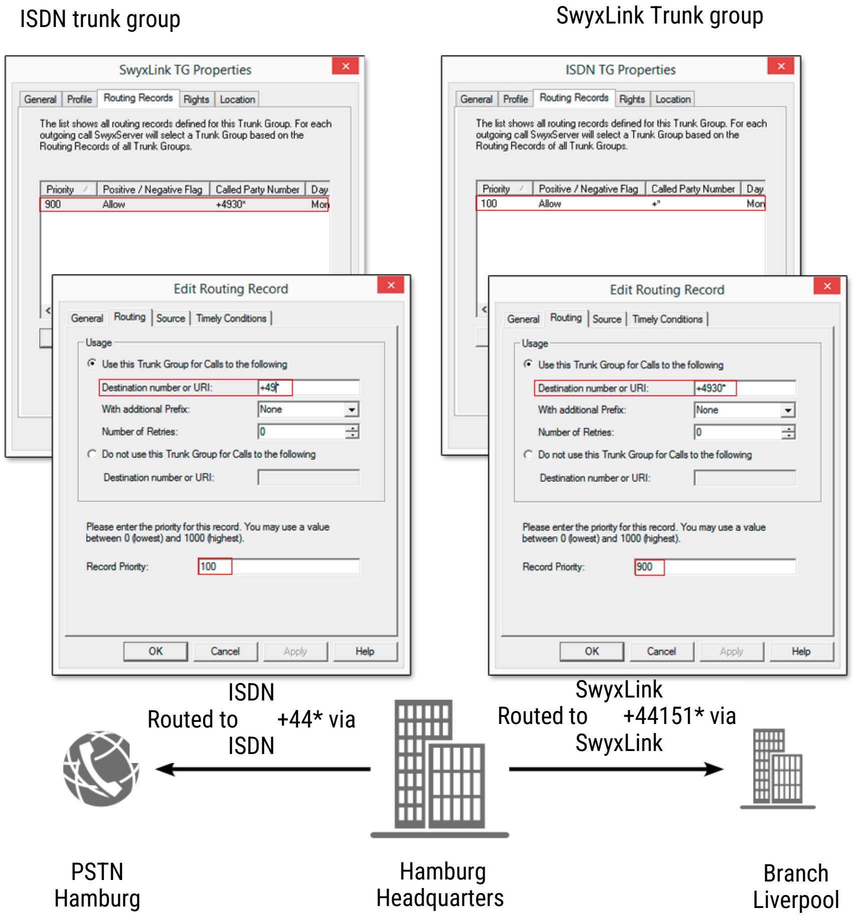
Where do calls go if they can't be assigned within a SwyxServer?

Outgoing calls can be forwarded (dependent on the dialed number, time conditions and/or the caller himself) via various paths, e.g. SIP provider or ISDN. These routes can be specified individually with a different priority (0-1000) for each trunk group.

Example:

In Manchester you have an ISDN trunk into the public phone network and a SwyxLink connection to a branch in Liverpool. All calls to Liverpool (+44151) should go via the SwyxLink.*

You set up a route for the trunk group in which SwyxLink is a member (Public number: +44151), setting a high priority, e.g. 900. Set up a route for the ISDN trunk group (e. g. for England- destination number/URI: +44*), but with a low priority (e. g. 100). If the SwyxLink line is busy, i.e. all configured channels are in use, interrupted or deactivated, the calls will be established via the low priority connection (here: ISDN).*



SwyxLink TG Properties

The list shows all routing records defined for this Trunk Group. For each outgoing call SwyxServer will select a Trunk Group based on the Routing Records of all Trunk Groups.

Priority	Positive / Negative Flag	Called Party Number	Day
900	Allow	+4930*	Mon

Edit Routing Record

Usage

● Use this Trunk Group for Calls to the following

Destination number or URI: +49*

With additional Prefix: None

Number of Retries: 0

○ Do not use this Trunk Group for Calls to the following

Destination number or URI:

Please enter the priority for this record. You may use a value between 0 (lowest) and 1000 (highest).

Record Priority: 100

ISDN TG Properties

The list shows all routing records defined for this Trunk Group. For each outgoing call SwyxServer will select a Trunk Group based on the Routing Records of all Trunk Groups.

Priority	Positive / Negative Flag	Called Party Number	Day
100	Allow	+*	Mon

Edit Routing Record

Usage

● Use this Trunk Group for Calls to the following

Destination number or URI: +4930*

With additional Prefix: None

Number of Retries: 0

○ Do not use this Trunk Group for Calls to the following

Destination number or URI:

Please enter the priority for this record. You may use a value between 0 (lowest) and 1000 (highest).

Record Priority: 900

If you later set up an economical SIP connection, you can specify a route for this for all of the United Kingdom (+44*) with a higher priority (e. g. 800). The connection attempts are made in priority order, i. e. in this case, first the SwyxLink connection, then the SIP connection and then the connection via ISDN is selected.

You can find an overview of the available routes in Administration in the directory "Forwarding table".

Routing configuration

Repeated connection attempts with least cost routing

Extended Least Cost Routing

14.1 ROUTING CONFIGURATION

A routing is always assigned to a specific trunk group, so that it is effectively a property of this trunk group. Rules are created based on the dialed destination numbers, and placeholders can be used. The routing can be formulated positively (Use this Trunk Group for Calls to the following) or negatively (Do not use this Trunk Group for Calls to the following). The routing records can be prioritized. A sequence order can thus be defined within the routings, e.g. "Try first on trunk group A, then on trunk group B". The caller number of the calling SwyxWare user, the group membership or the user's location can be taken into account in the decision on which trunk group is selected.

For SwyxLink trunks with configured intersite settings a routing record is created automatically. This entry is not editable.

If the trunk group consists of several trunks, the trunk with this number is selected. (e.g. ***Public numbers of this trunk***, Page 270). If no trunk matching the caller number is found within the selected trunk group, the trunk signaling the most information about the caller is selected. The number signaled externally arises according to the valid setting on this trunk in the field "Outgoing calls if Calling Party Number / URI is not assigned".

Example:

You have two ISDN connections e.g. each with five MSNs. For each of these connections you set up a trunk group:

- User A has an internal number, for which there is a call number mapping to trunk group 1,

- User B has an internal number, for which there is a call number mapping to trunk group 2.

- There are routing records for both trunk groups with the same priority and the same destination number range.

If one of these users calls an external number, then a trunk group is selected using the dialed number and the priority. If these criteria do not lead to a preferred trunk group, the trunk group is randomly selected, i.e. also trunk group 1 can be selected for user 2. If e.g. Hide Number is configured on the trunk groups for unassigned caller numbers, then - without the user intending this - his number is displayed on one call and not on another. To prevent this, when the trunks are similar you can manage both in one trunk group, regardless of the fact that two different ISDN connections are represented.

Routing Records and selection prefix for trunk groups

If a user defines which trunk group should be used for the next call by using the assigned selection prefix, no further routing records are applied.

See ***13.1 Configure trunk groups***, Page 227.

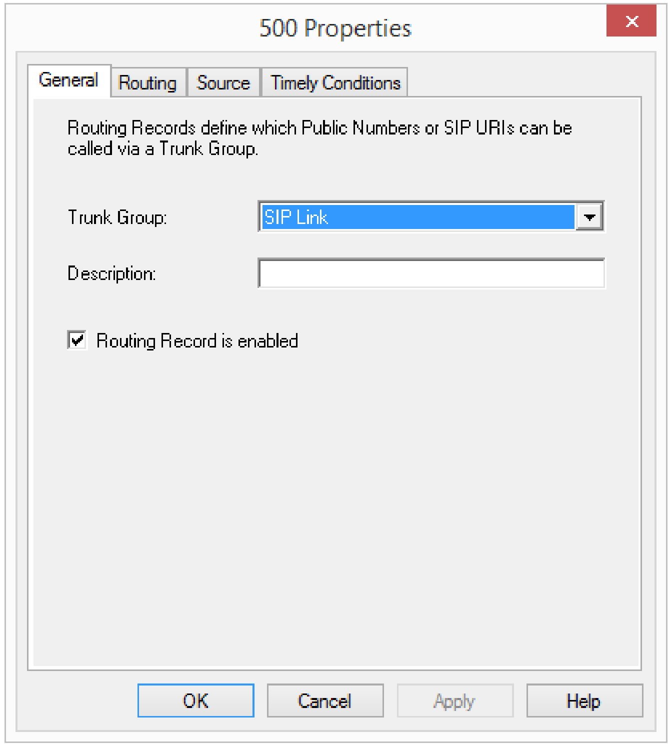
This is how you define a route

1 Open the SwyxWare Administration and choose the SwyxServer.

2 On the left side of the SwyxWare Administration window, click with the right mouse button on "Forwarding Table" and select the entry "Add Routing Record..." in the context menu.
The window labeled "Properties of ...." will open.

3 Specify the relevant parameters on the tabs, and end your inputs with "OK".
A new entry is created in the forwarding table; it applies to the specified trunk group.

The "General" Tab



Routing Records define which Public Numbers or SIP URIs can be called via a Trunk Group.

Trunk Group: SIP Link

Description:

☑ Routing Record is enabled

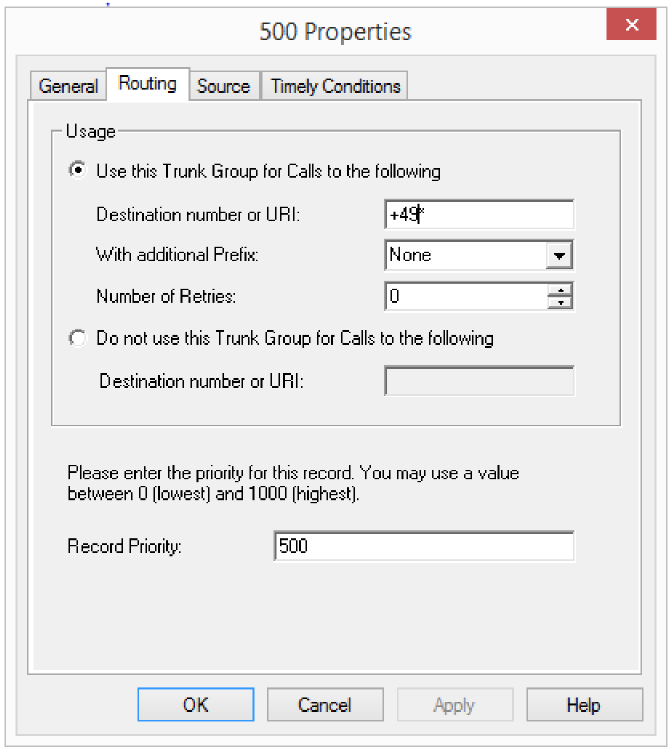
Specify on this tab the trunk group to which this record type should apply. You can also insert a short description here.

Trunk Group

Each entry in the forwarding table applies to exactly one trunk group. When a newly created entry is closed with "OK", it is applied immediately for the trunk group for which it was configured. You can only specify a route for an existing trunk group; select an available trunk group from the selection list.

If the record type should not be active at the time, deactivate the checkbox "Routing Record is enabled".

The "Routing" Tab



Usage

● Use this Trunk Group for Calls to the following

Destination number or URI: +49*

With additional Prefix: None

Number of Retries: 0

○ Do not use this Trunk Group for Calls to the following

Destination number or URI:

Please enter the priority for this record. You may use a value between 0 (lowest) and 1000 (highest).

Record Priority: 500

Specify on this tab the forwarding criteria to be used in relation to the number or URI.

Usage

Activate "Use this Trunk Group for Calls to the following" if you want to forward calls over these trunks which meet the following conditions.

Give the public numbers or URI that should go over this trunk. You can use placeholders here (*10.5 Placeholder*, Page 152).

In the field "With additional Prefix", you have several options:

- None
  In this case, no further prefix (Call-by-Call provider selection) is added to the destination number.

- <Number>
  Enter directly into the field a numerical sequence, which is then prefixed to every destination number that is routed via this trunk group, e.g. "01013".

Specify how often a connection attempt should be repeated (standard: 0). If LCR is not used, but instead the call by call prefix of an economical but heavily overloaded provider is dialed directly, these repeats can be useful in order to try this least expensive provider a number of times.

Activate "Do not use this Trunk Group for Calls to the following" if you don't want to send calls with certain destinations via this trunk group.

For each routing record, you can allow or deny only one type of condition.

Example of the use of placeholders:

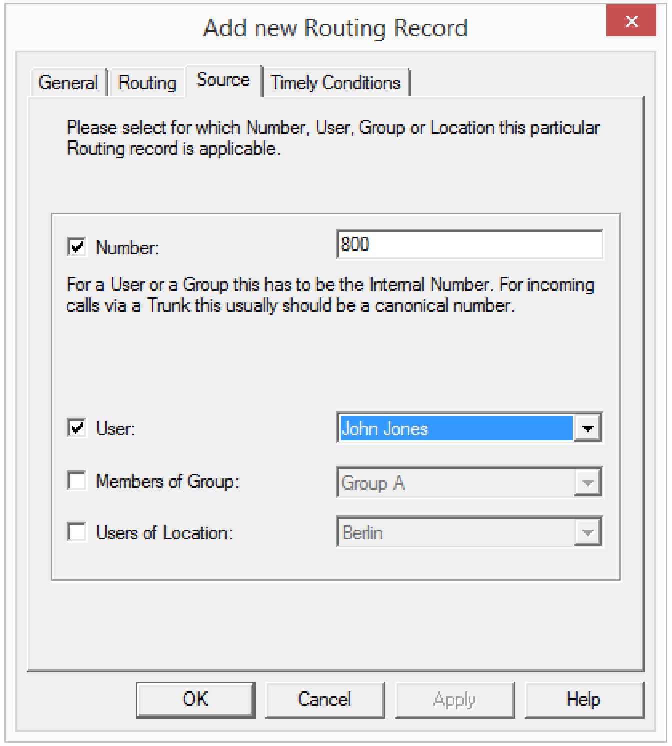
If you want to allow only external numbers for a trunk group, then you must enter the following:

- Under "Use this Trunk Group for Calls to the following", in the field "Destination number or URI", enter "+*". All calls going to an external number (canonical format, e.g. +4420 5666777) are then allowed
- Under "Do not use this Trunk Group for Calls to the following", in the field "Destination number or URI", enter "*". All calls that are not explicitly allowed above are then disallowed. As a result of this setting, calls intended for internal subscribers (not in canonical format) are not routed via this trunk group.

Record Priority

Specify the priority with which this forwarding is applied to a call. You can decide a priority between 0 (low) and 1000 (high).

The "Source" Tab


Add new Routing Record

Please select for which Number, User, Group or Location this particular Routing record is applicable.

☑ Number: 800

For a User or a Group this has to be the Internal Number. For incoming calls via a Trunk this usually should be a canonical number.

☑ User: John Jones

☐ Members of Group: Group A

☐ Users of Location: Berlin

You can say on this tab whether the origin of the call is used for making a decision. If nothing is configured, the routing rule applies to all calls.

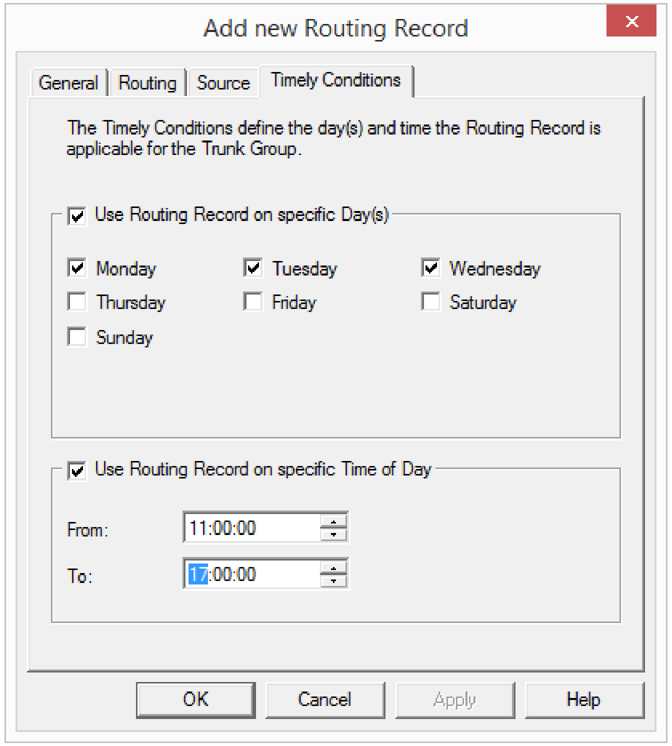
Phone number

You can enter an internal number or URI here. The routing rule then applies to all calls which signal this number or URI (internal SwyxWare user or group). If calls coming over this trunk are to be forwarded according to this rule, enter the number or URI here in canonical format. The number is matched from the beginning onward. Enter here e.g.: "21", the routing rule applies to all callers, whose number starts with a "21", see *10.5 Placeholder*, Page 152.

User, Members of Group and Users of Location

You can use further selection criteria here. This rule can be set for a particular SwyxWare user or for the members of a group. Belonging to a location can also be a selection criterion. You can also combine the two criteria "Members of Group" and "Users of Location" (e.g. All users of the "Support" group at the "Munich" location). The criterion "Number" can equally be combined with the other criteria (User, Members of Group and Users of Location). In combinations, both criteria must be satisfied (logical AND).

The "Timely Conditions" Tab



The Timely Conditions define the day(s) and time the Routing Record is applicable for the Trunk Group.

☑ Use Routing Record on specific Day(s)

☑ Monday ☑ Tuesday ☑ Wednesday
□ Thursday □ Friday □ Saturday
□ Sunday

☑ Use Routing Record on specific Time of Day

From: 11:00:00

To: 17:00:00

On this tab you specify time-related conditions (weekdays, time of day) for a routing. You can give both weekdays and also times on the defined weekdays.

Use Routing Record on specific Day(s)

If you want to set up the route dependent on days of the week, activate the checkbox "Use Routing Record on specific Day(s)". Then activate the checkboxes of the weekdays for which this route should apply.

Use Routing Record on specific Time of Day

If you want to set up the route dependent on a time of day, activate the checkbox "Use Routing Record on specific Time of Day". Then specify a period for which this route should be active.

14.2 REPEATED CONNECTION ATTEMPTS WITH LEAST COST ROUTING

SwyxWare is able to repeat connection attempts over different trunks. For calls to external numbers, the connection attempts are repeated. The mechanism for repeats is as follows:

The trunk group that has the routing record with the highest priority for this call is determined in the first attempt, and from this group a trunk is selected which matches the caller's public number. If the routing record gives a specific call by call prefix, this is prefixed to the dialed number.

If no connection is established, the next routing record by priority is subsequently selected. Depending on the configuration, this can also be the same trunk group again.

Example:

	Trunk Group	Priority	Number	Prefix	Repetitions
1	TG1	500	+*	01013	2
2	TG2	600	+*	-	0
3	TG2	400	+*	01033	0
4	TG3	300	+*	-	0

	Trunk Group	Priority	Number	Prefix	Repetitions
5	TG4	200	+*	-	0

In this example, an attempt is first made to dial a call via the trunk group TG2 (priority 600), and this is followed by three attempts (one + two repeats) to establish a connection via TG1 (priority 500) with the help of the LCR module. After this, one further connection attempt each (repeat = 0) is made with, in the order of priority, TG2 (with fixed prefix 01033), then TG3 and then TG4.

14.3 EXTENDED LEAST COST ROUTING

Extended Least Cost Routing enables a remote access to the public network (SwyxGate).

Example:

When creating the connection between a SwyxWare user at the London site to a subscriber in the vicinity of the Dortmund site, the SwyxServer at the London site can determine that the dialed subscriber can be reached via the Trunk based on the parameters of the Trunk assigned to Dortmund. This means that the telephone connection from London to Dortmund is e. g. first made via the WAN connection and then via the ISDN Trunk in Dortmund to the external subscriber in ISDN.

A common wish is that the calls from London can signal a calling party number from London. On the "Numbers" tab of the corresponding trunk, you can define which number should be signaled e.g. in ISDN to the called party. The ISDN trunk in Dortmund then must be able to use foreign numbers (i. e. a London number) for outgoing calls. The ISDN function "CLIP no screening" is used for this: it has to be requested separately from your provider.

The Least Cost Routing of the SwyxServer in Dortmund and the corresponding provider is naturally used once again for the connection via the SwyxGate in Dortmund to the external subscriber.

15 ISDN CONNECTIONS

Installation of ISDN cards for the connection to the public telephone network or an old telephone system, and setting up of the corresponding ISDN trunks and trunk groups

This function is not available for SwyxON.

ISDN trunks are all ISDN lines, - whether for the S0 Basic Rate Interface Connection or the S2m Primary Rate Interface - with which a Swyx gateway (SwyxGate) is connected via ISDN cards to the public telephone network or a superior or subordinate telecommunication system.

Please note that SwyxWare only works with the ISDN cards of the SX2 family. For information on updating the relevant card drivers, please refer to *5.6.3 Updating the ISDN Card Drivers*, Page 66.

15.1 BASICS FOR THE ISDN CONNECTION

Before an ISDN trunk is set up in the SwyxWare Administration, the ISDN card must be installed.

There are various connection types, which differ according to the provision of the service provider (*PSTN Access*, Page 245), as well as different operating modes on the SwyxWare itself (*Connection Types for the ISDN Lines*, Page 245).

Connection Types for the ISDN Lines

The lines of an ISDN card can be used in different ways.

Operation Directly with the Public ISDN

In this configuration, the ISDN card is operated directly with an ISDN connection to the public telephone network (PSTN).

Operation with an Existing Telecommunication System as a Sub-telecommunication System

In this situation, a telecommunication system exists, which has a connection to the PSTN, and the ISDN card is connected to this telecommunication system. SwyxWare is a sub-telecommunication system in this case and SwyxWare does not have direct access to the PSTN.

See *D.2 Connection of SwyxWare as Sub-telecommunication System on a Main Telecommunication System*, Page 420.

Operation as a Main System with a Sub-telecommunication System

SwyxWare has a connected sub-telecommunication system (sub-PBX) and the line to be configured connects the main system and the sub-telecommunication system.

See *D.1.4 Connecting a Sub-telecommunication System (Sub-PBX) to SwyxWare*, Page 419.

PSTN Access

Furthermore, there is a difference between a PSTN connection, which has a line with one line number and an extension range, and one which has one line with several MSNs.

Operation with One Line Number and Extension Range

In this configuration, the ISDN card is operated with a direct dialing-in ISDN line. This connection is assigned a phone number. An extension range is defined in addition to this number (*The "Numbers" Tab*, Page 270). Each SwyxWare user can now be assigned one or more numbers from this extension range. A subscriber's complete telephone number is then e.g. composed of the phone number and the extension number.

Example:

Phone number 12345, subscriber number 777
-> Number 12345777

Operation with One Line with Several MSNs

When this configuration is used, it is possible to operate the ISDN card simultaneously with other ISDN devices using a common connection. When operating with MSNs, one or more MSNs are assigned to the ISDN trunk during configuration. SwyxWare thus only processes calls, which are directed to these MSNs. This makes it possible to assign additional numbers to other terminal equipment such as a fax machine. The MSNs listed in the configuration can be assigned in any way to the SwyxWare users. Since, to be unique, an MSN can only be assigned to exactly one user, the maximum number of users is limited by the number of available MSNs. Because the maximum number of MSNs is usually 10, this configuration is only recommended for smaller systems.

Operation with a Basic Rate Interface (BRI)

The Basic Rate Interface (BRI) provides 2 channels. Your provider can supply you with one line or with a line with several MSNs for your line connection.

The ISDN card SX2 QuadBRI can operate up to four Basic Rate Interfaces.

Operation with a Primary Multiplex Access (PRI)

A Primary Rate Interface (PRI) is always a direct dialing-in line. In contrary to a Basic Rate Interface (BRI) with 2 available channels, it supplies a maximum of 30 available channels.

A Group of Connections - Line Group

If the number of available channels is not sufficient, several lines can be combined in order to increase capacity. Both the switching and SwyxWare will treat this group of lines as a single line with a greater number of channels. A line with a free channel will be searched for automatically. This takes place in a way which is fully transparent for the user and it does not require any additional configuration.

15.2 INSTALLATION OF THE ISDN CARDS

The ISDN card can be installed in the same computer on which the SwyxServer is also installed. In the standard installation, the SwyxGate service is also installed. This service controls the ISDN lines, which appear as ISDN trunk in SwyxWare Administration.

In order to be able to install a SwyxGate on a separate computer, the SwyxServer must already be installed and operable. For the SwyxGate installation you will need

- the server name and
- the name of the domain account, which was created in preparation for the installation of the SwyxServer

Before the ISDN cards are inserted, they must be configured for operation.

A maximum of four SX2 ISDN cards can be operated simultaneously in a system. An SX2 DualPRI is counted as two cards. Mixed operation of different cards is possible, but a maximum of 76 B channels is supported in one computer.

For information about the different ISDN cards available and their possible combinations, see

FAQ: Overview to different PCI cards and slot types and ways to combine them https://service.swyx.net/hc/en-gb/articles/360000631409-Overview-to-different-PCI-cards-and-slot-types-and-ways-to-combine-them

(You may need to be logged in to view the content)

15.2.1 PREPARATION OF THE SX2 QUADBRI BEFORE INSERTION

The ISDN card (SX2 QuadBRI or SX2-express DualPRI) has to be configured with jumpers and DIP switches before can be installed into the computer.

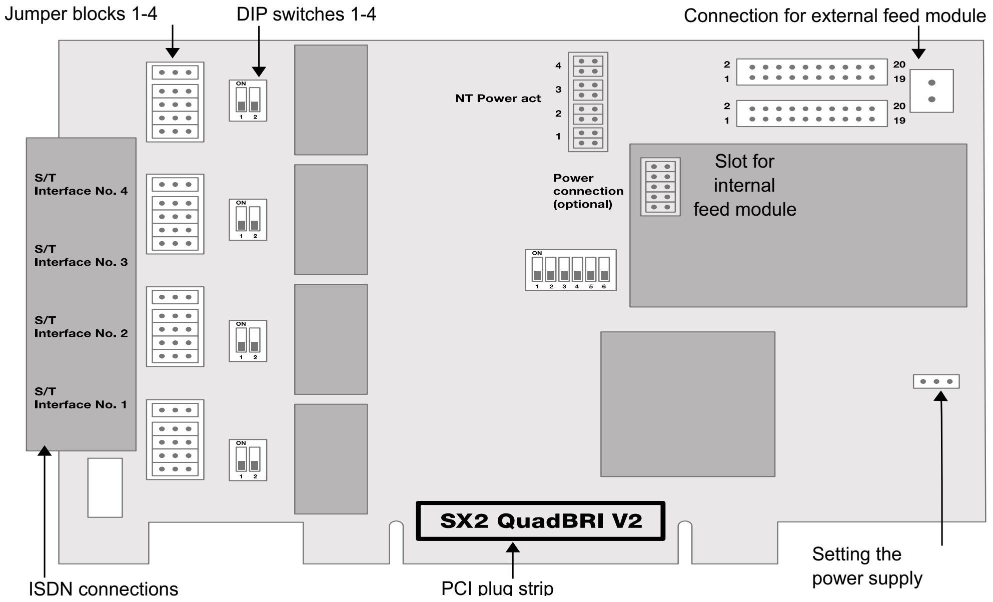
The operating mode (TE/NT) and the bus termination must be configured for each line of the SX2 QuadBRI or SX2-express DualPRI before insertion.

Requirement for further description: Requirement for further description: The SX2 QuadBRI or SX2-express DualPRI is directly in front of you, with the PCI plug strip facing down and the S0 connections to the left.

Configuration of the Operating Mode

- TE mode is set if the ISDN connection is connected to an NTBA or the SwyxWare is configured as a subsystem.
- NT mode is set if the ISDN connection is used for an external subsystem or directly connected ISDN telephones are to be used.

Each BRI bus connection is a jumper block with five assigned jumpers. If all five jumpers are inserted to the left, the connection is configured as NT. If all five jumpers are on the right-hand side of the block, the connection is configured as TE. So on one board some connections can operate in NT mode and other in TE mode at the same time.



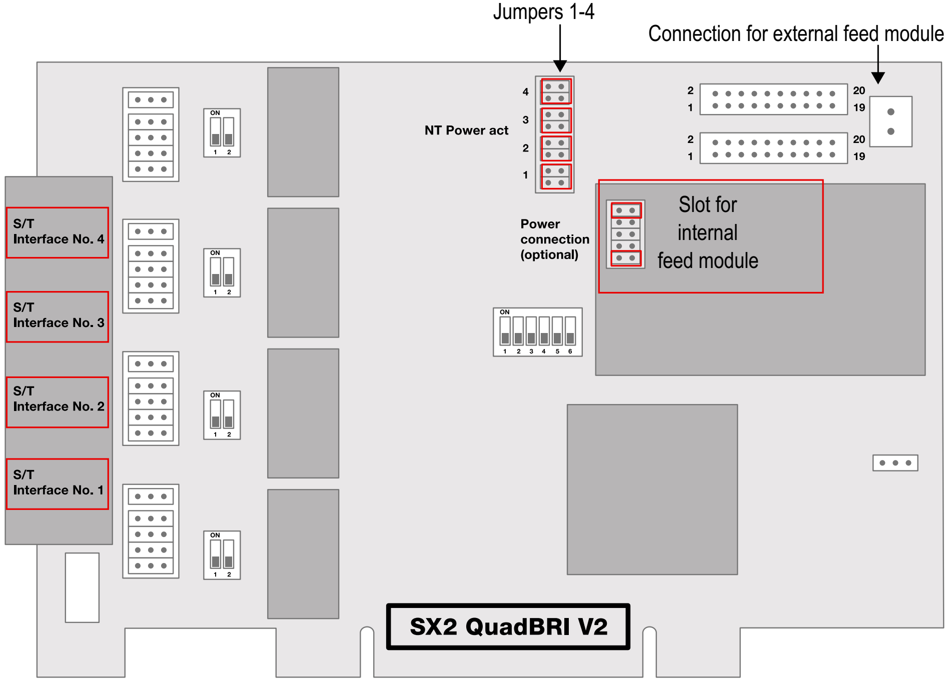
All five jumpers of one block must have the same position, e.g. all facing to the right, or all facing to the left.

After the installation of the driver software, the same operating type must be set in the configuration dialog. It is therefore not sufficient to configure the operating mode on the hardware only or in the software only.

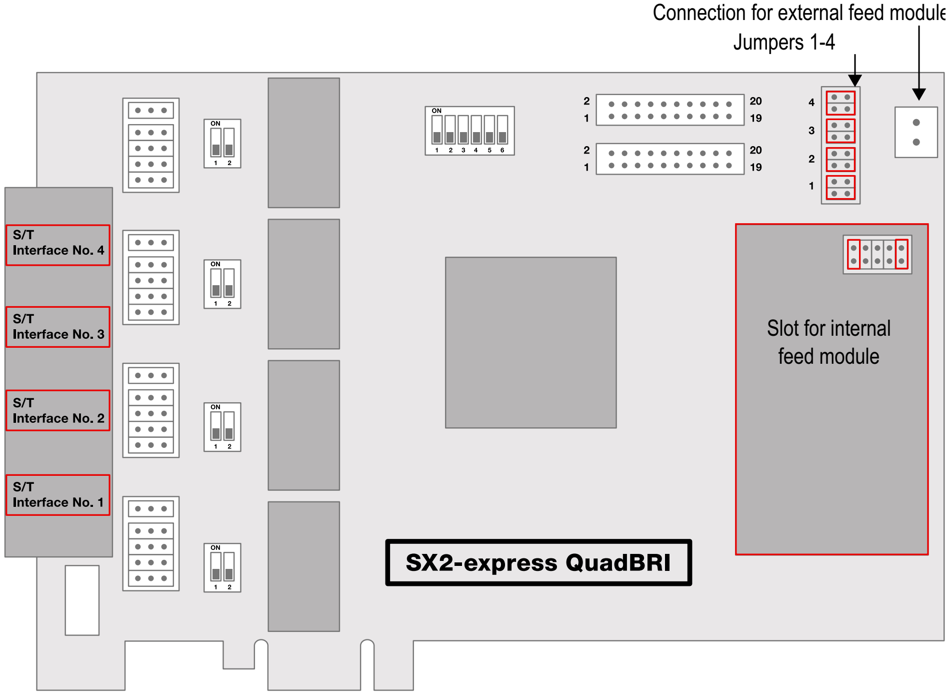
Configuration of the supply voltage in NT mode

An interface configured for NT mode can be fed with 40V from an optional external feed module. Connect this feed module to the green connector on the upper right side of the SX2 QuadBRI or SX2-express DualPRI.

Using the SX2 QuadBRI V2 with an external feed module you have to insert additionally the two outer jumpers on the plug-in slot of the internal feed module (see figure below).



For each NT interface to be fed, set two jumpers for each port to which you want to supply power. Afterwards, ISDN devices that are intended for supply from the public line can also be operated directly on the SX2 QuadBRI V2 or SX2-express DualPRI.



Please ensure that you use the feed module only for interfaces that are configured for NT mode, Otherwise the interface will be damaged.

Alternatively, you can mount an internal feed module directly on the SX2 Quad-BRI.

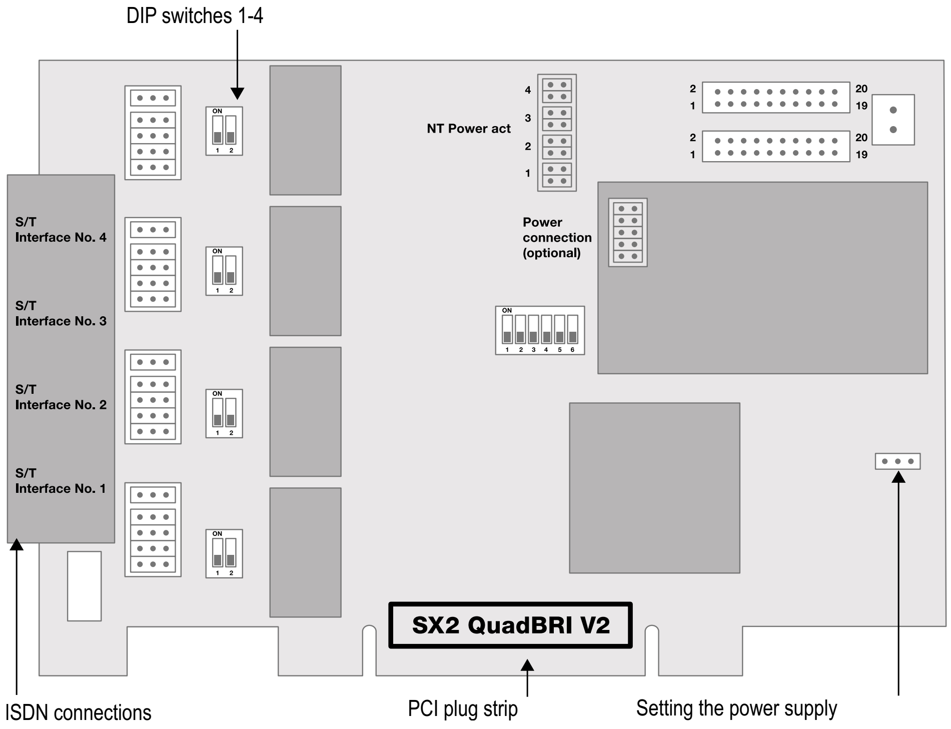
Do not use an internal and an external feed module at the same time.

Configuration of the SO bus termination

- In TE mode, the termination depends on the cabling.
- In NT mode the termination should be switched on, since the card then normally represents the end of the BRI bus.

Next to the block of jumpers for a connection, you will find a two-pole DIP switch which can be used to configure the BRI bus terminal.

If both pins of the switch are in the "ON" position, the 100ohm terminal is switched on, otherwise it is switched off.



Both pins must have the same setting.

Configuration of the PCI bus power supply (not for SX2-express DualPRI)

On the right side of the SX2 QuadBRI is a three-pole jumper field for setting the PCI bus power supply.

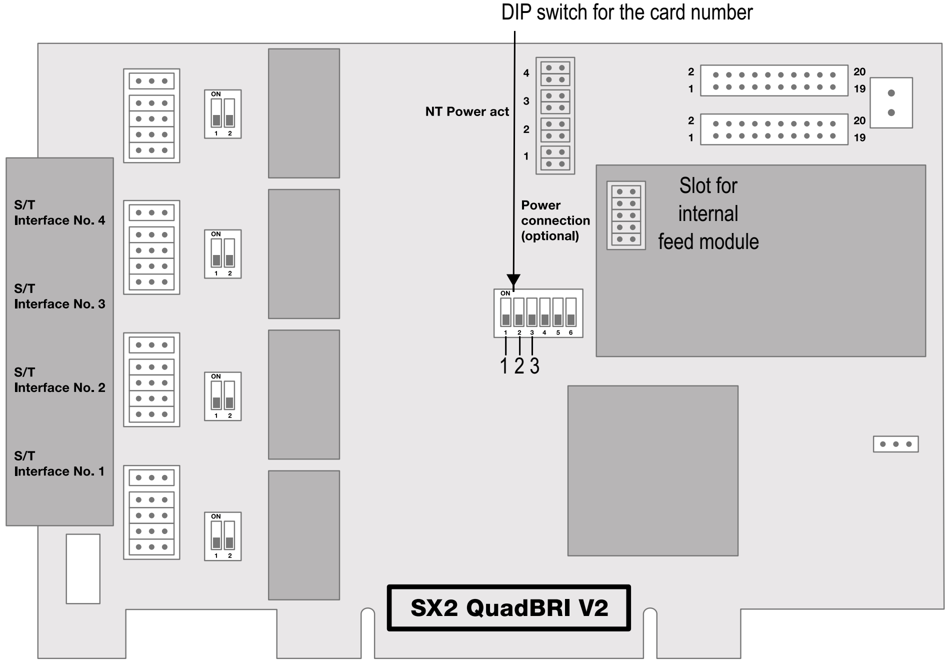
Make sure that the jumper is at the correct setting for the computer's main board.

Left ("3V3 reg") for an environment with 5V, right for an environment with 3.3V, which will be found on older main boards.

Configuration of the card number

You can set the card number with the six-pole DIP switch in the middle of the SX2 QuadBRI.

SX2 QuadBRI V2



For SX2 QuadBRI V2 the following assignment is valid:

Switch 1	Switch 2	Switch 3	Card number
off	off	on	1
off	on	off	2

Switch 1	Switch 2	Switch 3	Card number
off	on	on	3
on	off	off	4
on	off	on	5
on	on	off	6
on	on	on	7
off	off	off	assigned automatically

If you use several cards in one system, please make sure that either one card number was assigned for all cards, or automatic card number assignment is set for all cards.

SX2-express DualPRI

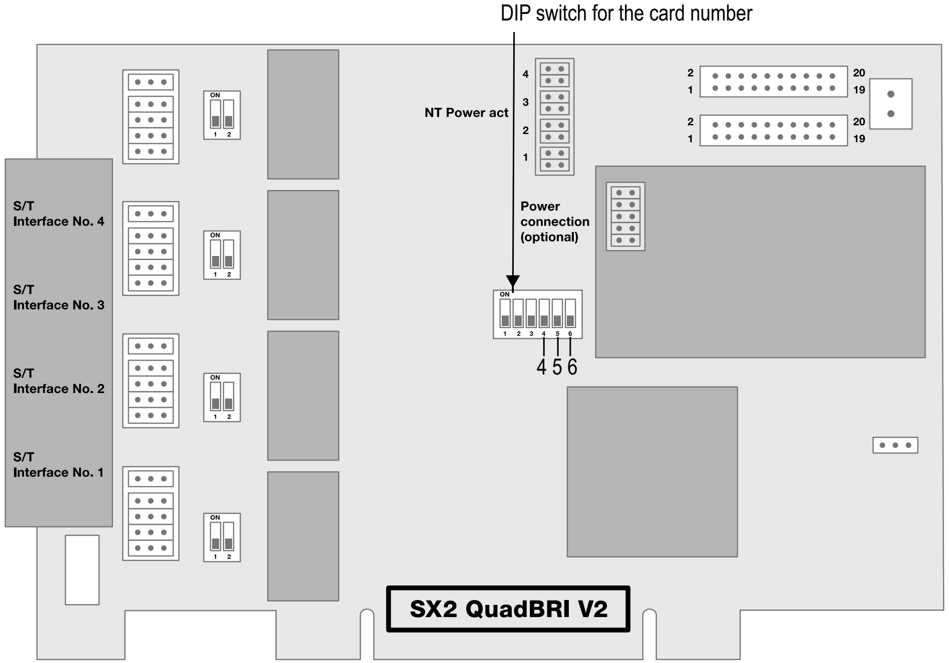


Fig. 15-1: Card number configuration of SX2-express DualPRI

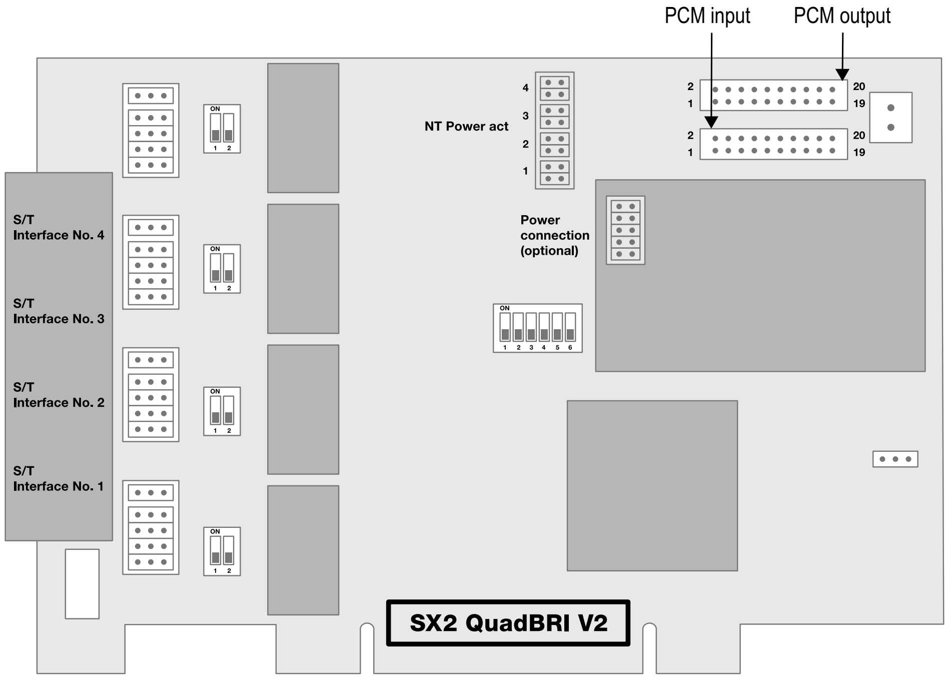
For SX2-express DualPRI, another assignment is valid:

Switch 4	Switch 5	Switch 6	Card number
on	off	off	1
off	on	off	2
on	on	off	3
off	off	on	4
on	off	on	5
off	on	on	6
on	on	on	7
off	off	off	assigned automatically

If you use several cards in one system, please make sure that either one card number was assigned for all cards, or automatic card number assignment is set for all cards.

PCM bus connection

The SX2 QuadBRI / SX2-express DualPRI has two 20-pole jacks for connection with an optional PCM cable.



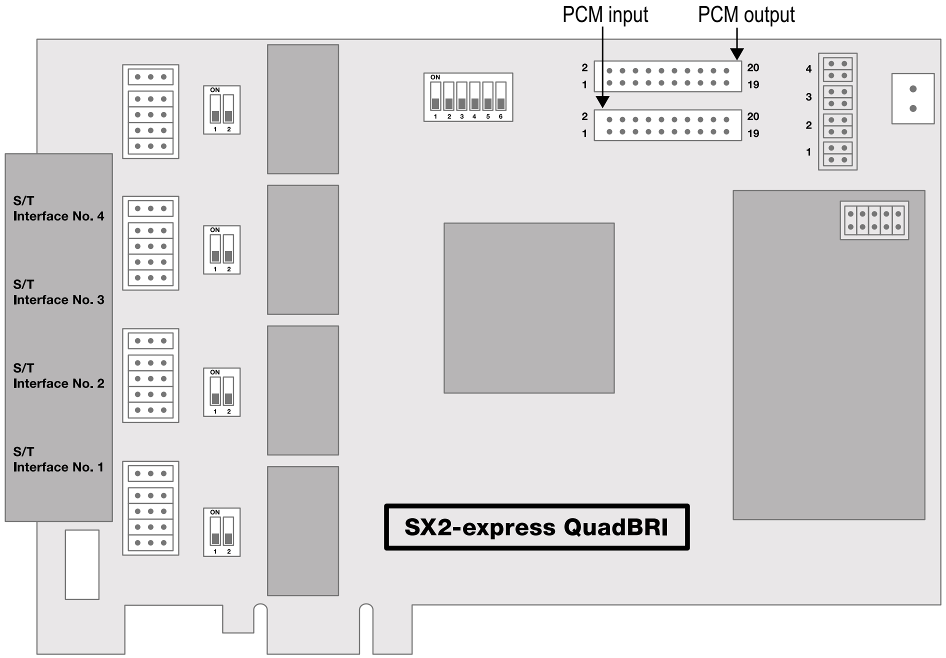


Fig. 15-2: PCM connection of SX2-express DualPRI

The upper jack is the output, the lower jack the input. Connect the SX2 cards with the PCM cable, by connecting the output jack of one card to the input jack of another card.

Please keep in mind that the connection cable differs between both SX2 boards (SX2 QuadBRI or SX2-express DualPRI). A mixed operation using both card types in one computer is not supported.

LED Status Display

To each BRI connection one of the four LEDs is assigned.. The number of the connection corresponds to the number of the LED.

The following illustration shows a slot of the SX2 QuadBRI to identify the Basic Rate Interfaces 1 to 4, shown here as L(ine) 1 to 4:

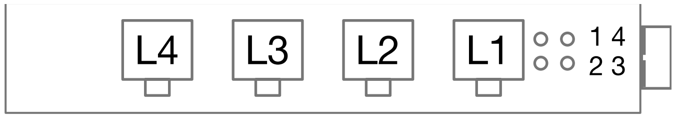


Fig. 15-3: Lines of the SX2 QuadBRI

The following assignments are valid:

LED	Statement
off	Layer 1 deactivated
red glowing	Layer 1 activated
green glowing	Layer 2 activated
green, blinking	At least one connection is active
red, blinking	The line is being configured

After the hardware for the SX2 QuadBRI has been configured according to the use scenario, insert it into the computer on which SwyxGate is to be installed.

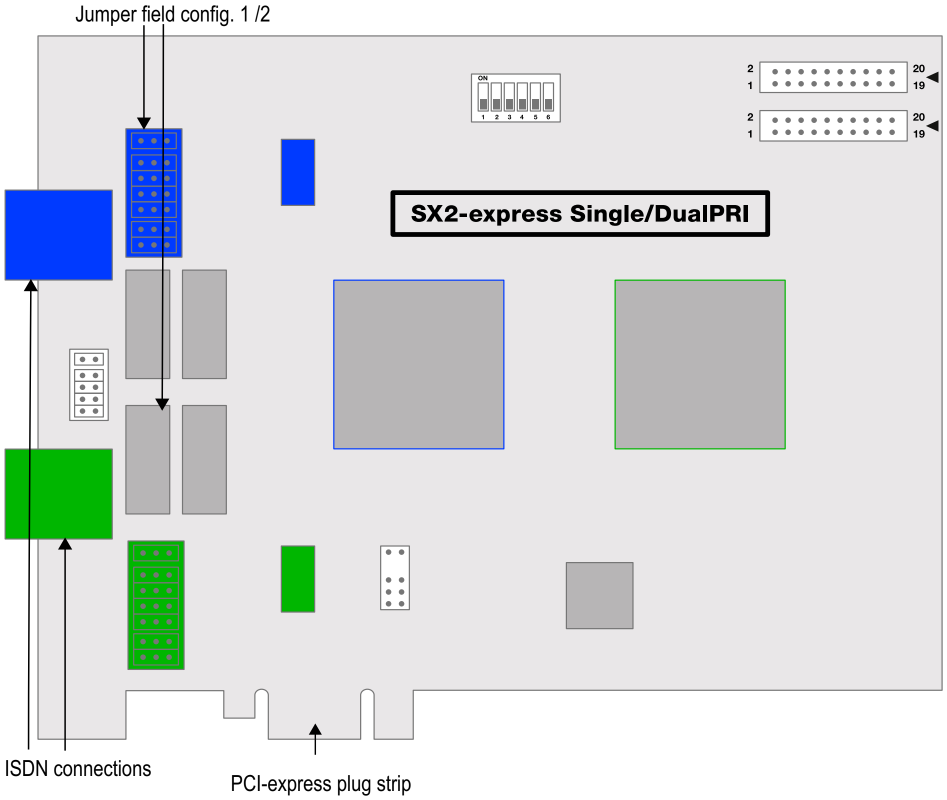
After the card has been installed physically, it will automatically be recognized the next time the computer is booted and a request for the installation of the driver software will appear.

15.2.2 PREPARATION OF SX2-EXPRESS SINGLEPRI / SX2-EXPRESS DUALPRI

The connection configuration must be configured for each E1 connection before it is inserted.

Requirement for further description: Requirement for further description: The SX2-express SinglePRI / SX2-express DualPRIis lying in front of you with the PCI plug strip facing down and the E1 connections to the left.

A jumper field, which are in the near vicinity of the E1 connection plug, are assigned to each E1 connection.



Connection Configuration

The connection configuration allows each E1 connection of the SX2-express SinglePRI or SX2-express DualPRI to be adapted to four different cable assignments.

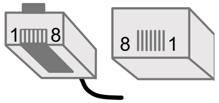
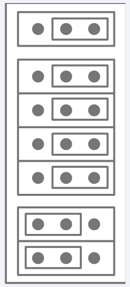
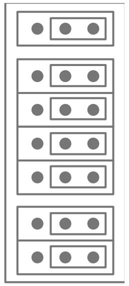
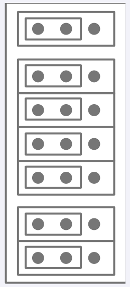


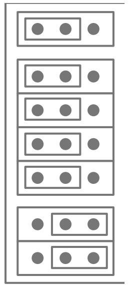
Fig. 15-4: Counting pins of the connector plug (RJ45)

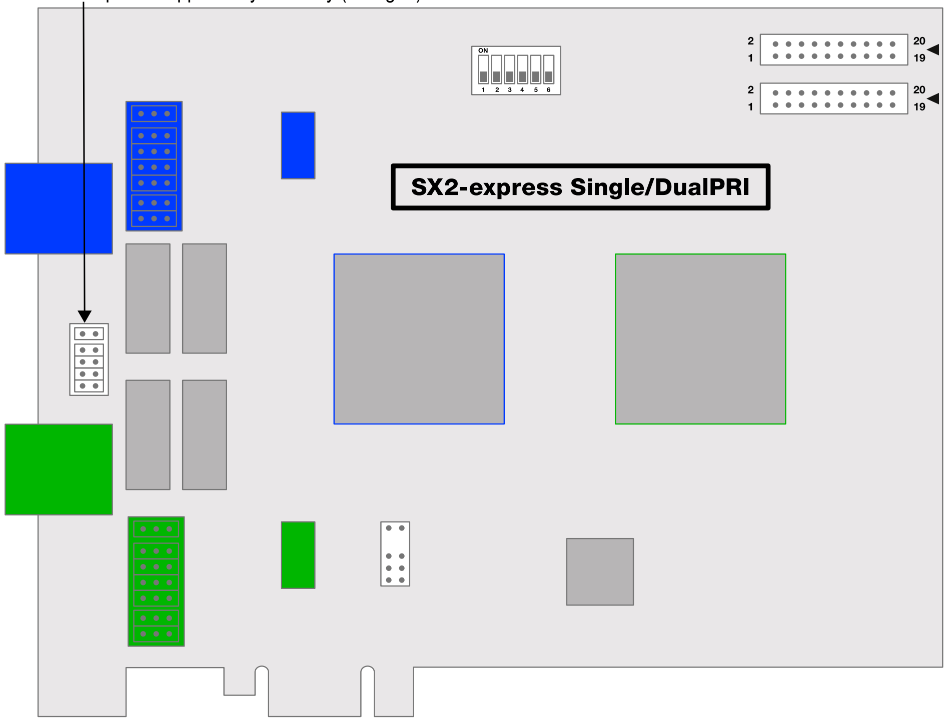
Jumper	Pin configuration, RJ45 jack

	Pin1 = TX+
	Pin2 = TX-
	Pin4 = RX+
	Pin5 = RX-

	Pin6 = TX+
	Pin3 = TX-
	Pin4 = RX+
	Pin5 = RX-

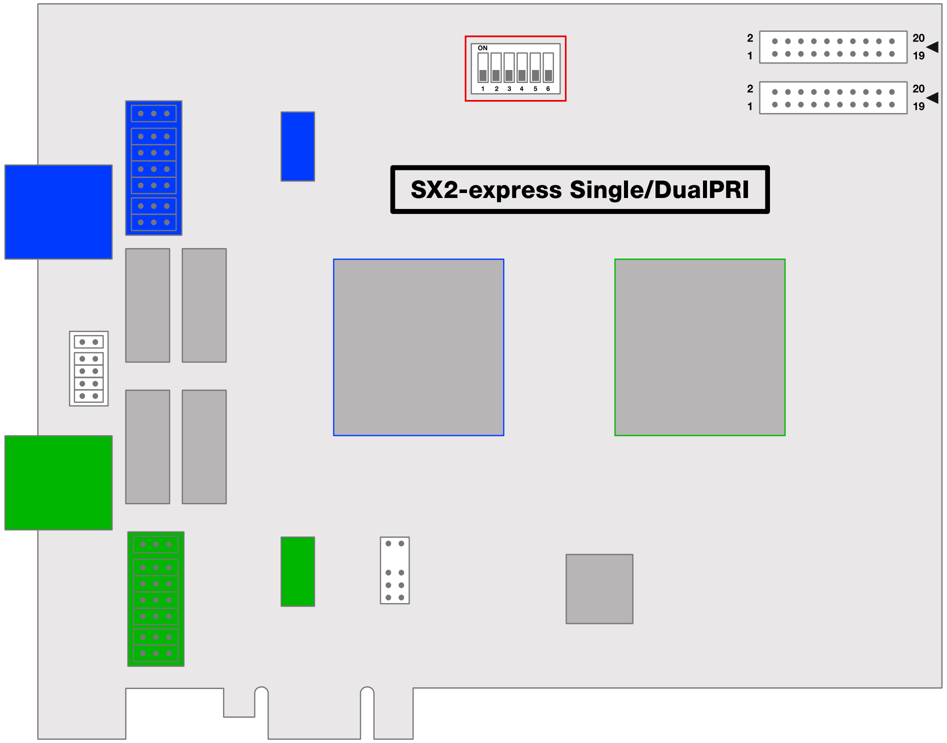
	Pin1 = RX+
	Pin2 = RX-
	Pin4 = TX+
	Pin5 = TX-

	Pin6 = RX+
	Pin3 = RX-
	Pin4 = TX+
	Pin5 = TX-


Jumper to support SwyxStandby (config. 3)

Configuration of the card number

You can set the card number with the six-pole DIP switch in the upper middle of the SX2-express SinglePRI / SX2-express DualPRI.



Only Dip switches 1 to 4 are used. The following assignment is valid:

Switch 1	Switch 2	Switch 3	Switch 4	Card number
on	off	off	off	1
off	on	off	off	2
on	on	off	off	3
off	off	on	off	4
on	off	on	off	5
off	on	on	off	6
on	on	on	off	7
off	off	off	on	8
on	off	off	on	9
off	on	off	on	10
on	on	off	on	11
off	off	on	on	12
on	off	on	on	13
off	on	on	on	14
on	on	on	on	15
off	off	off	off	assigned automatically

If you use several cards in one system, please make sure that either one card number was assigned for all cards, or automatic card number assignment is set for all cards.

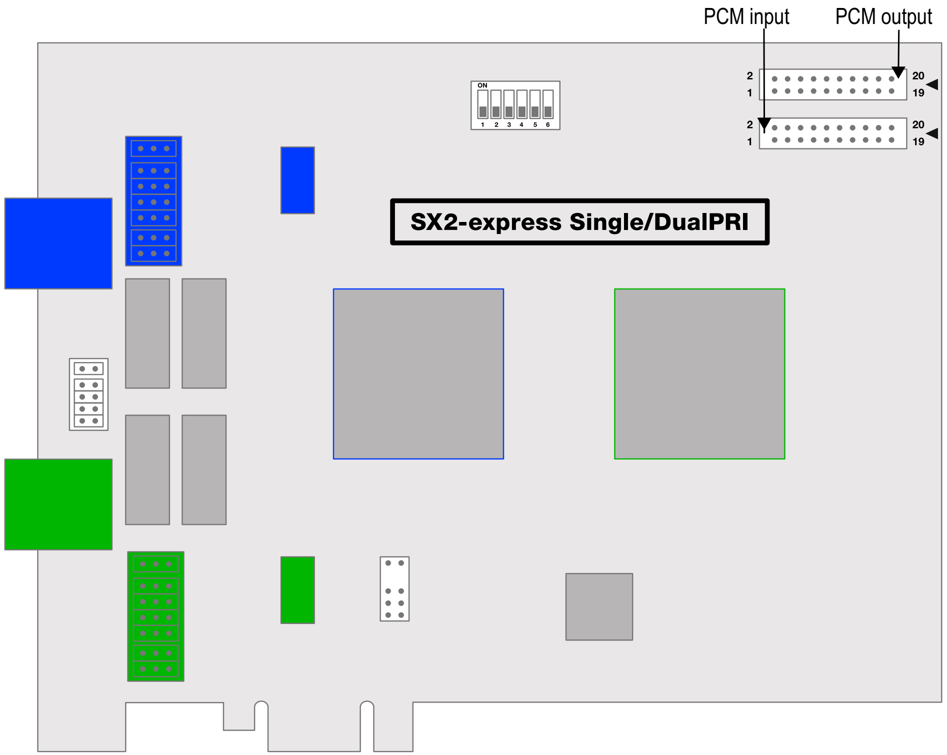
PCM bus connection

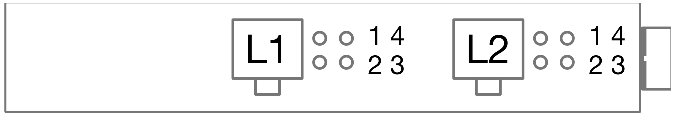
The SX2-express SinglePRI / SX2-express DualPRI has two 20-pole jacks for connection with an optional PCM cable.

The upper jack is the output. The lower jack is the input. Connect the SX2 cards with the PCM cable, by connecting the output jack of one card to the input jack of another card.

LED Status Display

Each E1 connection of the SX2-express SinglePRI / SX2-express DualPRI has a status display consisting of two red and two green LEDs.





The following assignments are valid:

LED	LED	Statement
1	off	Layer 1 deactivated
1	red glowing	Layer 1 activated
2	green glowing	Layer 2 activated
3	green, blinking	At least one connection is active
4	red, blinking	The line is being configured

This is how you install the ISDN cards in your computer

This is how you install the drivers for the ISDN card

15.2.2.1 CONFIGURATION OF THE ISDN CARD

If you would like to connect the card to a direct dialing in line, you must make some configuration changes for the ISDN PC card driver.

You can change the defined parameters in the driver software of the ISDN card at a later point in time.

This is how you modify the ISDN PC card driver configuration

1. Run computer management, the simplest possibility: (the easiest way is to use the context menu for "My Computer" on the Windows Desktop).
2. Select "Manage".
   The Microsoft Management Console (MMC) will be started.
3. Select "Device Manager" in the console structure.
   A list of all installed devices will now be shown on the right. There you will find the following entry under "Network Cards": "SX2 DualPRI".
4. Enter the appropriate settings under "Properties".
   - Select "ISDN Parameters" on the "Advanced" tab.
     Select the "Port" tab in the dialog which is displayed.
   - To switch to a line configured for direct dialing-in, please choose "Point to Point" and close both this tab and the previous tab by clicking on "OK". This setting is deactivated for PRI cards, as PRI cards are always on the direct dialing-in line.

See also *App. M: Configuration of the ISDN Driver*, Page 472.

If the line is configured as an SX2 card, the LED which is associated with this line will blink. This simplifies the identification when operating several SX2 cards.

Configuration of the Line Termination

The line termination will be configured in the software settings. Default value: 120 Ohm.

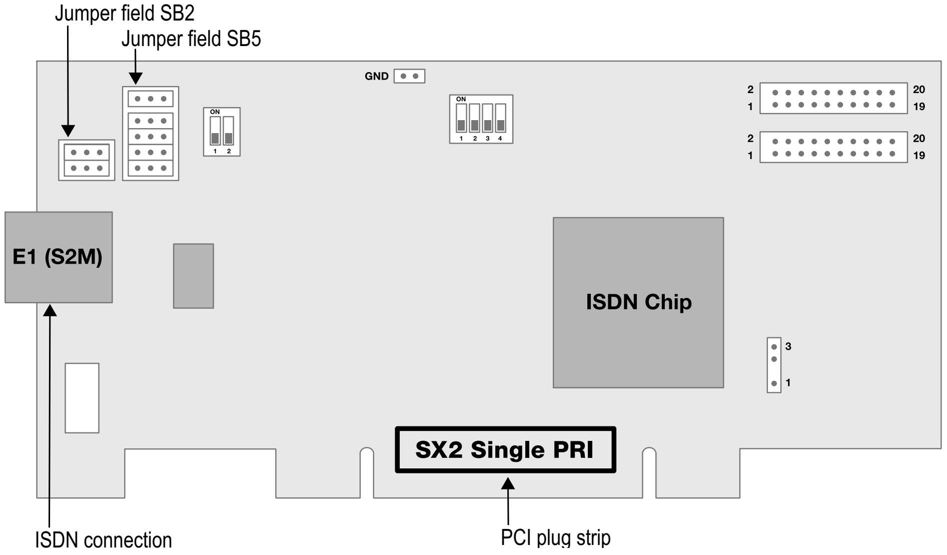
This is how you change the line termination of SX2-express Single-PRI or SX2-express DualPRI

1. Run computer management, the simplest possibility: (the easiest way is to use the context menu for "My Computer" on the Windows Desktop).
2. Under "ISDN Controller" switch to the corresponding SX2-express board.
3. There are settings for each Controller. On the right side mark the controller and choose the line termination you want in the dropdown list.
   You can choose between 120, 110,100 and 75 Ohm.
4. Save the changes with "OK" and close the Device Manager.

15.2.3 PREPARATION OF THE SX2 SINGLEPRI

The connection configuration and the line termination must be configured for each E1 connection of the SX2 SinglePRI before it is inserted.

Requirement for further description: The SX2 SinglePRI is laying in front of you with the PCI plug strip facing down and the E1 connections to the left.



Two jumper fields, which are in the near vicinity of the E1 connection plug, are assigned to the E1 connection. In the following, the field with two jumpers will be referred to as SB2 and the field with five jumpers will be referred to as SB5. The suffixes L and R indicate whether all jumpers of the respective jumper field are inserted to the left (L) or to the right (R). SB5R means, for example, that all jumpers of the SB5 field are inserted on the right.

Connection Configuration

The connection configuration allows the E1 connection to be adapted to four different cable assignments.

Occupation of the Plug Bridges	Pin configuration, RJ45 jack

SB2L and SB5R	Pin1 = TX+
	Pin2 = TX-
	Pin4 = RX+
	Pin5 = RX-

Occupation of the Plug Bridges	Pin configuration, RJ45 jack

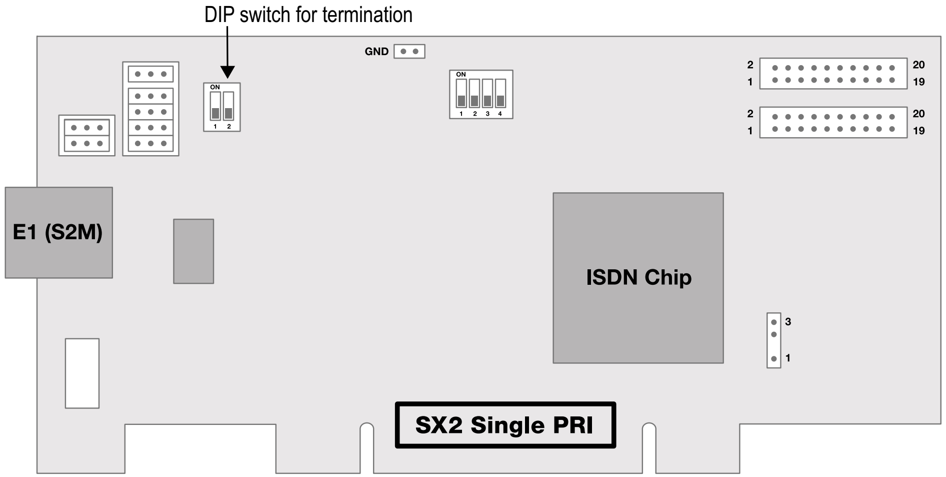
SB2R and SB5R	Pin3 = TX+
	Pin6 = TX-
	Pin4 = RX+
	Pin5 = RX-

SB2L and SB5L	Pin1 = RX+
	Pin2 = RX-
	Pin4 = TX+
	Pin5 = TX-

SB2R and SB5L	Pin3 = RX+
	Pin6 = RX-
	Pin4 = TX+
	Pin5 = TX-

Configuration of the Line Termination

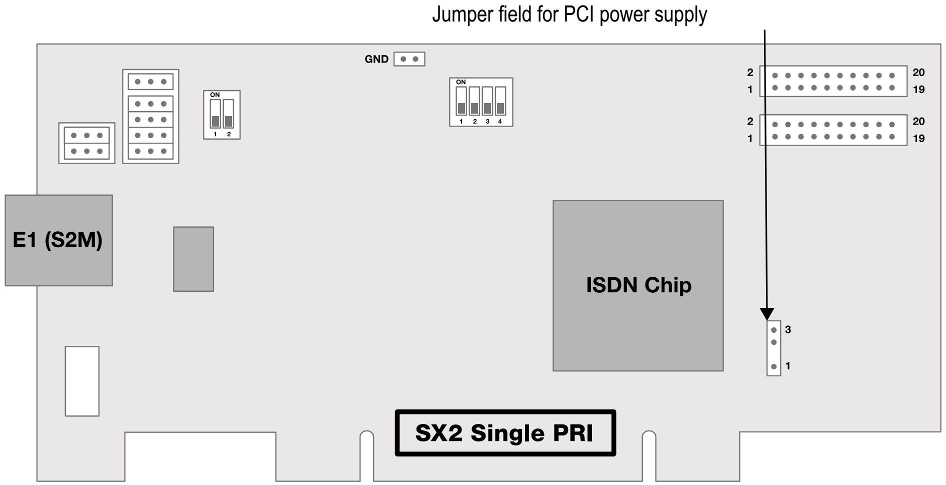
On the right next to the plug bridge fields for the E1 connection you will find a two-pole DIP switch with which the line termination can be configured.



- If both pins of the switch are in the "OFF" position, no termination is switched on.
- If the left pin is on the "OFF" position and the right pin is on the "ON" position, this means that this has a 120 ohm line termination.
- If the left pin is on the "ON" position and the right pin is on the "OFF" position, this means that this has a 75 ohm line termination.

Configuration of the PCI bus power supply

On the lower right side of the SX2 SinglePRI is a three-pole jumper field for setting the PCI bus power supply.



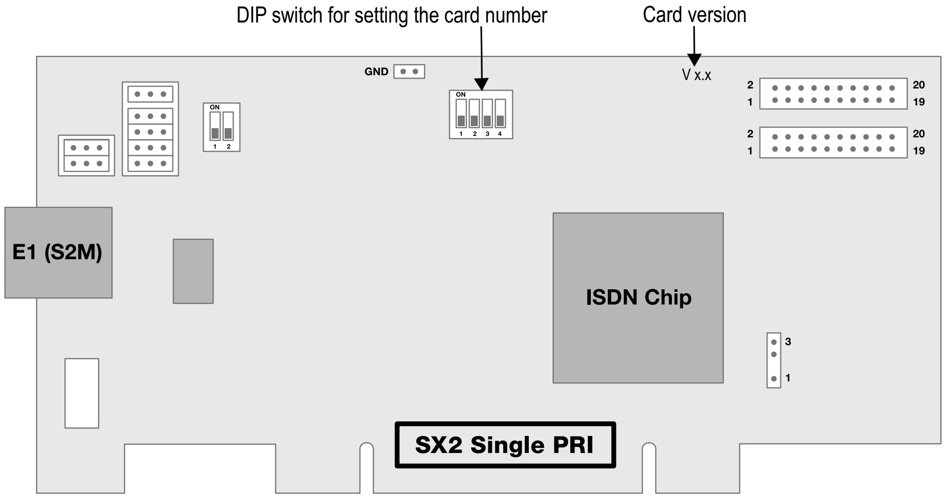
Make sure that the jumper is at the correct setting for the computer's main board.

Lower for an environment with 3V, upper for an environment with 5V, which will be found on older main boards.

Configuration of the card number

You can set the card number with the four-pole DIP switch in the upper middle of the SX2 SinglePRI.

Please keep in mind that SX2 SinglePRI V2 and V3 only differ in the configuration of the card number.



For SX2 SinglePRI V2 the following assignment is valid:

Switch 1	Switch 2	Switch 3	Switch 4	Card number
off	off	off	on	1
off	off	on	off	2
off	off	on	on	3
off	on	off	off	4
off	on	off	on	5
off	on	on	off	6
off	on	on	on	7
on	off	off	off	8
on	off	off	on	9
on	off	on	off	10
on	off	on	on	11
on	on	off	off	12
on	on	off	on	13
on	on	on	off	14
on	on	on	on	15
off	off	off	off	assigned automatically

For SX2 SinglePRI V3 the following assignment is valid:

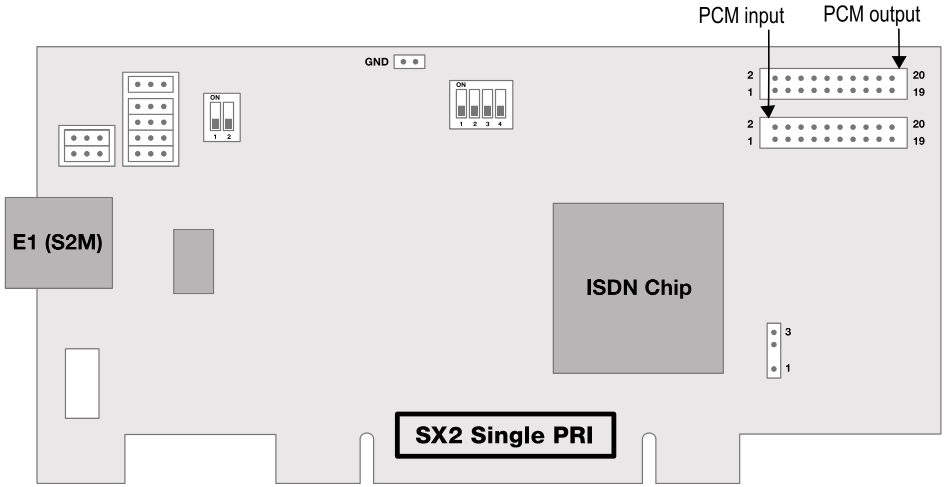
Switch 1	Switch 2	Switch 3	Switch 4	Card number
on	off	off	off	1
off	on	off	off	2
on	on	off	off	3
off	off	on	off	4
on	off	on	off	5
off	on	on	off	6
on	on	on	off	7
off	off	off	on	8
on	off	off	on	9
off	on	off	on	10
on	on	off	on	11
off	off	on	on	12
on	off	on	on	13
off	on	on	on	14
on	on	on	on	15

Switch 1	Switch 2	Switch 3	Switch 4	Card number
off	off	off	off	assigned automatically

If you use several cards in one system, please make sure that either one card number was assigned for all cards, or automatic card number assignment is set for all cards.

PCM bus connection

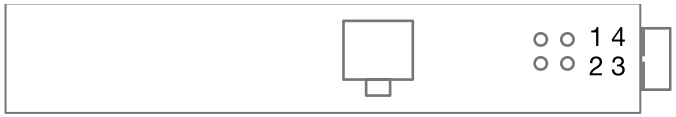
The card has two 20-pole jacks for connection with an optional PCM cable.



The upper jack is the output. The lower jack is the input. Connect the SX2 cards with the PCM cable by connecting the output jack of a SX2 card with the input jack of another SX2 card.

LED Status Display

The E1 connection of the SX2 SinglePRI has a status display consisting of two red and two green LEDs.



The following assignments are valid:

LED	LED	Statement
1	off	Layer 1 deactivated
1	red glowing	Layer 1 activated
2	green glowing	Layer 2 activated
3	green, blinking	At least one connection is active
4	red, blinking	The line is being configured

This is how you install the ISDN cards in your computer

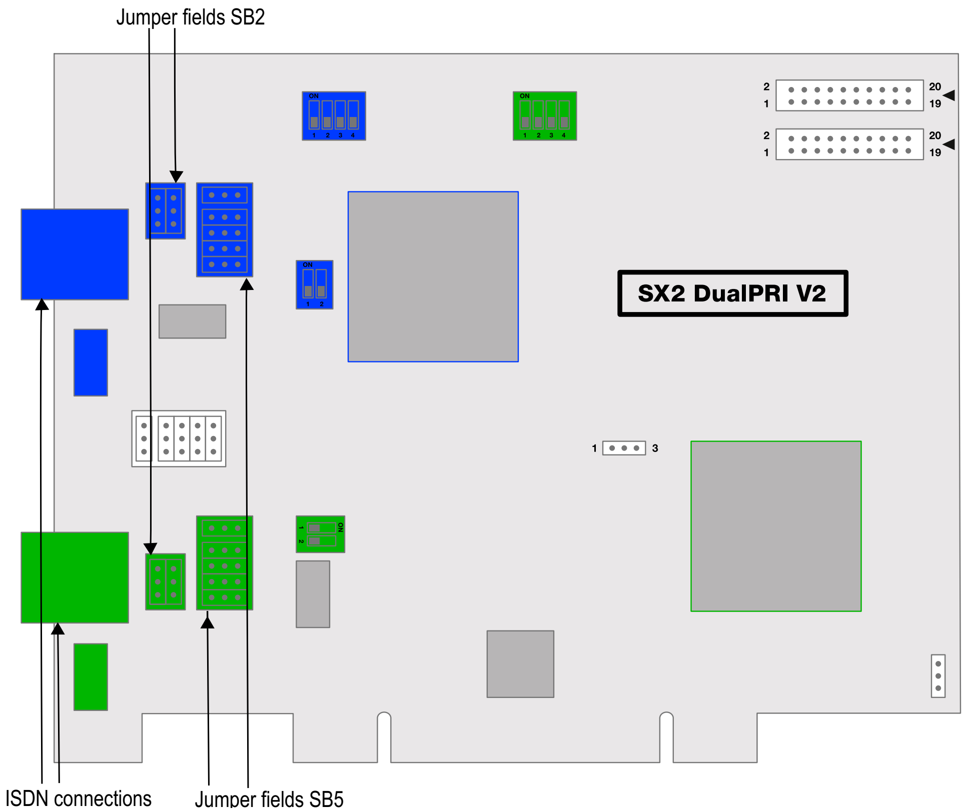
This is how you modify the ISDN card driver configuration

15.2.4 PREPARATION OF THE SX2 DUALPRI

The connection configuration and the line termination must be configured for each E1 connection of the SX2 DualPRI V2 before it is inserted.

Requirement for further description: The SX2 DualPRI V2 is laying in front of you with the PCI plug strip facing down and the E1 connections to the left.

Two jumper fields, which are in the near vicinity of the E1 connection plug, are assigned to each E1 connection. In the following, the field with two jumpers will be referred to as SB2 and the field with five jumpers will be referred to as SB5. The suffixes L, R, O and U indicate whether all jumpers of the respective jumper field are inserted to the left (L), to the right (R), above (O) or below (U). SB5R means, for example, that all jumpers of the SB5 field are inserted on the right.



Connection Configuration

The connection configuration allows each E1 connection of the SX2 DualPRI V2 to be adapted to four different cable assignments.

Occupation of the Plug Bridges	Pin configuration, RJ45 jack

SB2O and SB5R	Pin1 = TX+
	Pin2 = TX-
	Pin4 = RX+
	Pin5 = RX-

SB2U and SB5R	Pin3 = TX+
	Pin6 = TX-
	Pin4 = RX+
	Pin5 = RX-

SB2O and SB5L	Pin1 = RX+
	Pin2 = RX-
	Pin4 = TX+
	Pin5 = TX-

SB2U and SB5L	Pin3 = RX+
	Pin6 = RX-
	Pin4 = TX+
	Pin5 = TX-

Configuration of the Line Termination

On the right next to the plug bridge fields for each connection you will find a two-pole DIP switch with which the line termination can be configured.

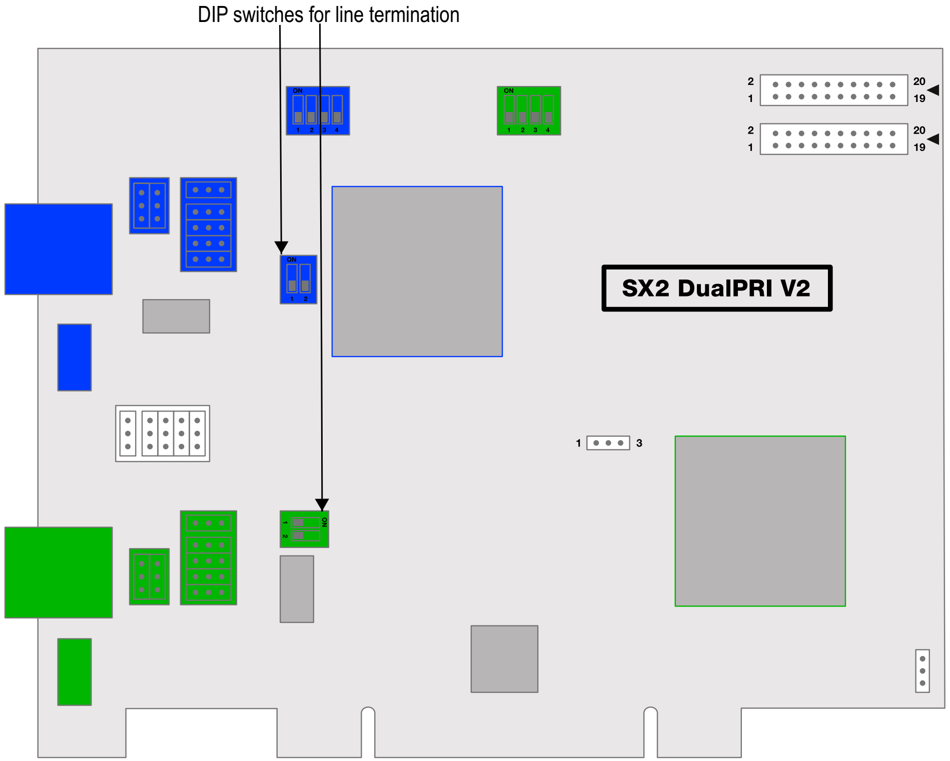
- If both pins of the switch are in the "OFF" position, no termination is switched on.
- If the left pin is on the "OFF" position and the right pin is on the "ON" position, this means that this has a 120 ohm line termination.
- If the left pin is on the "ON" position and the right pin is on the "OFF" position, this means that this has a 75 ohm line termination.

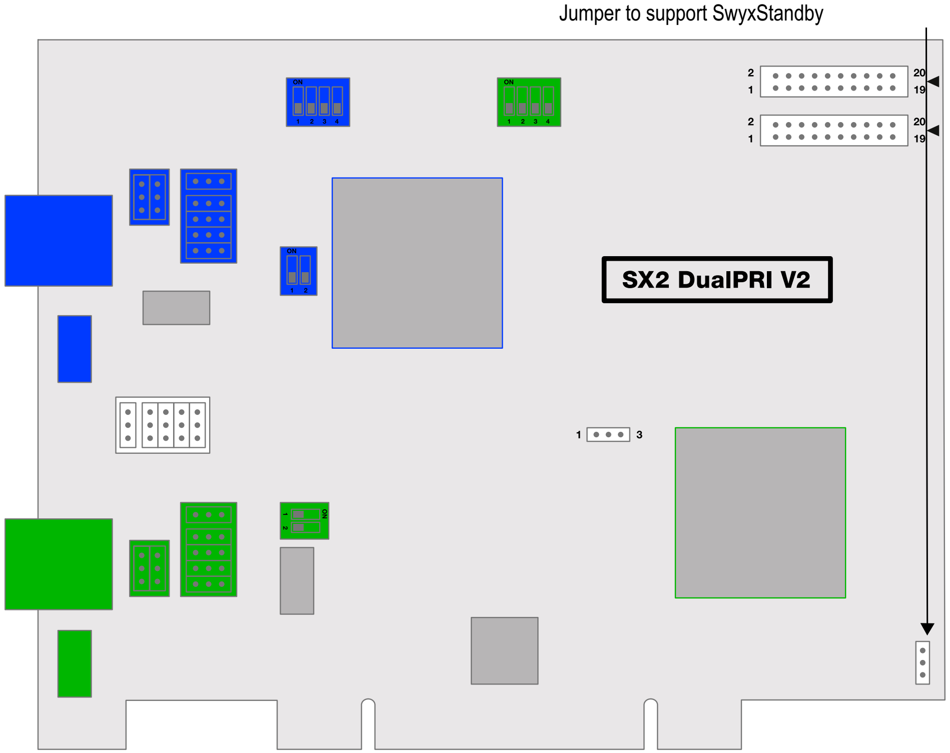
Configuration of the PCI bus power supply

On the lower right side of the SX2 DualPRI V2 is a three-pole jumper field for setting the PCI bus power supply.

Make sure that the jumper is at the correct setting for the computer's main board.

Lower for an environment with 3V, upper for an environment with 5V, which will be found on older main boards.





SwyxStandby support

The card supports the SwyxWare option pack SwyxStandby.

In order to activate this function on the SX2 DualPRI V2, please make sure that the six-pole jumper is inserted between the two ISDN connections; if this jumper is not present, the card cannot support the standby option.

Configuration of the Interrupt assignment

In the middle of the SX2 DualPRI is a three-pole jumper field.

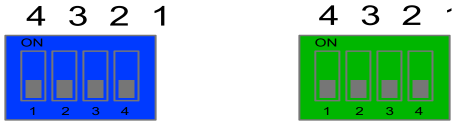
Make sure that the plug is in the left position. It is thereby ensured that separate interrupts are applied, as required in the driver software.

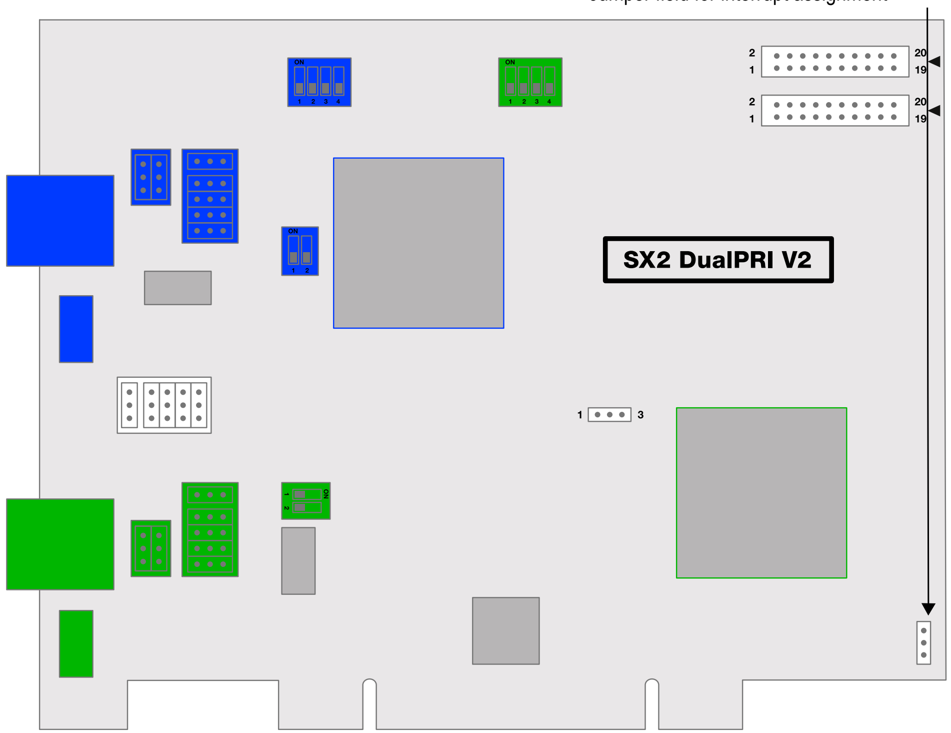
Configuration of the card number

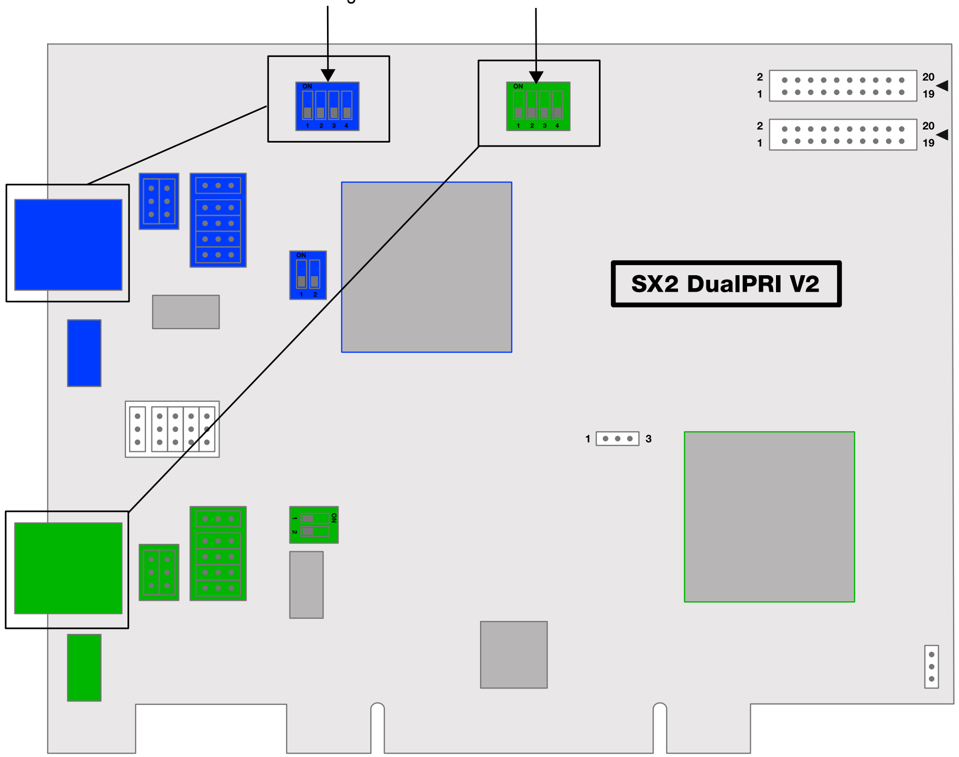
You can set the card number with the four-pole DIP switch in the upper middle of the SX2 DualPRI V2.

The left DIP switch applies to the upper connector, the right DIP switch to the lower connector.

Please note the numbering of the particular switches:




Jumper field for interrupt assignment


Configuration of the card number

The numbering on the board may differ from this documentation.

The following assignment is valid:

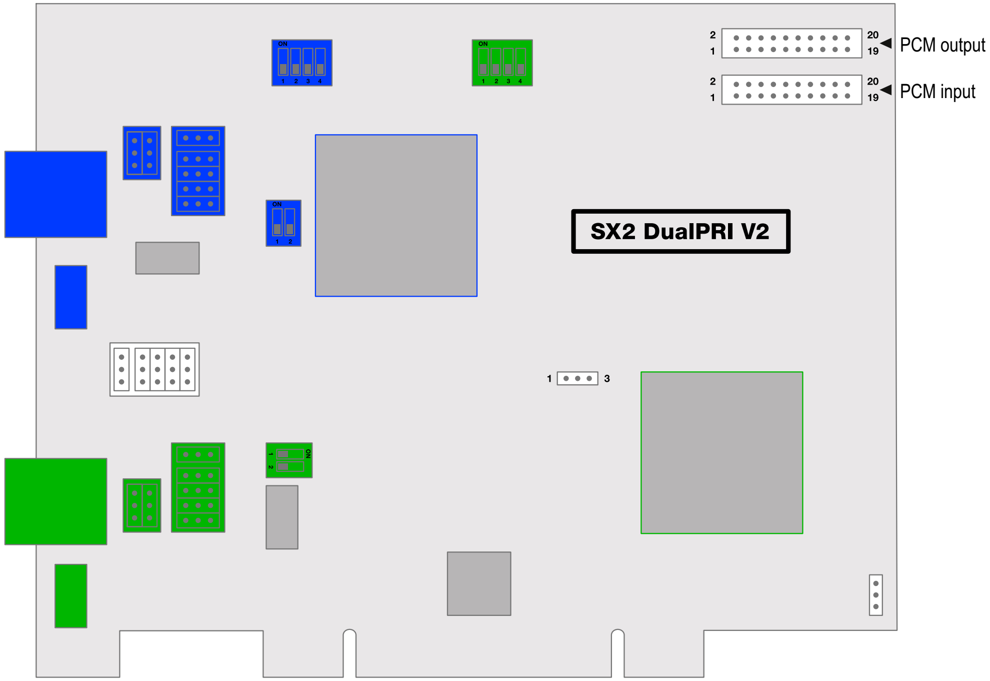
Switch 1	Switch 2	Switch 3	Switch 4	Card number
on	off	off	off	1
off	on	off	off	2
on	on	off	off	3
off	off	on	off	4
on	off	on	off	5
off	on	on	off	6
on	on	on	off	7
off	off	off	on	8
on	off	off	on	9
off	on	off	on	10
on	on	off	on	11
off	off	on	on	12
on	off	on	on	13
off	on	on	on	14
on	on	on	on	15

Switch 1	Switch 2	Switch 3	Switch 4	Card number
off	off	off	**off**	assigned automatically

If you use several cards in one system, please make sure that either one card number was assigned for all cards, or automatic card number assignment is set for all cards.

PCM bus connection

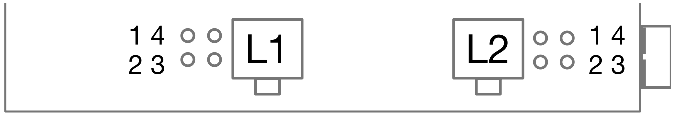
The SX2 DualPRI V2 card has two 20-pole jacks for connection with an optional PCM cable.



The upper jack is the output. The lower jack is the input. Connect the SX2 cards with the PCM cable, by connecting the output jack of one card to the input jack of another card.

LED Status Display

Each E1 connection of the SX2 DualPRI V2 has a status display consisting of two red and two green LEDs.



The following assignments are valid:

LED	LED	Statement
1	off	Layer 1 deactivated
1	red glowing	Layer 1 activated
2	green glowing	Layer 2 activated
3	green, blinking	At least one connection is active
4	red, blinking	The line is being configured

15.2.5 INSERTION OF THE ISDN CARD

The insertion of the ISDN cards is nearly identical and therefore they are explained together in this chapter.

After the card has been installed physically, it will automatically be recognized the next time the computer is booted and a request for the installation of the driver software will appear.

You may find more recent drivers for the ISDN cards in the download area of the homepage:

enreach.com/products/support/support-downloads.html

Do the necessary hardware configuration before the insertion. See 15Preparation of the SX2 DualPRI, Page 259.

It is absolutely necessary that you turn off the computer and remove the mains plug from the power supply whenever you are doing something which requires you to open the computer case!

Do not touch any of the electronic components of the computer card during the entire installation process. The electronic components of the computer card can be damaged by electrostatic discharges!

For safety reasons, it is necessary that you disconnect all connection cables from the telephone network before you open the computer case.

This is how you install the ISDN cards in your computer

1. Turn off your computer and pull the respective mains plug out of the socket.
2. Open your computer.
3. Remove the screw from the metal panel covering a free PCI-express (expansion) slot:

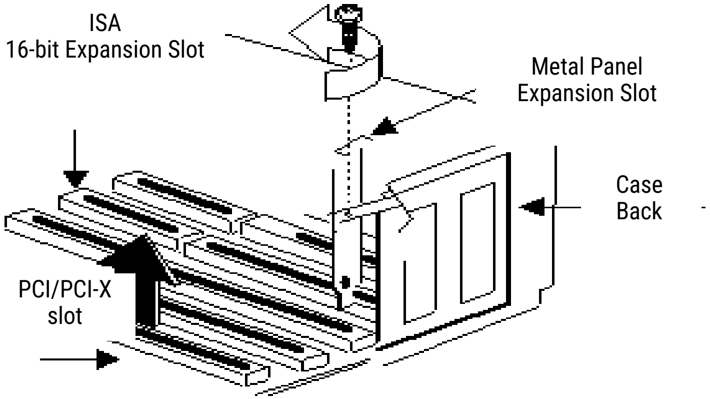


Fig. 15-5: Removing the Metal Panel

4. Insert the ISDN card into a free PCI or PCI-X plug-in slot.
5. Use the screw you just removed to secure the card.
6. Connect the SX2 DualPRI to the S2m ISDN connections with the cables provided.

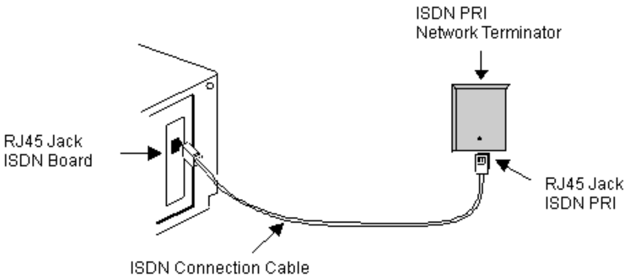


Fig. 15-6: Connecting the ISDN Cable

7. Close your computer and restore the power supply by plugging in the mains plug.

15.2.6 INSTALLATION OF THE SOFTWARE FOR THE ISDN CARD

The computer recognizes the card after the next restart, and the driver software can be installed.

This is how you install the drivers for the ISDN card

1. Follow the instructions given by the hardware wizard.
2. When you are asked to enter the source for the driver, select "Enter other source".
3. Put the SwyxWare DVD into your DVD ROM drive.
   Click on "Next >".
4. Select the driver files. They can be found at https://www.enreach.de/produkte/support/support-downloads.html#cat_6
5. During the installation of the driver you will be asked to enter the ISDN switching type or the D-channel protocol.
6. Select the ISDN exchange type or the switch protocol used by your telephone company (in Europe this is Euro-ISDN (DSS1)).
   Click on "Next>".

7 Follow the wizard's instructions and then click on "Finish" in the dialog "Completing the wizard".

You can check to see if the driver installation was successful by checking the entries in the Device Manager in the 'Network Cards' category.

> You can check the operation of the installed ISDN cards with the utilities. See *E.4.1 Test Programs for the SX2 Card Family*, Page 427.

15.2.7 CONFIGURATION OF THE ISDN CARD

If you would like to connect the card to a direct dialing in line, you must make some configuration changes for the ISDN card driver.

You can change the defined parameters in the driver software of the ISDN card at a later point in time.

This is how you modify the ISDN card driver configuration

1 Run computer management, the simplest possibility: (the easiest way is to use the context menu for "My Computer" on the Windows Desktop).

2 Select "Manage".
The Microsoft Management Console (MMC) will be started.

3 Select "Device Manager" in the console structure.
A list of all installed devices will now be shown on the right. There you will find the following entry under "Network Cards": "SX2 DualPRI".

4 Enter the appropriate settings under "Properties".
- Select "ISDN Parameters" on the "Advanced" tab.
  Select the "Port" tab in the dialog which is displayed.
- Zur To switch to a line configured for direct dialing-in, please choose "Point to Point" and close both this tab and the previous tab by clicking on "OK".

See also *App. M: Configuration of the ISDN Driver*, Page 472.

> If the line is configured as an SX2 card, the LED which is associated with this line will blink. This simplifies the identification when operating several SX2 cards.

15.3 CREATION OF AN ISDN TRUNK GROUP

When you create a single trunk, you are asked for the trunk group to which this newly created trunk should belong.

General parameters such as permissions, location and routings are specified in this group. When creating a trunk, you then simply assign the trunk group to the trunk. As a member of the group, the trunk is thus given the corresponding parameters.

Alternatively, when creating a trunk, you can also generate the corresponding trunk group directly.

This is how you create an ISDN trunk group

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunk Groups" and select the entry "Add Trunk Group..." in the context menu.
The "Add Trunk Group..." wizard will appear.

3 Click on "Next>".

4 Name and description of the trunk group:
Enter the name of the trunk group, and a description.
Click on "Next>".

5 Type of trunk group:
Enter here the type of trunk group, in this case "ISDN".

6 Enter the profile for this trunk group in the lower field "Profile".
See also *15.3.1 Profile of an ISDN trunk group*, Page 266.
Click on "Next >".

7 Definition of routing:

Specify for which calls this Trunk Group should be used. When entering call numbers or URIs you can use placeholders (*), e.g. "+*" for all external numbers or "*" for all internal numbers. Multiple numbers/URIs are separated by a semicolon. You have several different options:

- for all external calls
- only for external calls to the following destination number or SIP-URI
- for all external calls and all unassigned internal numbers
- for the following internal numbers

Click on "Next>".

8 Call Permission
Specify the Calling Rights profile for the Trunk Group. This Calling Rights profile applies to the incoming calls over this Trunk Group.
See also *Call permission of a trunk group*, Page 129.
Click on "Next>".

9 Location profile:
Define the location. This profile also includes the definition of e.g. country code and public line access.
Click on "Next>".

10 Click "Finish".
The new ISDN trunk group is created, and is available for further configuration.

15.3.1 PROFILE OF AN ISDN TRUNK GROUP

Depending on the connection you can select an appropriate profile for the trunk group. Dependent on this profile, the representation of the numbers is also thereby specified.

There are several predefined profiles available:

Profile	Explanation
Standard DDI	● Outgoing call Calling party number Extension Destination number: Subscriber ● Incoming call Calling party number Subscriber Destination number: Extension
Standard MSN	● Outgoing call Calling party number Subscriber Destination number: Subscriber ● Incoming call Calling party number Subscriber Destination number: Subscriber
Italy DDI	● Outgoing call Calling party number Extension Destination number: ISDN Italy ● Incoming call Calling party number ISDN Italy Destination number: Extension
Italy MSN	● Outgoing call Calling party number Subscriber Destination number: ISDN Italy ● Incoming call Calling party number ISDN Italy Destination number: ISDN Italy
Netherlands	● Outgoing call Calling party number Calling party number: ISDN Netherlands CLIP Destination number: national ● Incoming call Calling party number Calling party number: ISDN Netherlands CLIP Destination number: national
Switzerland (MSN)	● Incoming call Calling party number Subscriber Destination number: national ● Outgoing call Calling party number Subscriber Destination number: Subscriber

Profile	Explanation
Switzerland (DDI)	● Incoming call Calling party number Extension Destination number: national ● Outgoing call Calling party number Subscriber Destination number: Extension
Belgium	● Incoming call Calling party number Subscriber Destination number: national ● Outgoing call Calling party number Subscriber Destination number: Subscriber
DDI with CLIP no screening	● Outgoing call Calling party number CLIP no screening Destination number: Subscriber ● Incoming call Calling party number Subscriber Destination number: Extension
MSN with CLIP no screening	● Outgoing call Calling party number CLIP no screening Destination number: Subscriber ● Incoming call Calling party number Subscriber Destination number: Subscriber
Internal Lines	● Outgoing call Calling party number Destination number: Dial as a PBX user Destination number: transparent ● Incoming call Calling party number: transparent Destination number: Destination number: Dial as a PBX user

If you set a different number representation, by choosing a different option from the selection list, the changed profile is stored under a different name (customized).

See also *10.6.1 NumberFormatProfiles.config*, Page 155.

15.4 CREATION OF AN ISDN TRUNK

If SwyxServer and the SwyxWare Administration are already installed, then following the insertion of the ISDN card and the creation of an ISDN trunk group you can set up an ISDN trunk.

In the standard installation of the SwyxServer software, the corresponding service SwyxGate which is responsible for the link-up of ISDN lines is automatically installed. During the installation of an ISDN trunk you give the name of the computer on which the SwyxGate service is installed. This service is then used by the ISDN trunk.

The administration of an ISDN trunk is handled with the SwyxWare Administration. Please start SwyxWare Administration as described in *7.1 Registration on SwyxWare Administration*, Page 80. If you are not yet connected to this server, please connect now as described in *How to connect to a SwyxServer*, Page 83.

This is how you create an ISDN Trunk

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunks" and select the entry "Add Trunk..." in the context menu.

3 An "Add new Trunk Wizard" opens up.
Click on "Next>".

4 Trunk name:
Enter a name and a short description for the new trunk here.
Click on "Next>".

5 Selection of a trunk group:
Select the trunk group here to which this trunk should be assigned. General settings such as routings, rights and location-specific parameters are specified in the trunk group. You can use "New Trunk Group..." to create a new trunk group, and then continue with the creation of a trunk.

6 Numbers:
Enter here the public phone numbers to be used by this trunk, see *This is how you add numbers for this trunk*, Page 270

See also *This is how you create an ISDN trunk group*, Page 265.
Click on "Next >".

7 Codecs:
With the help of the Codec you select how the voice is compressed for transmission. The following options are available:

If the Codec priority "Prefer Quality" is selected, the Codecs are provided in the sequence G.722, G.711a, G.711µ, G.729 and Fax over IP. Specify the filter(s) you want. The Codec G.722 is deactivated by default, because it would only be supported up to the ISDN gateway.

- Voice, high bandwidth (G.711a, G.711µ)
  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64kbits/s.
- Voice, low bandwidth (G.729)
  High compression. A voice connection requires approximately 24kbits/s.
- Fax
  In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration. A fax connection using T.38 requires approximately 20kbits/s.

If the Codec priority "Prefer low bandwidth" is selected, the Codecs sequence changes to G.729, G.722, G.711a, G.711µ, Fax over IP. The Codec G.722 is deactivated by default, because it would only be supported up to the ISDN gateway. The aim here is to use as little bandwidth as possible. Here too, specify the filter(s).

8 Click on "Next>".
Both voice compressions can be activated for a voice connection. In this case the SwyxServer decides which compression is applied.

9 Number of ISDN channels:
Give the number of lines that are served by this trunk.

10 Computer name:
Give the name of the computer in which the card has been inserted. The SwyxGate service must also be installed on this computer, before this trunk can be used. Please use a WINS or the DNS name as the computer name. Alternatively you can also give the IP address of the computer directly. Do not enter ’localhost’ here.

11 Select ISDN ports:/
Select the ISDN card from the list. According to the ISDN card, the available ports are displayed. Select the port to be used. The selection of the port is visualized with the help of a blinking LED on the ISDN card. This lets you see easily which port the ISDN connection cable must be connected to.

12 Click "Finish".
The new Trunk is created, and is available for further configuration.

You can further configure the properties of this trunk after the installation. See *15.5 Configuring an ISDN Trunk*, Page 268.

For information on deactivating and reactivating a trunk, please see *13.2 Activating and deactivating a trunk*, Page 237.

15.5 CONFIGURING AN ISDN TRUNK

When you have created an ISDN trunk as described in *15.4 Creation of an ISDN trunk*, Page 267, you can subsequently change the settings of this trunk in the SwyxWare Administration, and e.g. add further MSNs.

When parameters of a trunk are changed, this change takes effect at once. There is no need to halt and restart any services for this.

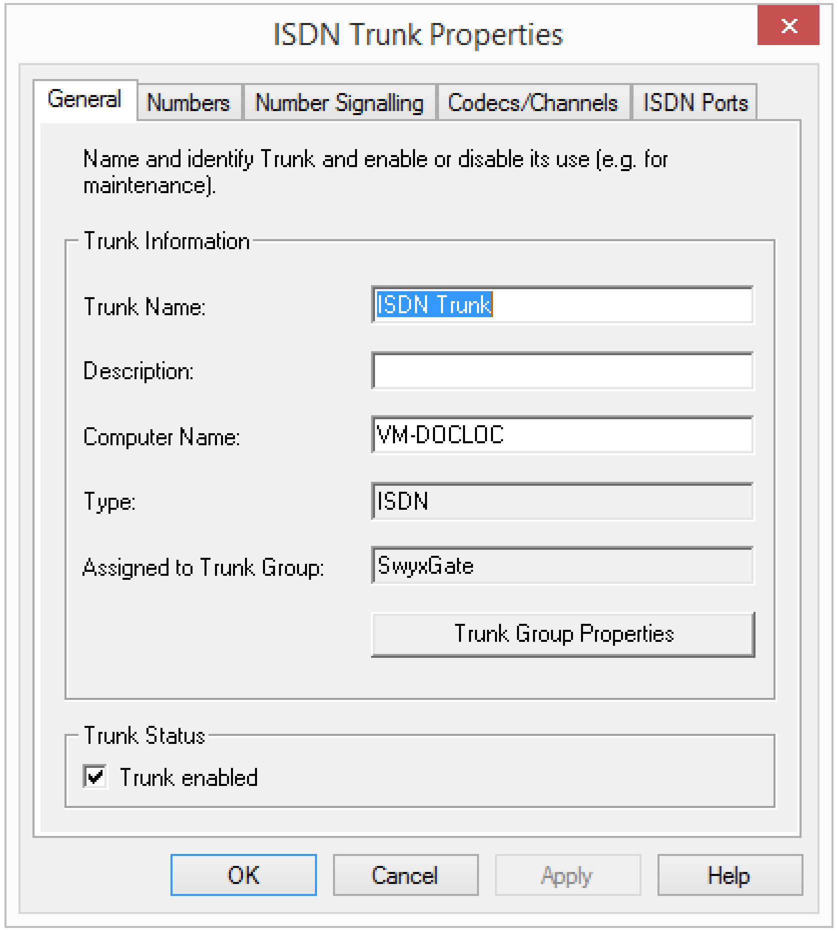
How to configure an ISDN trunk

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click on "Trunks", and in the right-hand window select the trunk you want to configure.

3 In the context menu, select "Properties".
In each case, the "Properties of..." window will appear.

The "General" Tab



ISDN Trunk Properties

Name and identify Trunk and enable or disable its use (e.g. for maintenance).

Trunk Information

Trunk Name: ISDN Trunk

Description:

Computer Name: VM-DOCLOC

Type: ISDN

Assigned to Trunk Group: SwyxGate

Trunk Status

☑ Trunk enabled

In this tab you can modify the name and description of the trunk.

Trunk information:

In the fields "Trunk Name" and "Description" you will find the descriptive information that is displayed in Administration.

The field "Computer Name" contains the name of the computer in which the service (LinkManager or SwyxGate) is installed.

The "Type" field indicates the type of the trunk, and "Trunk Group" the assigned Trunk Group. Both parameters cannot be retrospectively changed.

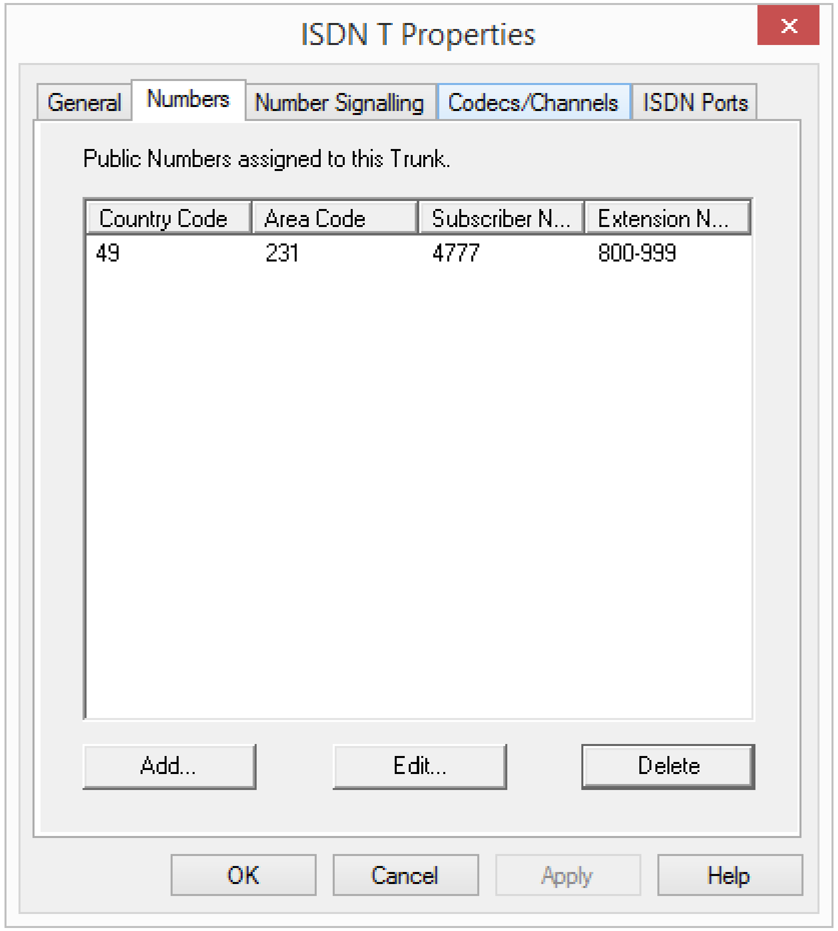
Using "Trunk Group Properties..." You will open the Properties of the according Trunk Group. You can edit the Properties of the Trunk Group directly.

Trunk status:

If you deactivate the checkbox "Trunk enabled", this gateway is blocked for further incoming or outgoing calls.

It won't be written in the change log, if a trunk was activated or deactivated.

The "Numbers" Tab



Public Numbers assigned to this Trunk.

Country Code	Area Code	Subscriber N...	Extension N...
49	231	4777	800-999

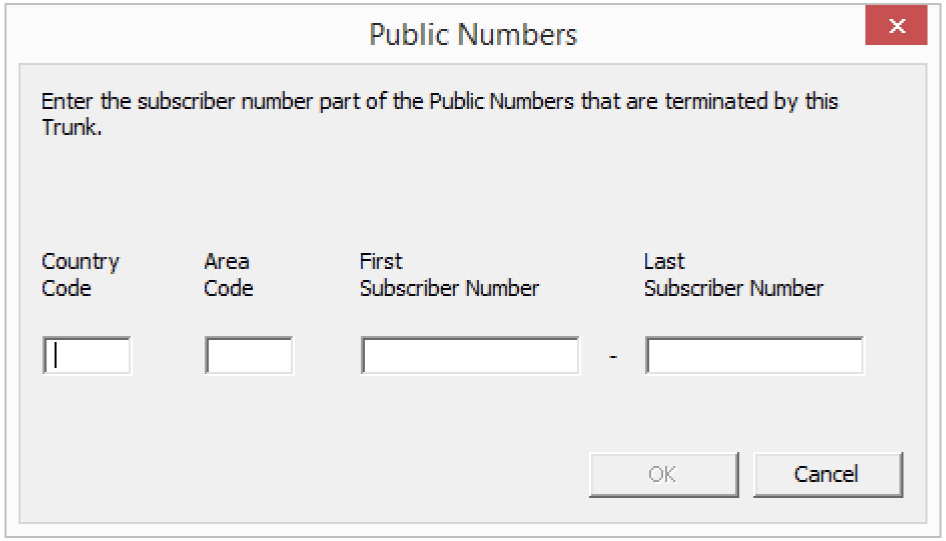
The following settings can be made:

Public numbers of this trunk

You can specify here which public numbers this trunk uses. External calls to these numbers go over this trunk. Calls with a Calling Party Number that is assigned to this trunk are routed over this trunk.

This is how you add numbers for this trunk

1 Click on "Add...".
The following window appears: "DDI numbers".



Enter the subscriber number part of the Public Numbers that are terminated by this Trunk.

2 Depending on the configuration of the trunk group, you can add numbers here:

- MSN
  If you have a line with MSNs, specify here an MSN that you want to assign to this ISDN trunk.
- DDI numbers (Direct Dialing In)
  If you have a direct dialing in line, specify the number range for this trunk here. Please specify the same number of digits in both fields (e.g. 000-599).

To ensure the unambiguity of the information, you must enter the complete phone number from SwyxWare V.13.20 onwards. In the new "Subscriber number" input field, enter the part of the phone number that follows the area code and precedes the extension (internal phone number).

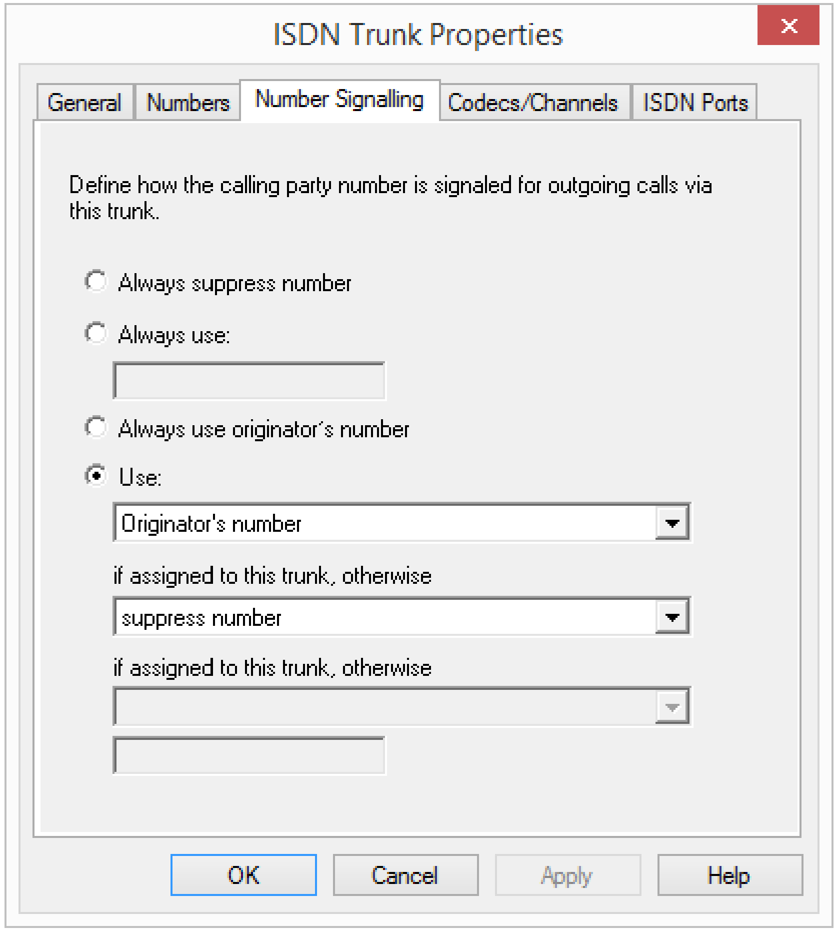
	Country code	Area code	Subscriber number	First extension	Last extension
e. g.	49	231	4777	100	200

This is how you add numbers for this trunk

The existing phone number entries are automatically extended by the new entry field "Subscriber number" when updating to V.13.20. Make sure that the automatic allocation is correct and adjust the corresponding entries manually as required.

3 End your inputs with "OK".

"Number signaling" tab



Define how the calling party number is signaled for outgoing calls via this trunk.

○ Always suppress number

○ Always use:

○ Always use originator's number

● Use:

Originator's number

if assigned to this trunk, otherwise

suppress number

if assigned to this trunk, otherwise

Here you specify whether, and how, the numbers for outgoing calls via this trunk should be signaled.

- Always suppress number
  In this case no number is signaled to the person being called (XXX), regardless of which number was configured for this trunk.

In Germany, the destination numbers 110 and 112 are reserved for emergency calls. The outgoing call number to these destination numbers is always signaled.

- Always Use This Number:
  You can specify a number or SIP-URI here which will always be signaled to the person being called (e.g. the operator's number), regardless of which number was configured for this trunk.

The number must be entered in canonical number format.

- Signal Caller Number
  Although the caller number is not configured for this trunk, the caller number is signaled to the person being called.

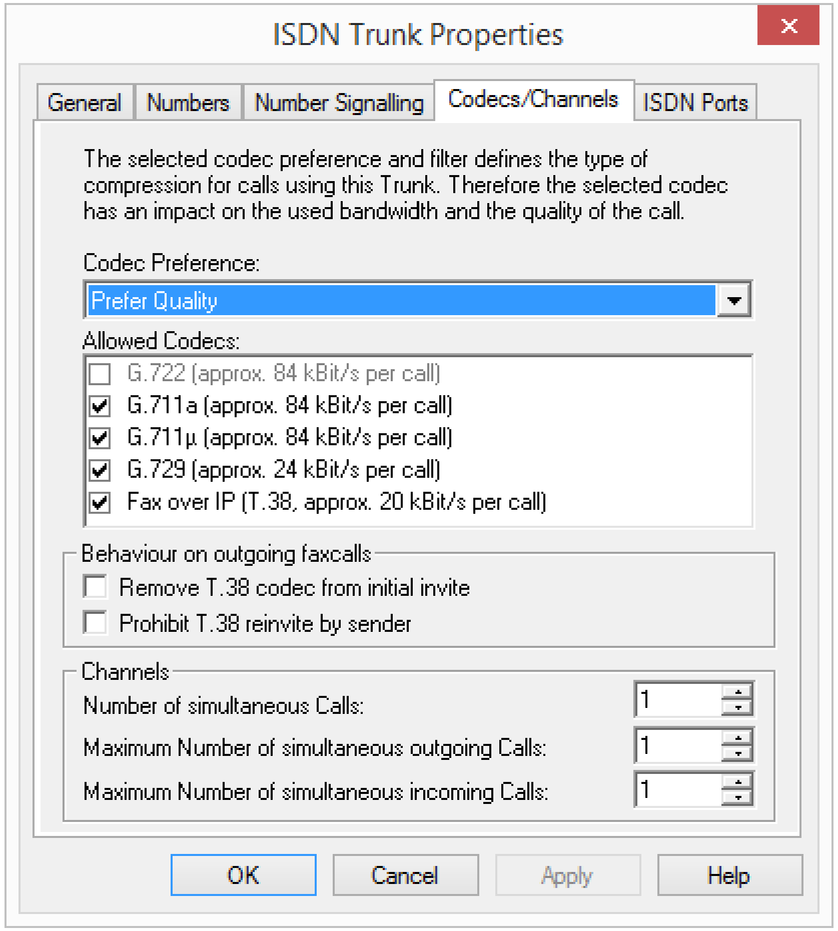
  Example:

  Customer A (number 88 333 44) calls employee B (number 55 666 77). Forwarding to his mobile phone is activated, i. e. an incoming call is routed outwards again. If the customer's number (88 333 44) should also be signaled externally, then this can be allowed here, although this number was not defined for this trunk.
- Use:
  You can specify here which number this trunk uses. You can specify the action for numbers that are assigned to this trunk as well as for numbers which have no assignment.

Use:	If assigned to this trunk, otherwise:	If assigned to this trunk, otherwise:	Entry
Origination Number	Number of the transferor		
	Hide number		
	Don't use this trunk		
	Use the following number		<Number>
Number of the transferor	Origination Number	Hide number	
		Don't use this trunk	
		Use the following number	<Number>
	Hide number		

For Number Signalling, the line characteristic "Clip no Screening" must be enabled on the line, otherwise the number is suppressed.

The "Codecs/Channels" Tab



ISDN Trunk Properties

The selected codec preference and filter defines the type of compression for calls using this Trunk. Therefore the selected codec has an impact on the used bandwidth and the quality of the call.

Codec Preference: Prefer Quality

Allowed Codecs:

- □ G.722 (approx. 84 kBit/s per call)
- ☑ G.711a (approx. 84 kBit/s per call)
- ☑ G.711µ (approx. 84 kBit/s per call)
- ☑ G.729 (approx. 24 kBit/s per call)
- ☑ Fax over IP (T.38, approx. 20 kBit/s per call)

Behaviour on outgoing faxcalls

- □ Remove T.38 codec from initial invite
- □ Prohibit T.38 reinvite by sender

Channels

Number of simultaneous Calls: 1

Maximum Number of simultaneous outgoing Calls: 1

Maximum Number of simultaneous incoming Calls: 1

The following settings can be made:

Codecs

If the Codec priority "Prefer Quality" is selected, the Codecs are provided in the sequence G.722, G.711a, G.711µ, G.729 or Fax over IP. The Codec G.722 is deactivated by default, because it would only be supported up to the ISDN gateway. Specify the filter(s) you want:

- Voice, highest bandwidth (G.722) is deactivated, as this Codec is not supported for an ISDN trunk.
- Voice, high bandwidth (G.711a, G.711µ)
  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64kbits/s.
- Voice, low bandwidth (G.729)
  High compression. A voice connection requires approximately 24kbits/s.
- Fax over IP
  In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration. A fax connection using T.38 requires approximately 20kbits/s.

If the Codec priority "Prefer low bandwidth" is selected, the Codecs sequence changes to G.729, G.722, G.711a, G.711µ, Fax over IP. The Codec G.722 is deactivated by default, because it would only be supported up to the ISDN gateway. The aim here is to use as little bandwidth as possible. Here too, specify the filter(s). G.722 is deactivated, as this Codec is not supported for an ISDN trunk.

Click on "Next>".

If there are several voice codecs selected, SwyxServer will filter voice data according to the current settings. The communicating sides will have to decide which voice codec to use.

It won't be written in the change log, if a Codec was activated or deactivated. See also *7.7 Change log*, Page 117.

Action on fax receipt

When a fax connection is set up, the T.38 protocol is negotiated between the two devices involved. Certain variants of this negotiation may not be supported by some IP adapters. Use the following filter options to establish compatibility with such devices.

- Remove T.38 codec from initial invite
  Some IP adapters cannot correctly interpret an initial connection request which includes T.38 as well as voice Codecs.
  If this option is set, SwyxServer removes T.38 from the initial connection request. The fax devices first set up a voice connection and then switch to the fax protocol T.38 because of the fax tone (CED tone, 2100Hz).
- Prohibit T.38 reinvite by sender
  The receiving fax device switches to T.38 after detecting the fax tone (CED tone, 2100Hz). Alternatively, the switch to T.38 can be carried out by the sending fax device.
  Some IP adapters don't support switching by the sender.
  If this option is set, SwyxServer suppresses a switch to T.38 by the sender.

If the receiving side involves a combined phone/fax device (fax switch), a fax data transmission is impossible when the option "Prohibit T.38 reinvite by sender" is activated.

The filter options can only be set when the Codec "Fax over IP (T.38...)" is activated.

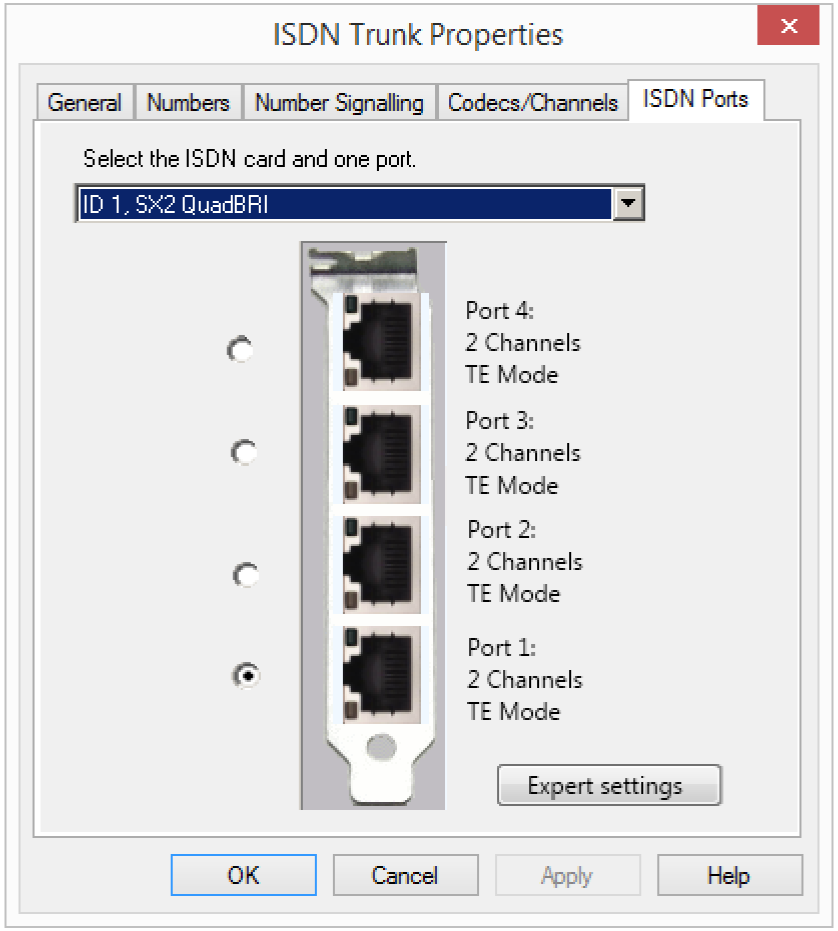
Channels

Specify how many channels (connections) should be simultaneously routed over this trunk. You can also determine how many outgoing and/or ingoing connections are established at most.

> *Example:*
>
> *You use a SX2 SinglePRI, which means that a maximum of 30 lines are available. If you configure a maximum of 10 channels for outgoing calls, then 20 lines remain free for you to be called.*

If channels were added or removed, you will find these changes in the change log. See also *7.7 Change log*, Page 117.

The "ISDN Ports" Tab


ISDN Trunk Properties

Select the ISDN card and one port.

ID 1, SX2 QuadBRI

○ Port 4: 2 Channels TE Mode

○ Port 3: 2 Channels TE Mode

○ Port 2: 2 Channels TE Mode

● Port 1: 2 Channels TE Mode

The following settings can be made:

Select ISDN card and port

Select the ISDN card from the list. According to the ISDN card, the available ports are displayed. Select the port to be used. The selection of the port is visualized with the help of a blinking LED on the ISDN card. This lets you see easily which port the ISDN connection cable must be connected to.

For information on deactivating and reactivating a trunk, please see *13.2 Activating and deactivating a trunk*, Page 237.

Please note that the available ISDN cards will only become visible within the "ISDN Ports" tab after the Swyx Gateway service is started.

Expert Settings

Further settings can be specified here. However, these should only be selected after explicit consultation with support!

15.6 INSTALLATION OF SEPARATED GATEWAYS (SWYXGATE)

In larger scenarios, e.g. with many ISDN lines, it may make sense not to operate gateways to the public telephone network (ISDN or analog lines) on the same computer on which the SwyxServer is already installed. In such an environment you can install so-called "separated gateways".

The installation of SwyxGates is similar to the installation of SwyxServer.

15.6.1 INSTALL SWYXGATE

The SwyxGate installation is part of the SwyxServer installation.

The installation of SwyxServer is carried out by a Microsoft Windows Installer file. The Windows Installer is an integral component of the Windows operating system.

If you would like to install SwyxGate separately, start the installation as described below.

Local administrator rights are required for the installation of a separate SwyxGate. The user under which the SwyxGate service is operated must be a domain user and a member in the group of SwyxWare administrators on the computer on which the SwyxServer is installed.

How to install SwyxGate

1. Close all Windows applications.
2. Put the SwyxWare DVD into your DVD ROM drive.
   The Setup program will start automatically.
   In case the setup does not start, double-click on the file autorun.exe, which is located on the SwyxWare DVD.
3. The SwyxWare Setup start page will appear.
4. Select "Install SwyxServer".
   Please follow the instructions and click on "SwyxServer".
5. Accept the license agreement.
6. Read the latest information.
7. Select here only SwyxGate as the component you would like to install.
   The field "Component Description" contains a description, the installation status and the corresponding memory space.
   - Destination Folder:
     Select the path where the chosen components should be installed. You should not change the default path unless there are very important reasons for doing so.
     For the shared files, you can enter the necessary target folder separately (the sub-directory \Share is usually used here).

   Disk cost

     With the help of "Disk cost" you can display the current disk space allocation of the available disks.
8. Start installation:
   - Installation will be carried out when you click "Next>" in this dialog. During this process the required files will be copied and the registration database entries will be made.

Complete the installation using the Configuration Wizard. See *15.6.2 Configuring SwyxGate*, Page 275.

15.6.2 CONFIGURING SWYXGATE

After the installation the Configuration Wizard starts. Use this Wizard to define the configuration parameters for the installed components.

This is how you configure SwyxGate

1. User account:
   Here you set the user account which should be used to start the SwyxWare system services (for example 'ippbx').
   In the case of a separate SwyxGate you can use as user account the same domain account that you used during the SwyxServer installation. Alternatively please use a domain account that is a member in the group of SwyxWare administrators.
   The user name should be selected by using the "Browse" button. You then only enter the password. The validity of your entries will be checked by the Setup program. This check may take several seconds. If there is an error in the entries an error message will appear and you can repeat the procedure.
2. Server name:
   Here enter the name or the IP address of your SwyxServer.
   All necessary information is passed on from the SwyxServer directly to SwyxGate.
3. After installation, set up ISDN trunks in the SwyxWare Administration. The link to SwyxGate is via the name of the computer on which the service was installed.
   See *This is how you create an ISDN Trunk*, Page 267.

15.7 UNINSTALLING

The following chapter describes how to uninstall SwyxGate and the driver software of the ISDN cards.

Uninstalling SwyxGate:

Uninstalling SwyxGate, Whereby Other Existing Components Remain

Uninstalling the SX2 Card Drivers

15.7.1 UNINSTALLING SWYXGATE:

If SwyxGate is no longer required on a computer you have the option of removing it.

Uninstalling SwyxGate, Whereby Other Existing Components Remain

If different SwyxWare components are installed on your server, and you only want to uninstall SwyxGate, you can select SwyxGate independently and uninstall it during maintenence.

This is how you uninstall SwyxGate when other components exist

1. Open the Windows Control Panel (Start | Settings | Control Panel).
2. Double-click on "Software".
3. Select the option "SwyxWare" found under "Change or Remove Program".
4. Click on "Modify".
   The installation wizard will open.
5. Click on "Next ".
6. Select the option "Modify".
7. Under SwyxGate select the option "Not available" and click on "Next".
8. Then exit the installation program.
   The Configurations Wizard will then be started.
9. After closing the Configuration Wizards, SwyxGate is uninstalled.

Please note that ISDN trunks which use this SwyxGate can no longer be operated. Change the settings of the ISDN trunk accordingly in the Swyx-Ware Administration.

15.7.2 UNINSTALLING THE SX2 CARD DRIVERS

If the ISDN SX2 cards are installed in another computer, and consequently the card drivers are no longer needed, you can uninstall them.

See also *How to update the drivers for SX2 cards*, Page 66.

This is how you uninstall the drivers for SX2 cards

1. Start the device manager on the "Hardware" tab under "Start | Settings | Control Panel | System".
2. Under "Network adapter" choose the menu item "Uninstall" in the context menu of the SX2 card.
   The drivers are then uninstalled.

16 SIP LINKS

Setting up and operating SIP trunks for the connection of the telephone system to VoIP and Internet telephony service providers

16.1 WHAT ARE SIP TRUNKS?

SIP trunks enable the use of VoIP services that are provided by carriers or service providers. The service provider provides you with a phone number or a number range. Alternatively the SwyxWare users can be assigned SIP addresses (SIP-URIs, e. g. "tom.jones@swyx.com") by the provider, which can be used as an "email address for a telephone". By this means, SwyxWare users can globally reach other SIP-URIs, and be reached themselves. If this service provider also offers gateway services, it will also be possible to reach any phone in the public telephone network via an SIP trunk and the underlying gateway of the provider.

An SIP trunk connects the software-based telephony system to a service provider, e.g. a SIP-ITSP (Internet Telephony Service Provider) or SIP provider for short (e.g. 1&1, outlook.com, GMX, etc.). Call connections are created and terminated via SIP (Session Initiation Protocol) as a communication protocol.

In SwyxWare, the connection is configured as a SIP trunk or SIP trunk group.

16.2 SCENARIO

A call can be routed via a SIP provider to another SIP client or to a number on the conventional telephone network.

The parameters required to log on to a SIP provider are configured for a trunk group. During logon, the SwyxLinkManager registers the SIP trunk with the SIP provider in order to have telephone communication with a SIP client directly via an IP route.

This registration is repeated regularly as long as the SIP provider does not have any other default settings.

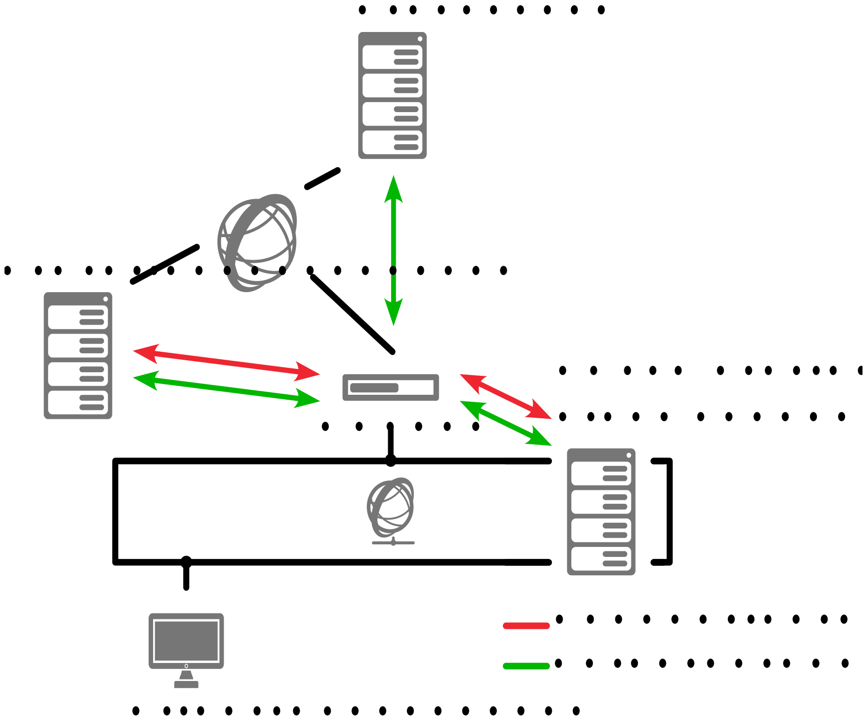


Fig. 16-1: Scenario - Call via SIP

When calling a SIP client (this can be a terminal device or a software-based telephony system), the call will be routed to the desired client via the SIP provider. As part of this process, the SwyxLinkManager is responsible for the transmission of the logon information and the voice data as well as for the creation and termination of the connection. The voice data are routed directly to the SIP client without being routed via the SIP provider.

If this SIP link calls a number in the public telephone network (PSTN), the call will first be routed to the SIP provider via the IP route and goes from there to the appropriate phone number via the public network.

Overview of Compatible SIP Providers

The knowledge base contains a list of possible SIP providers, which are compatible with SwyxWare. This list includes additional SIP provider profiles that are not included in the basic version of SwyxWare. You can read about this in the knowledge base:

SIP provider
enreach.com/products/sip-provider.html

STUN

STUN is a network protocol that recognizes the existence and type of firewalls and NAT routers and takes this information into consideration. It enables the uncomplicated use of devices (e.g. SIP telephones) and programs in networks that should receive information from the Internet.

STUN helps to identify the current public IP address of the line. This is necessary in order for the opposite terminal to correctly address and return your call data.

See RFC Standard (RFC 3489).

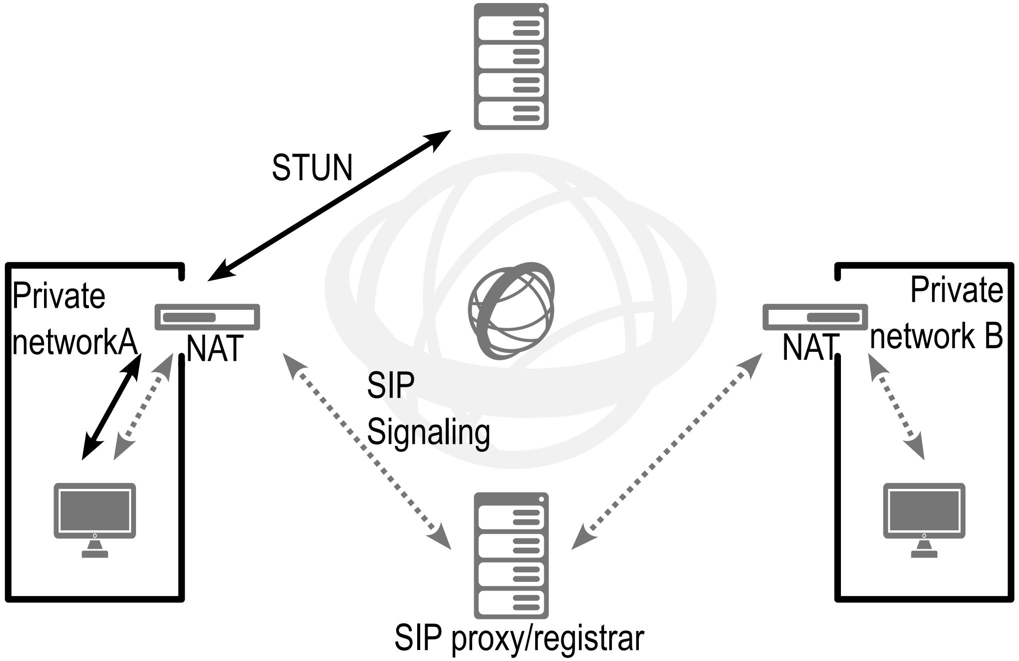


Fig. 16-2: STUN

STUN messages are sent by the SwyxLinkManager at least every 10 seconds as long as there is no other data traffic circulating via the corresponding port. This ensures that the NAT router's NAT table (masquerading) cannot be destroyed again and that changes to the external IP address of the NAT router can be transmitted. This means that SwyxWare SIP trunks can also be operated with a DSL connection that is terminated every 24 hours by the IP provider and thus receives a new IP address.

Therefore, STUN messages, SIP logon, the SIP connection creation, and the voice data are sent via the NAT router.

If a firewall exists, it must be disabled for this type of communication. The rules required are described below and must be configured in the appropriate syntax in your firewall.

- Sending STUN messages
  The SwyxLinkManager sends STUN messages from port 65002 to the configured STUN server. The destination port for STUN messages is usually port 3478, but there are exceptions, e. g., SIPGate uses port 10000.
- Receiving STUN messages
  STUN response messages should also be permitted.
- SIP messages
  SIP messages are sent by the SwyxLinkManager from port 65002 to the SIP port of the SIP provider. The SIP port is usually the well-known port 5060. The return route for the responses should also be enabled.

Please note that when using a NAT router, port forwarding must be configured so that the SIP messages, which are received on the public IP address of the NAT router on port 5060 are also forwarded to the SwyxLinkManager on port 65002 in the internal network.

16.3 CREATING A SIP TRUNK GROUP

We recommend creating a SIP trunk group before creating a SIP trunk.

General parameters such as permissions, location and routings are specified in this group. When creating a trunk, you then simply assign the trunk group to the trunk. As a member of the group, the trunk is thus given the corresponding parameters.

How to create a SIP trunk group

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunk Groups" and select the entry "Add Trunk Group..." in the context menu.
The "Add Trunk Group..." wizard will appear.

3 Click on "Next>".

4 Name and description of the trunk group:
Enter the name of the trunk group, and a description.
Click on "Next>".

5 Type of trunk group:
Enter the type of trunk group here, in this case "SIP".

6 Enter the profile for this trunk group in the lower field "Profile". If your provider does not appear in the list, select "Customized".
See *16.3.1 Profile of a SIP Trunk Group*, Page 281.
Click on "Next >".

If you select a predefined profile, the corresponding provider parameters will be set automatically. Configuration steps (7) "SIP settings (registration)" to (10) "Settings for the STUN server" are redundant.

7 SIP settings (registration)
You can obtain the parameters required for the SIP connection from your SIP provider. Proceed as follows to enter them.
If the SIP provider only permits registered connections, check the "Activate SIP registration" box and enter the name of the registrar or the IP address, along with the mapped port. The registrar is the address to which the REGISTER messages are sent.

The port must match the selected transport protocol. Leave the filed empty if you did not receive information on the port by your provider. The port is determined via DNS query.

Enter the time after which registration must be repeated (usually two minutes) under "Re-registration interval".
Click on "Next>".

8 SIP settings
Your SIP provider will provide the following parameters:
Proxy:
Enter the name or IP address of the SIP proxy and, if applicable, the mapped port. Here, the proxy is the provider's server, which sets up and terminates the connection.
Realm:
Enter the general component of the SIP address here. This is used to create your individual SIP-URI.
Example:

Your SIP provider is outlook.com. In this case, enter "outlook.com" as the realm here. Your SIP-URI will then comprise the individual component, e.g., "tom.jones" and the realm. Your SIP-URI will, therefore, be:

tom.jones@outlook.com

DTMF method:

This mode defines how the provider proceed with the keyboard input of a user during a call (DTMF signaling).

You can choose from a variety of options:

- None. DTMF signalization is deactivated
- RFC2833_Event: RFC2833_Event: DTMF signalization, based on the event mechanism described in RFC2833, will be used.
- Info Method DTMF Relay DTMF signalling as recommended by Cisco (applicationtype DtmfRelay) will be used

Click on "Next>".

9 Transport protocols and encryption
Select a transport protocol and, if applicable, the encryption mode.

Make sure that the selected transport protocol is supported by your provider.

See also *13.1.4 The "Encryption" tab of the SIP Trunk Group*, Page 233.

10 Settings for the STUN server
A STUN server can be used to identify the IP address of the line. Supports your provider STUN, so please enter the name or the IP address of the STUN server of your provider and the appropriate port.
If you would like to use STUN, although you have not received any STUN server information from the provider, you can use the free STUN server "stunserver.org" with port "3478".
Click on "Next>".

11 Definition of routing:
Specify for which calls this Trunk Group should be used. When entering call numbers or URIs you can use placeholders (*), e.g. "+*" for all external numbers or "*" for all internal numbers. Multiple numbers/URIs are separated by a semicolon. You have several different options:

- for all external calls
- only for external calls to the following destination number or SIP-URI
- for all external calls and all unassigned internal numbers
- For the following internal numbers
- Create no routing records for the moment

Click on "Next>".

12 Call Permission
Specify the Calling Rights profile for the Trunk Group. This Calling Rights profile applies to the incoming calls over this Trunk Group.
For further information please refer to sectionCall permission of a trunk group
Click on "Next >".

13 Location profile:
Define the location. This profile also includes the definition of e.g. country code and public line access.
Click on "Next>".

14 Click "Finish".
The new SIP trunk group is created, and is available for further configuration.

For changing the SIP Trunk Group properties subsequently, see *13.1 Configure trunk groups*, Page 227.

16.3.1 PROFILE OF A SIP TRUNK GROUP

SwyxWare offers numerous predefined profiles.

If you select a predefined profile, the corresponding provider parameters will be set automatically. If the parameters do not match your settings or your provider is not listed, you can change these parameters in the trunk group properties once you have created the trunk group.

See *13.1.3 The "SIP" Tab of the SIP Trunk Group*, Page 232.

Please contact your specialist dealer for an overview of compatible SIP providers and the functions they offer in relation to SwyxWare.

When you create the SIP trunk group on a UC tenant (SwyxON), the corresponding selection list contains only those profiles that are supported by SwyxON.

The Enreach knowledge base contains a related entry, which is constantly updated. Simply visit:

SIP provider
enreach.com/products/sip-provider.html

16.4 CREATING A SIP TRUNK

Once you have the information you need from your provider in respect of the SIP connection and a SIP trunk group has been set up, you can proceed to create SIP trunks.

The SwyxLinkManager service, which is responsible for linking SIP lines, is automatically installed with the standard version of the SwyxServer software.

The administration of a SIP trunk is handled with the SwyxWare Administration. Please start SwyxWare Administration as described in *7.1 Registration on SwyxWare Administration*, Page 80. If you are not yet connected to this server, please connect now as described in *How to connect to a SwyxServer*, Page 83.

How to create a SIP trunk

1. Open the SwyxWare Administration and choose the SwyxServer.
2. In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunks" and select the entry "Add Trunk..." in the context menu.
3. An "Add new Trunk Wizard" opens up.
   Click on "Next>".
4. Trunk name:
   Enter a name and a short description for the new trunk here.
   Click on "Next>".
5. Selection of a trunk group:
   Select the trunk group here to which this trunk should be assigned.
   General settings such as routings, rights and location-specific parameters are specified in the trunk group. You can use "New Trunk Group..." to create a new trunk group, and then continue with the creation of a trunk.
   See also *How to create a SIP trunk group*, Page 280.
   Click on "Next >".
6. SIP trunk provider/User data
   Enter the user data you obtained from your SIP provider here.
   SIP provider
   This is purely an information field (the SIP provider is defined in the configuration of the trunk group).
   User ID:
   The user ID is combined with the realm to create the SIP address (URI).
   User name and password:
   The user name and password are required for user authentication.
7. Numbers:
   Please enter the Public Numbers to be routed by this Trunk..
   If your provider has configured several numbers or ranges of numbers for you, enter only one number or one range here, and add the others subsequently in the trunk properties (*The "Numbers" Tab*, Page 285).
8. SIP-URI
   Enter the SIP addresses (URIs) to be managed by this trunk here. A SIP has the following format:
   SIP:<Name 1>@<Name 2>
   where <Name 1> represents the user name and <Name 2> the realm. Although the realm is set by default when the trunk group is selected, it can be overwritten individually here.
   To make things easier, you can use '*' as a placeholder, e.g., enter '*@company.com' for all users with the realm 'company.com'.
9. Codecs:
   With the help of the Codec you select how the voice is compressed for transmission. The following options are available:

If the Codec priority "Prefer Quality" is selected, the Codecs are provided in the sequence G.722, G.711a, G.711µ, G.729 or Fax over IP. Specify the filter(s) you want:

- Voice, highest bandwidth (G.722)
  HD quality
- Voice, high bandwidth (G.711a, G.711µ)
  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64kbits/s.
- Voice, low bandwidth (G.729)
  High compression. A voice connection requires approximately 24kbits/s.
- Fax
  In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration. A fax connection using T.38 requires approximately 20kbits/s.

If the Codec priority "Prefer low bandwidth" is selected, the Codecs sequence changes to G.729, G.722, G.711a, G.711µ, Fax over IP. The aim here is to use as little bandwidth as possible. Here too, specify the filter(s).

Click on "Next>".

10 Voice channels:
Enter how many calls may be routed via this trunk at the same time.
Using a SIP trunk, the provider will define how many connections at the same time will be possible. The maximum number of channels will be defined by the bandwidth to the provider and the Codec settings (i. e. the bandwidth per call).

11 Computer name:
Enter the name of the computer on which the SwyxLinkManager is managed. Use the name of the computer as it appears in the computer properties.

12 Click "Finish".
The new Trunk is created, and is available for further configuration.

For changing the SIPTrunk properties subsequently, see *16.5 Configuring a SIP Trunk*, Page 283.

16.5 CONFIGURING A SIP TRUNK

When you have created a SIP trunk as described in 16Creating a SIP Trunk, Page 282, you can subsequently change the settings of this trunk in the SwyxWare Administration.

When parameters of a trunk are changed, this change takes effect at once. There is no need to halt and restart any services for this.

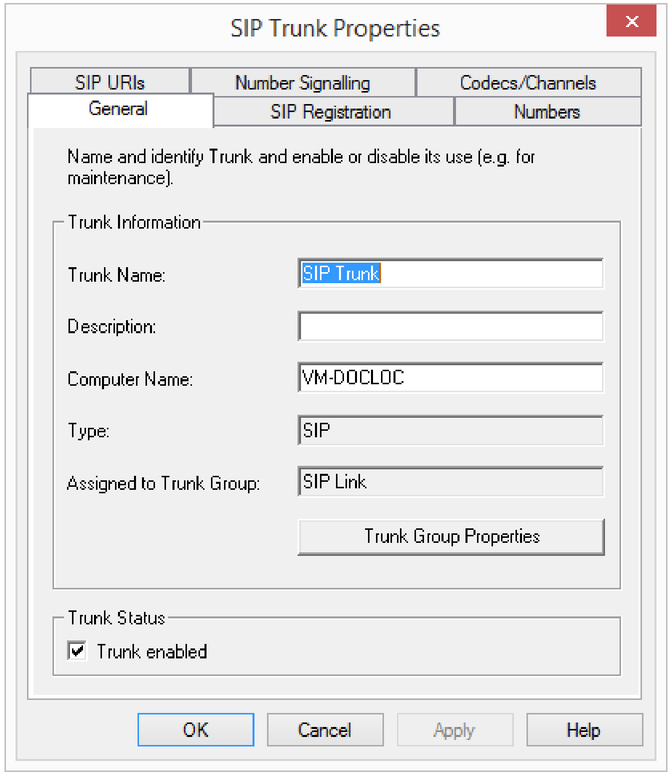
How to configure a SIP trunk

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click on "Trunks", and in the right-hand window select the trunk you want to configure.

3 In the context menu, select "Properties".
In each case, the "Properties of..." window will appear.

The "General" Tab



Name and identify Trunk and enable or disable its use (e.g. for maintenance).

Trunk Information

Trunk Name: SIP Trunk

Description:

Computer Name: VM-DOCLOC

Type: SIP

Assigned to Trunk Group: SIP Link

Trunk Status

☑ Trunk enabled

In this tab you can modify the name and description of the trunk.

Trunk information:

In the fields "Trunk Name" and "Description" you will find the descriptive information that is displayed in Administration.

The field "Computer Name" contains the name of the computer in which the service (SwyxLinkManager or SwyxGate) is installed.

The "Type" field indicates the type of the trunk, and "Trunk Group" the assigned Trunk Group. Both parameters cannot be retrospectively changed.

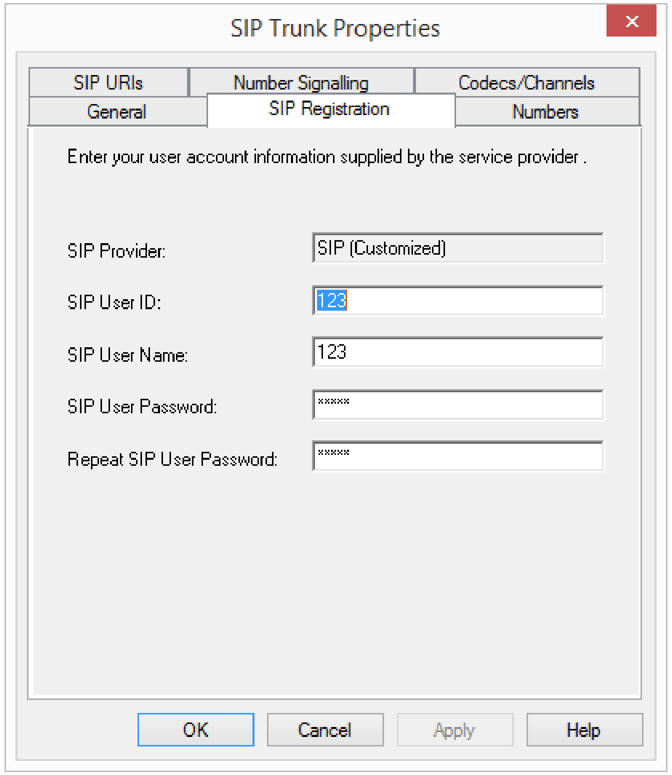
Using "Trunk Group Properties..." You will open the Properties of the according Trunk Group. You can edit the Properties of the Trunk Group directly.

Trunk status:

If you deactivate the checkbox "Trunk enabled", this gateway is blocked for further incoming or outgoing calls.

It won't be written in the change log, if a trunk was activated or deactivated.

The "SIP Registration" Tab



Enter your user account information supplied by the service provider .

SIP Provider: SIP (Customized)

SIP User ID: 123

SIP User Name: 123

SIP User Password: *****

Repeat SIP User Password: *****

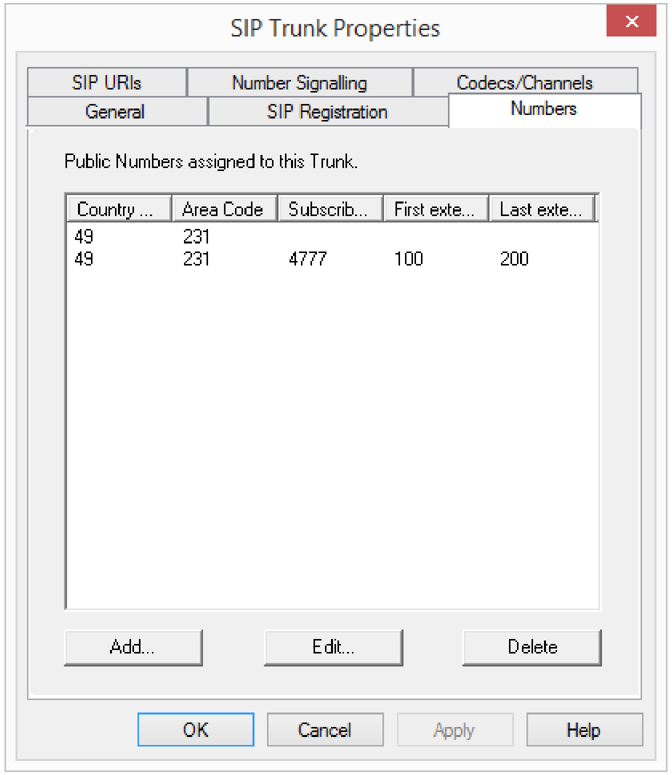
The registration data of the SIP provider to which this SIP trunk is establishing a connection appears on this tab.

The "SIP Provider" field is simply an information field (the SIP provider is defined in the configuration of the associated trunk group).

The access parameters defined specifically for this trunk appear under "User ID", "User Name" and "User Password". Your SIP provider will provide the corresponding parameters.

Note: Most SIP providers enter only a user name and no user ID. In this case, enter the user name in both fields.

The "Numbers" Tab



Public Numbers assigned to this Trunk.

Country ...	Area Code	Subscrib...	First exte...	Last exte...
49	231			
49	231	4777	100	200

The following settings can be made:

Public numbers of this trunk

You can specify here which public numbers this trunk uses. External calls to these numbers go over this trunk. Calls with a Calling Party Number that is assigned to this trunk are routed over this trunk.

To ensure the unambiguity of the information, you must enter the complete phone number from SwyxWare V.13.20 onwards. In the new "Subscriber number" input field, enter the part of the phone number that follows the area code and precedes the extension (internal phone number).

	Country code	Area code	Subscriber number	First extension	Last extension
e. g.	49	231	4777	100	200

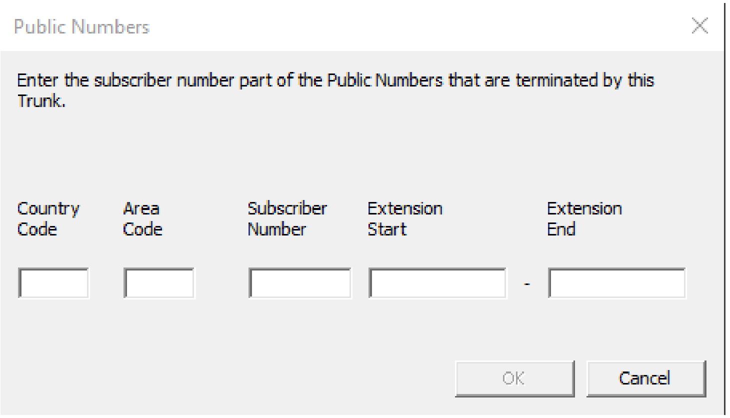
This is how you add numbers for this trunk

The existing phone number entries are automatically extended by the new entry field "Subscriber number" when updating to V.13.20. Make sure that the automatic allocation is correct and adjust the corresponding entries manually as required.

SIP URIs see *10.1.3 SIP-URIs*, Page 147.

This is how you add numbers for this trunk

1 Click on "Add...".
The following window appears: "Numbers".



Public Numbers

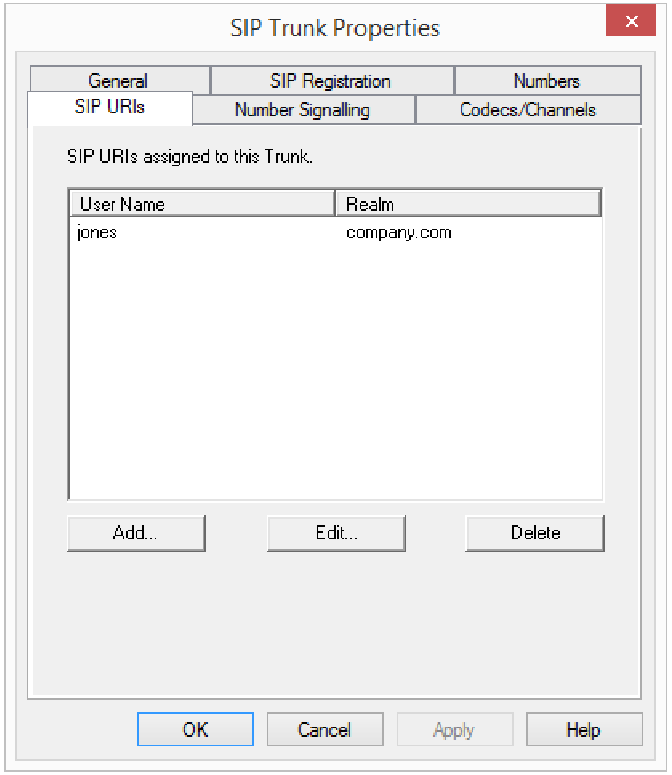
Enter the subscriber number part of the Public Numbers that are terminated by this Trunk.

2 You can add either an individual number or a range of numbers.

3 End your inputs with "OK".

To add several numbers or ranges, simply select "Add" the relevant number of times.

The "SIP-URIs" Tab



SIP Trunk Properties

SIP URIs assigned to this Trunk.

User Name	Realm
jones	company.com

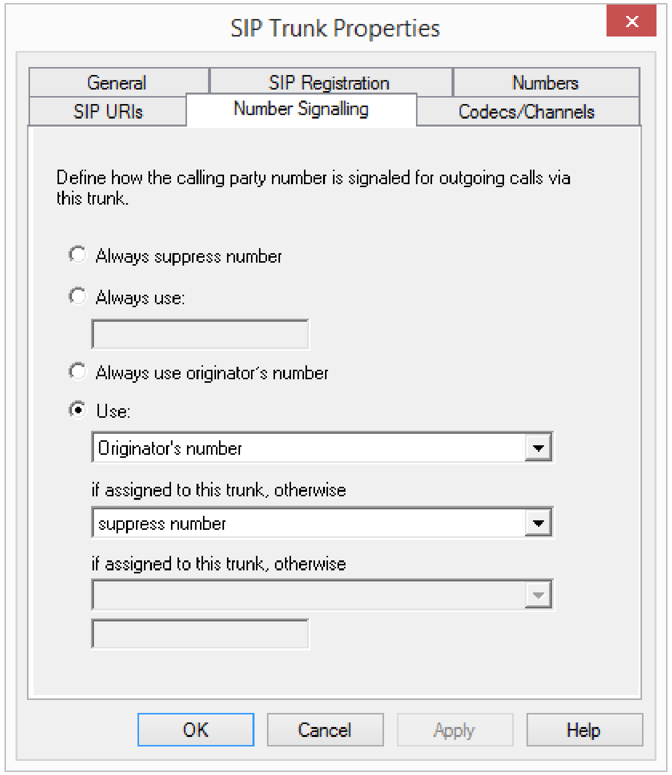
The following settings can be made:

A list of SIP-URIs mapped to this trunk appears here.

Click on "Add" to enter more SIP-URIs. To edit or delete a SIP-URI, highlight it in the list.

"Number signaling" tab

Here you specify whether, and how, the numbers for outgoing calls via this trunk should be signaled.



SIP Trunk Properties

General | SIP Registration | Numbers
SIP URIs | Number Signalling | Codecs/Channels

Define how the calling party number is signaled for outgoing calls via this trunk.

○ Always suppress number

○ Always use:

○ Always use originator's number

● Use:

Originator's number

if assigned to this trunk, otherwise

suppress number

if assigned to this trunk, otherwise

- Always suppress number
  In this case no number is signaled to the person being called (XXX), regardless of which number was configured for this trunk.

In Germany, the destination numbers 110 and 112 are reserved for emergency calls. The outgoing call number to these destination numbers is always signaled.

- Always Use This Number:
  You can specify a number or SIP-URI here which will always be signaled to the person being called (e.g. the operator's number), regardless of which number was configured for this trunk.

The number must be entered in canonical number format.

- Signal Caller Number
  Although the caller number is not configured for this trunk, the caller number is signaled to the person being called.

  Example:

  Customer A (number 88 333 44) calls employee B (number 55 666 77). Forwarding to his mobile phone is activated, i. e. an incoming call is routed outwards again. If the customer's number (88 333 44) should also be signaled externally, then this can be allowed here, although this number was not defined for this trunk.

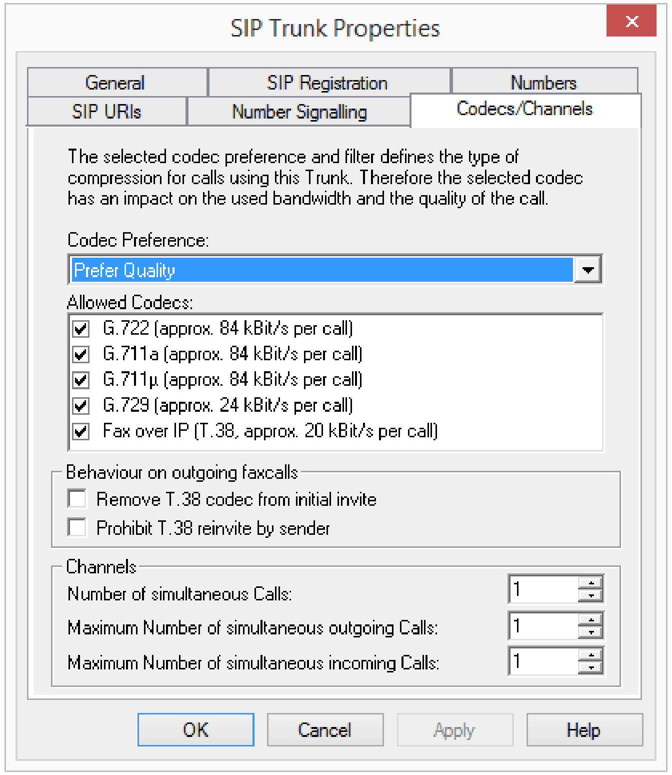
- Use:
  You can specify here which number this trunk uses. You can specify the action for numbers that are assigned to this trunk as well as for numbers which have no assignment.

Use:	If assigned to this trunk, otherwise:	If assigned to this trunk, otherwise:	Entry
Origination Number	Number of the transferor		
	Hide number		
	Don't use this trunk		
	Use the following number		<Number>
Number of the transferor	Origination Number	Hide number	
		Don't use this trunk	

Use:	If assigned to this trunk, otherwise:	If assigned to this trunk, otherwise:	Entry
		Use the following number	<Number>
	Hide number		

For Number Signalling via a SIP trunk, the provider must support the feature "ClipNoScreening". For further information see Support of the feature ClipNoScreening on SIP trunks https://service.swyx.net/hc/en-gb/articles/360000011599-Support-of-feature-ClipNoScreening-for-SIP-trunks (You may need to be logged in to view the content).

The "Codecs/Channels" Tab



SIP Trunk Properties

The selected codec preference and filter defines the type of compression for calls using this Trunk. Therefore the selected codec has an impact on the used bandwidth and the quality of the call.

Codec Preference: Prefer Quality

Allowed Codecs:

- ☑ G.722 (approx. 84 kBit/s per call)
- ☑ G.711a (approx. 84 kBit/s per call)
- ☑ G.711µ (approx. 84 kBit/s per call)
- ☑ G.729 (approx. 24 kBit/s per call)
- ☑ Fax over IP (T.38, approx. 20 kBit/s per call)

Behaviour on outgoing faxcalls

- □ Remove T.38 codec from initial invite
- □ Prohibit T.38 reinvite by sender

Channels

Number of simultaneous Calls: 1

Maximum Number of simultaneous outgoing Calls: 1

Maximum Number of simultaneous incoming Calls: 1

The following settings can be made:

Codecs

Here you can define the type of compression to be used on this connection.

If the Codec priority "Prefer Quality" is selected, the Codecs are provided in the sequence G.722, G.711a, G.711µ, G.729 or Fax over IP. Specify the filter(s) you want:

- Voice, highest bandwidth (G.722)
  HD quality

- Voice, high bandwidth (G.711a, G.711µ)
  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64kbits/s.
- Voice, low bandwidth (G.729)
  High compression. A voice connection requires approximately 24kbits/s.
- Fax over IP
  In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration. A fax connection using T.38 requires approximately 20kbits/s.

If the Codec priority "Prefer low bandwidth" is selected, the Codecs sequence changes to G.729, G.722, G.711a, G.711µ, Fax over IP. The aim here is to use as little bandwidth as possible. Here too, specify the filter(s).

Click on "Next>".

If there are several voice codecs selected, SwyxServer will filter voice data according to the current settings. The communicating sides will have to decide which voice codec to use.

It won't be written in the change log, if a Codec was activated or deactivated. See also *7.7 Change log*, Page 117.

Action on fax receipt

If the T.38 protocol is negotiated for the establishment of a fax connection between the devices involved, certain variants of this negotiation may possibly not be supported by some IP adapters. Use the following filter options to establish compatibility with such devices.

- Remove T.38 codec from initial invite
  Some IP adapters cannot correctly interpret an initial connection request which includes T.38 as well as voice Codecs.
  If this option is set, SwyxServer removes T.38 from the initial connection request. The fax devices first set up a voice connection and then switch to the fax protocol T.38 because of the fax tone (CED tone, 2100Hz).
- Prohibit T.38 reinvite by sender
  The receiving fax device switches to T.38 after detecting the fax tone (CED tone, 2100Hz). Alternatively, the switch to T.38 can be carried out by the sending fax device.
  Some IP adapters don't support switching by the sender.
  If this option is set, SwyxServer suppresses a switch to T.38 by the sender.

If the receiving side involves a combined phone/fax device (fax switch), a fax data transmission is impossible when the option "Prohibit T.38 reinvite by sender" is activated.

The filter options can only be set when the Codec "Fax over IP (T.38...)" is activated.

16.6 SENDING FAXES VIA SIP CONNECTION

You can also send faxes via a SIP connection. To do this, your SIP provider must offer the T.38 standard used or G.711 by SwyxWare.

You will need to set up a dedicated SIP trunk, which is mapped to the SIP trunk group of this provider, but has the codec "Fax over IP (T.38, around 20 kbit/s per call)" (*The "Codecs/Channels" Tab*, Page 288).

16.7 CONFIGURING THE FIREWALL FOR A SIP TRUNK

The SwyxLinkManager is responsible for logon to the SIP provider, the creation of the SIP connection and the forwarding of external voice data. The firewall must be configured appropriately in order for the SwyxLinkManager to be able to communicate with SIP providers and opposite terminals on the public Internet.

The following example will illustrate how to configure the firewall:

In order to do this, the SwyxLinkManager and SwyxServer must be installed on the same computer.

The SwyxServer is located on the local network and, therefore, has a private IP address (e.g., 192.168.100.5). The employee workstations running Desktop Clients and SwyxPhones are also located in this private IP address range (192.168.100.x). The route from the private IP range to the Internet runs via an NAT (Network Address Translation) router, which also acts as a firewall. This NAT router is on the one hand within the private IP address range (e.g. 192.168.100.1) and on the other hand within the public Internet IP network (e.g. 217.194.238.2).

SwyxWare supports the NAT types "Full Cone NAT", "Restricted Cone NAT" and "Port Restricted Cone NAT".

In general, the communication from the private IP address range functions in such a way that the NAT router is used to create a connection into the Internet and, for example, the webserver reached while surfing only sees the public IP address of the NAT router (217.194.248.2) and it sends its answers or the web contents to this public IP address only. The NAT router has a table in which it records the connections made by clients from the private IP range to the Internet and which it uses to route the responses from the public range back to the clients in the private IP address range. This table consist primarily of entries in which the private IP address and the port of the client are associated with the public IP address and the port of the NAT router for a connection via the NAT router into the Internet. In this manner, responses from the Internet can be forwarded to the NAT router and from this router to the corresponding client. This connection is only maintained for a matter of seconds, depending on the router.

The use of SIP in connection with firewalls or NAT is rather complex, because most firewalls/NAT routers cannot assign the dynamically-mapped ports to the signaling connection. In this context, the network protocol STUN can be of help.

STUN

STUN is a network protocol that recognizes the existence and type of firewalls and NAT routers and takes this information into consideration. It enables the uncomplicated use of devices (e.g. SIP telephones) and programs in networks that should receive information from the Internet.

STUN helps to identify the current public IP address of the line. This is necessary in order for the opposite terminal to correctly address and return your call data.

For more information on the STUN protocol, please see the corresponding RFC standard (RFC 3489).

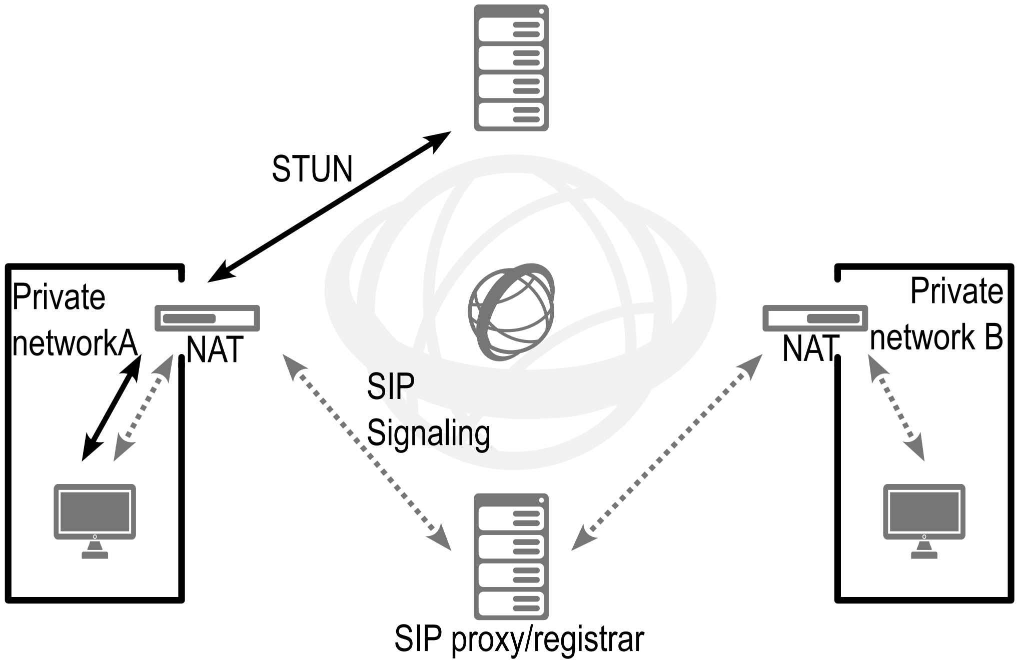


Fig. 16-3: SIP/STUN

The STUN messages are sent by SwyxLinkManager at least every 10 seconds (provided no other data traffic flows via the corresponding port) to ensure that the NAT (masquerading) table of the NAT router is not destroyed again and to detect potential changes to the external IP address of the NAT router. This means that the SIP links of SwyxWare can also be operated behind a DSL connection that is terminated every 24 hours by the IP provider and thus receives a new IP address.

Therefore, STUN messages, SIP logon, the SIP connection creation, and the voice data are sent via the NAT router.

If a firewall exists, it must be disabled for this type of communication only. The rules required for this are described below and must be configured in the appropriate syntax in your firewall.

The SwyxLinkManager sends STUN messages from port 65002 to the configured STUN server. The destination port for STUN messages is usually port 3478 but there are exceptions, e.g. SIPGate uses port 10000.

STUN response messages should also be allowed. SIP messages are sent by the SwyxLinkManager from port 65002 to the SIP port of the SIP provider. The SIP port is usually the well-known port 5060. The return route for the responses should also be enabled.

The SwyxLinkManager uses ports 55000-56000 for sending and receiving voice data on the Internet. The destination address and the destination port cannot be limited in advance because this is solely dependent on the SIP opposite terminal, which is unknown (e.g., X-Lite Client, GMX Netphone or similar).

The reverse direction must also be cleared. This results in the following set of rules for the firewall:

- Clearance for sending UDP, STUN and SIP messages as well as audio packets from the IP address and ports 55000-56000 and 65002 of the SwyxLinkManager to STUN port 3478 of any STUN server and SIP port 5060 of a SIP provider (e. g., IP: 192.168.100.5, Port: 55000 - 56000, 65002=">" IP: [STUN Server]/[Proxy Server], Port: 3478, 5060).
- Enabling of receipt of UDP, SIP and STUN messages at port 65002 of the SwyxLinkManager.

  Example:

  IP: [STUN server]/[Proxy server], port: any = ">" IP:192.168.100.5, port: 65002
- Enabling of outgoing voice data of the SwyxLinkManager.

  Example:

  IP:192.168.100.5, Port: 55000 - 56000 = ">" IP: any, port: any
- Enabling of incoming voice data to the SwyxLinkManager.

  Example:

  IP: any, port: any = ">", IP: 192.168.100.5, Port: 55000 - 56000

The above rules can also be formulated in a different way. However, this model is appropriate if your firewall supports QoS for the audio data streams (as with e.g. LANCOM routers/firewalls).

17 SWYXLINK (SERVER-SERVER CONNECTION)

Setting up and operating SwyxLinks to connect SwyxServers via IP links.

A SwyxLink trunk must be configured separately but consistently on each of the two SwyxServers involved in the process. The configuration of a connection takes place locally on one side and remotely on the other side. The service SwyxLinkManager must be active on the local side.

In order to guarantee error-free operation, the following settings must correspond on both sides of the SwyxLink:

- Trunk name
- SIP user ID within the "SIP Registration" tab
- Codecs
- Max. number of Concurrent Calls
- Type of Intersite connection (in the same organization, from another organization or without any presence interaction)

The following parameters must be configured differently on both sides:

- Managed
- Remote Server
- Numbers

The administrator must guarantee the consistency of the configuration data on both sides of a SwyxLink trunk.

Creating a SwyxLink Trunk Group

Creating a SwyxLink Trunk

Configuring a SwyxLink Trunk

Properties of the SwyxLink Connection

17.1 THE BASICS

Prior to the server-server link there is a SwyxServer and a trunk (in this case SwyxGate) in each location (London and Liverpool) with the assigned SwyxWare users. Both locations function completely independently and can only contact one another via the public telephone network (ISDN). The SwyxServer in Liverpool only recognizes the SwyxWare users in Liverpool, the London SwyxServer only recognizes the SwyxWare users in London.

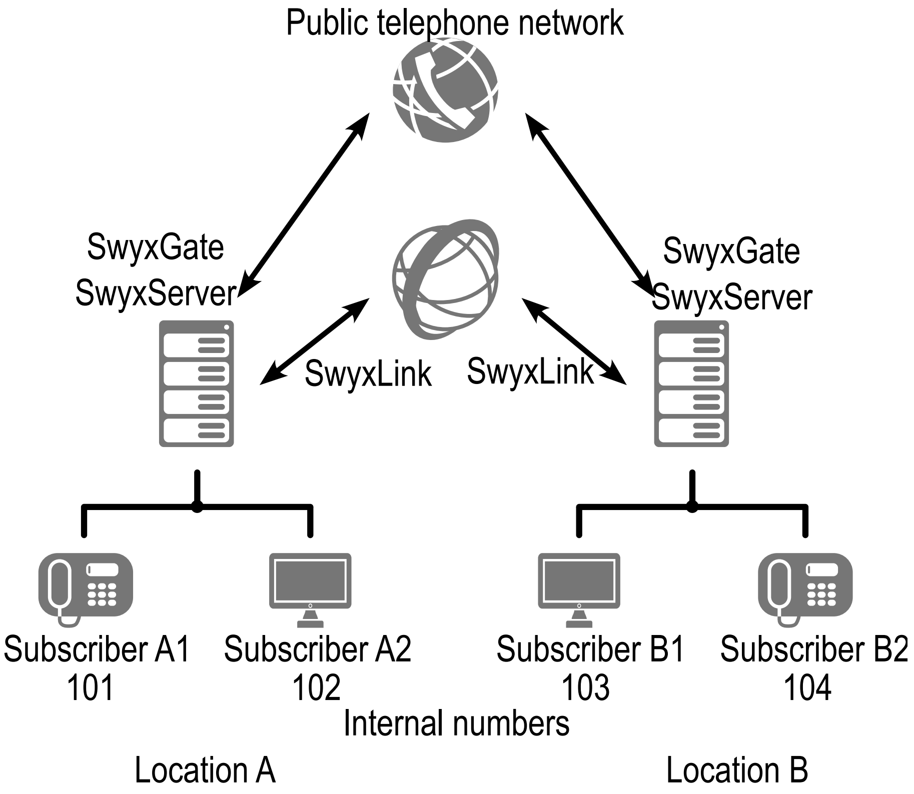


Fig. 17-1: Connection of locations in server-server link

The two existing SwyxServers can be linked with one another, i.e., a connection is established, which is represented by a SwyxLink Trunk at each location. If a number belonging to the Liverpool location is dialed in London, it will now be recognized by the SwyxServer as one of the Liverpool numbers. The call will then be directly established using the IP connection.

The configuration of an "Intersite connection" within the SwyxLink trunk means that status information ("Available", "Away", "Logged off", "Do Not Disturb", "Speaking") can now be exchanged between users who are logged in to different servers. Furthermore, users logged-on to different serves may now also communicate via the Collaboration, Video and Instant Messaging features. The relationships within the user and group properties can be used, following the trunk configuration, to define which users/groups on other servers should be signaled about the status. This configuration also makes the users visible in the respective Global Phonebook of the connected SwyxServer.

Detailed scenarios are used to explain the concept of location linking in *26.3 Linking of two locations (head office and branch)*, Page 389. In this section, you will also find more detailed examples for the individual parameters used.

17.2 CREATING A SWYXLINK TRUNK GROUP

We recommend creating a SwyxLink trunk group before creating a SwyxLink trunk.

General parameters such as permissions, location and routings are specified in this group. When creating a trunk, you then simply assign the trunk group to the trunk. As a member of the group, the trunk is thus given the corresponding parameters.

How to create a SwyxLink trunk group

1. Open the SwyxWare Administration and choose the SwyxServer.
2. In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunk Groups" and select the entry "Add Trunk Group..." in the context menu.
   The "Add Trunk Group..." wizard will appear.
3. Click on "Next>".
4. Name and description of the trunk group:
   Enter the name of the trunk group, and a description.
   Click on "Next>".
5. Type of trunk group:
   Enter the type of trunk group here, in this case "SwyxLink".
   The profile will then also be for "SwyxLink".
   Click on "Next>".
6. Definition of routing:
   Specify for which calls this Trunk Group should be used. When entering call numbers or URIs you can use placeholders (*), e.g. "+*" for all external numbers or "*" for all internal numbers. Multiple numbers/URIs are separated by a semicolon. You have several different options:
   - for all external calls
   - only for external calls to the following destination number or SIP-URI
   - for all external calls and all unassigned internal numbers
   - For the following internal numbers
   - Create no routing records for the moment

   Click on "Next>".
7. Call Permission
   Specify the Calling Rights profile for the Trunk Group. This Calling Rights profile applies to the incoming calls over this Trunk Group.
   See also *Call permission of a trunk group*, Page 129.
   Click on "Next>".
8. Location profile:
   Define the location. This profile also includes the definition of e.g. country code and public line access.
   Click on "Next>".
9. Click "Finish".

The new SwyxLink trunk group is created, and is available for further configuration.

For changing the SwyxLink Trunk Group properties subsequently, see *17.4 Configuring a SwyxLink Trunk*, Page 296.

17.3 CREATING A SWYXLINK TRUNK

In order to make an additional SwyxServer available within SwyxWare, you can configure a SwyxLink trunk in the SwyxWare Administration. Each SwyxLink trunk represents a connection to a SwyxServer with the parameters configured for this purpose.

The SwyxLinkManager service, which is responsible for linking SwyxLink lines, is automatically installed with the standard version of the SwyxServer software.

The administration of a SwyxLink trunk is handled with the SwyxWare Administration. Please start SwyxWare Administration as described in *7.1 Registration on SwyxWare Administration*, Page 80. If you are not yet connected to this server, please connect now as described in *How to connect to a SwyxServer*, Page 83.

How to configure a new SwyxLink trunk

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunks" and select the entry "Add Trunk..." in the context menu.

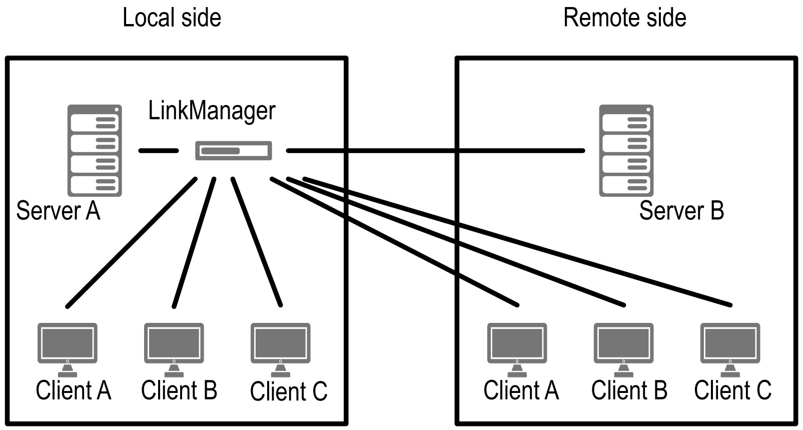
3 An "Add new Trunk Wizard" opens up.
Click on "Next>".

4 Trunk name:
Enter a name and a short description for the new trunk here.
Click on "Next>".

5 Selection of a trunk group:
Select the trunk group here to which this trunk should be assigned. General settings such as routings, rights and location-specific parameters are specified in the trunk group. You can use "New Trunk Group..." to create a new trunk group, and then continue with the creation of a trunk.
See also *How to create a SwyxLink trunk group*, Page 293.
Click on "Next >".

6 SwyxLink trunk:
Each inter-location connection is managed by exactly one SwyxLinkManager. If you would like to manage the SwyxLink on this side of the connection, select "Locally managed SwyxLink trunk". This SwyxLink must then be configured on the other side as "Remotely managed".
Click on "Next >".

7 Select remote SwyxServer (when locally managed only):
Enter the name of the SwyxServer for which this SwyxLink trunk is to be configured here.
With "Check server...", SwyxServer establishes a test connection to the remote SwyxServer.
Make sure that there is a transparent TCP/IP connection between the server on which the LinkManager service (local SwyxLink) is running, and all clients on the remote side and the SwyxServer.



Click on "Next >".
SwyxServer attempts to contact the remote server entered. If this attempt fails, you will receive a message. You can ignore the error message at this point and proceed with the creation of the trunk.
Click on "Next>".

8 Numbers:

Please enter the Public Numbers to be routed by this Trunk..

To map several individual numbers or number ranges, enter only one number or one range here, and add the others subsequently in the trunk properties (*The "Numbers" Tab*, Page 303).

Click on "Next >".

9 Codecs:

With the help of the Codec you select how the voice is compressed for transmission. The following options are available:

If the Codec priority "Prefer Quality" is selected, the Codecs are provided in the sequence G.722, G.711a, G.711µ, G.729 or Fax over IP. Specify the filter(s) you want:

- Voice, highest bandwidth (G.722)

  HD quality. A voice connection requires approximately 64kbits/s.
- Voice, high bandwidth (G.711a, G.711µ)

  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64kbits/s.
- Voice, low bandwidth (G.729)

  High compression. A voice connection requires approximately 24kbits/s.
- Fax

  In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration. A fax connection using T.38 requires approximately 20kbits/s.

If the Codec priority "Prefer low bandwidth" is selected, the Codecs sequence changes to G.729, G.722, G.711a, G.711µ, Fax over IP. The aim here is to use as little bandwidth as possible. Here too, specify the filter(s).

Click on "Next>".

10 Voice channels:

Enter how many calls may be routed via this trunk at the same time.

Using a SIP trunk, the provider will define how many connections at the same time will be possible. The maximum number of channels will be defined by the bandwidth to the provider and the Codec settings (i. e. the bandwidth per call).

Click on "Next>".

11 Intersite Settings:

You configure a connection to one or more further SwyxServers here. This configuration means that status information ("Logged off", "Away", "Do Not Disturb", "Speaking" etc.) can now be exchanged between users of different SwyxServers. As of version 2011 R2, the collaboration, video and instant messaging feature (only SwyxIt! Messenger, not Swyx Messenger) can be enabled for employees. Furthermore, users are shown in the Global Phonebook of the connected servers.

Various connection types are differentiated in the Intersite settings:

- Without any presence interaction:

  Choose this option if you do not want any status information to be published via this link. See also *I Without any presence interaction*, Page 299.

  Click on "Next>" and proceed with step (14).
- The remote SwyxServer is in the same organization:

  Choose this option if the remote SwyxServer is in the same organization as the SwyxServer you are presently administering. See *I In the same organization*, Page 299.

  Click on "Next" and proceed with step (12).
- The remote SwyxServer is in another organization:

  Choose this option if the remote SwyxServer is in another organization than the SwyxServer you are presently administering. See also *I From another organization*, Page 299.

  Click on "Next" and proceed with step (12).

12 Settings for cross-server status signaling/ communication:

Specify which numbers should be synchronized over this trunk, and what information should be transmitted.

Number synchronization

- Internal numbers

  If you activate this option, only the users' internal numbers will be shown in the Global Phonebook on all sites.

An absolute prerequisite for the synchronization of internal numbers is a valid and unique number plan, as otherwise, in the event of duplicates, individual numbers may be discarded. See also *10 Numbers and Number Mappings*, Page 146.

- Public numbers

If you activate this option, only the users' public numbers will be shown in the Global Phonebook on all SwyxServer sites.

- Internal and public call numbers

  When this option is selected, both the internal and the public call numbers of users will be shown in the Global Phonebook on all sites.

Data synchronization:

- User Pictures

  Say here whether the user pictures stored by the user should likewise be synchronized between the different servers. To save bandwidth, you can deactivate this option.

The trunk should be used for the transmission of:

- Calls.
- Video
- Collaboration
- SwyxIt!Meeting
- Status information or
- Instant Messaging

If you deactivate calls, the video, collaboration and SwyxIt! meeting features are deactivated automatically. If you deactivate the status information button, you are not able to choose Instant Messaging See also *Use of the trunk*, Page 299.

Click on "Next >".

13 If you have selected the Intersite connection "From another organization", then you select here the groups that should be visible on the remote SwyxServer.
Otherwise, proceed with step (14).
Click on "Next>".

When the Intersite connections are configured within the SwyxLink, status signaling between the different SwyxWare sites is not automatically activated. You then have to configure the relationship of the users/groups, to specify precisely who should be signaled about the status of another user or group. For how to configure the relationships between users and groups, see *11.2.8 The "Properties..." Dialog: The "Relationships" Tab*, Page 202

14 Computer name:
Enter the name of the computer on which the SwyxLinkManager is managed. Use the name of the computer as it appears in the computer properties.

15 Click "Finish".
The new Trunk is created, and is available for further configuration.

For changing the SwyxLinkTrunk properties subsequently, see *17.4 Configuring a SwyxLink Trunk*, Page 296.

17.4 CONFIGURING A SWYXLINK TRUNK

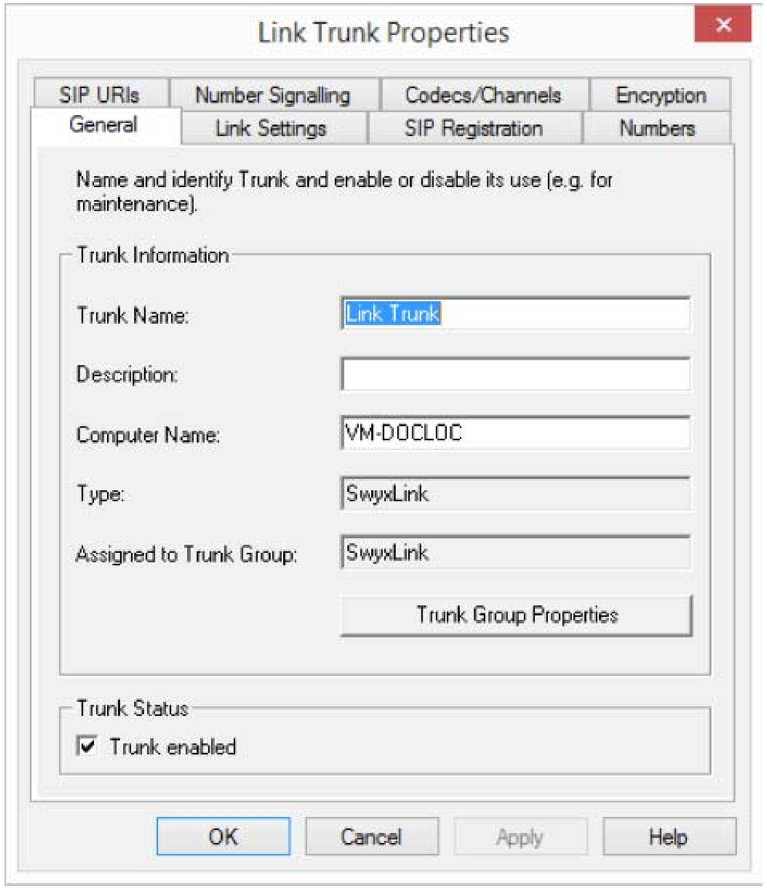
When you have created a SwyxLink trunk as described in *17.3 Creating a SwyxLink Trunk*, Page 294, you can subsequently change the settings of this trunk in the SwyxWare Administration.

When parameters of a trunk are changed, this change takes effect at once. There is no need to halt and restart any services for this.

How to configure a SwyxLink trunk

1. Open the SwyxWare Administration and choose the SwyxServer.
2. In the left side of the SwyxWare Administration window, click on "Trunks", and in the right-hand window select the trunk you want to configure.
3. In the context menu, select "Properties".
   In each case, the "Properties of..." window will appear.

The "General" Tab



Link Trunk Properties

Name and identify Trunk and enable or disable its use (e.g. for maintenance).

Trunk Information

Trunk Name: Link Trunk

Description:

Computer Name: VM-DOCLOC

Type: SwyxLink

Assigned to Trunk Group: SwyxLink

Trunk Status

☑ Trunk enabled

In this tab you can modify the name and description of the trunk.

Trunk information:

In the fields "Trunk Name" and "Description" you will find the descriptive information that is displayed in Administration.

The field "Computer Name" contains the name of the computer in which the service (LinkManager or SwyxGate) is installed.

The "Type" field indicates the type of the trunk, and "Trunk Group" the assigned Trunk Group. Both parameters cannot be retrospectively changed.

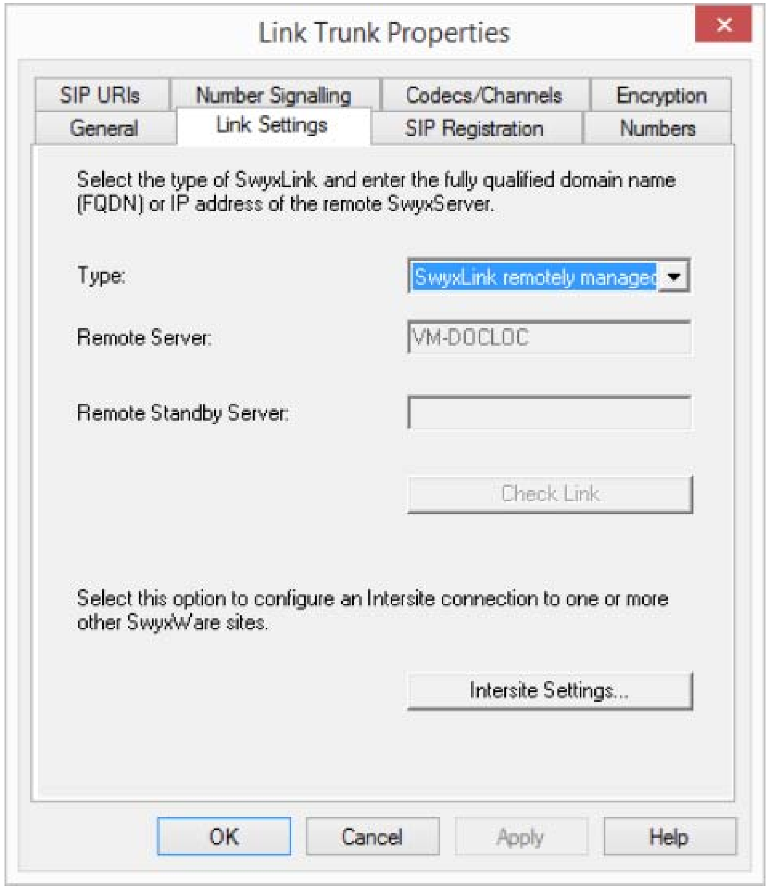
Using "Trunk Group Properties..." You will open the Properties of the according Trunk Group. You can edit the Properties of the Trunk Group directly.

Trunk status:

If you deactivate the checkbox "Trunk enabled", this gateway is blocked for further incoming or outgoing calls.

It won't be written in the change log, if a trunk was activated or deactivated.

The "Link Settings" Tab



Link Trunk Properties

Select the type of SwyxLink and enter the fully qualified domain name (FQDN) or IP address of the remote SwyxServer.

Type: SwyxLink remotely managed

Remote Server: VM-DOCLOC

Remote Standby Server:

Select this option to configure an Intersite connection to one or more other SwyxWare sites.

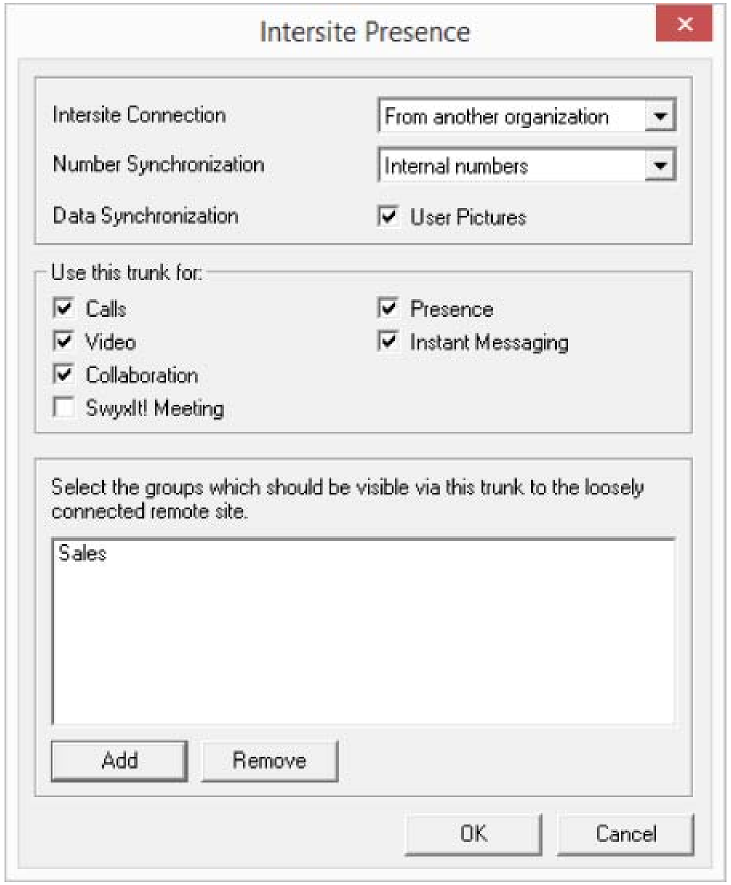
This tab contains information about managing the SwyxLink trunk.

The "Type" field indicates where the SwyxLink trunk is managed. If it is managed locally, i.e. by the SwyxServer on which the SwyxWare Administration is currently logged in, you will see the names of the computers on which this SwyxLinktrunk is managed remotely under Remote server. Please note that you can only change these settings on the site on which the SwyxLink trunk is locally managed.

Click on "Check Link" to launch an attempt to establish a connection with the remote SwyxServer.

You can use the "Intersite Settings..." button to configure a connection to one or more SwyxServers, in order to make user data and status information visible. This configuration means that status information ("Logged off", "Away", "Do Not Disturb", "Speaking" etc.) can be exchanged between users who are logged in to different SwyxServers. A distinction is made between a connection to a SwyxServer within a user's local organization, and to a SwyxServer outside the local organization.

Intersite Settings



Intersite Presence

Intersite Connection: From another organization

Number Synchronization: Internal numbers

Data Synchronization: ☑ User Pictures

Use this trunk for:

☑ Calls
☑ Video
☑ Collaboration
☐ SwyxIt! Meeting
☑ Presence
☑ Instant Messaging

Select the groups which should be visible via this trunk to the loosely connected remote site.

Sales

In the field "Intersite Connection" you can specify which type of connection is involved.

Intersite connection

- Without any presence interaction
  Choose "Without any presence interaction" if you want to disable status signaling across servers for this link.
- In the same organization
  Choose "In the same organization" if you want to set up a connection to a SwyxServer that is within an organization. With this connection type, all groups and users on all connected sites are visible in the Global Phonebook. The relationships within the user and group properties must be used to specify precisely who should be signaled about the status of a user or group.
- From another organization
  Choose "From another organization" if you want to set up a connection to a SwyxServer in a different organization. With this connection type, you can specify individual groups on your SwyxServer to be visible on the SwyxServer of the other organization. The relationships within the user and group properties must be used to specify precisely who should be signaled about the status of the users of a group. The administrator of the other server can take the corresponding action from his end, so that groups on his SwyxServer become visible on your site. Status signaling thus occurs only between users in selected groups. The users in these groups will also be displayed on both sites in the Global Phonebook.

Number synchronization

You use the "Number Synchronization" field to say whether internal, public or both numbers should be synchronized along with the user names between the different servers. A synchronization takes place automatically when changes have been made e.g. to user data, or when a SwyxServer has been restarted.

Data synchronization

In the "Data synchronization" field you can say whether the user pictures stored by the user should likewise be synchronized between the different servers. To save bandwidth, you can deactivate this option.

Use of the trunk

- Calls

If for some reason you do not want to make calls via this SwyxLink trunk, for instance if you have a flat rate for the PSTN, you can deactivate the "Calls" field. Status signaling via this SwyxLink trunk will then continue, but calls will be routed via the public telephone network (ISDN). If you deactivate this button, the trunk properties for Video, Collaboration and SwyxIt!Meeting below are deactivated automatically.

If you have deactivated the "Calls" field, you should publish the public numbers. In this case, choose the option "Public numbers" in the call number synchronization field!

- Video

If you permit video telephony to users outside the local server, this box should be checked.

- Collaboration

If the box is checked, the screen of participants can be transmitted across multiple servers.

- SwyxIt! Meeting

The transfer of desktops via SwyxIt! Meeting may only be selected, when Collaboration is activated.

- Presence

If you deactivate the field "Presence", there is no further status signaling via this SwyxLink trunk. However, the users will still be displayed in the Global Phonebook of the connected SwyxServer.

- Instant Messaging

By activating this check box, it is possible to exchange instant messages with users not logged in to the local server. This feature can only be used, when "status information" is activated.

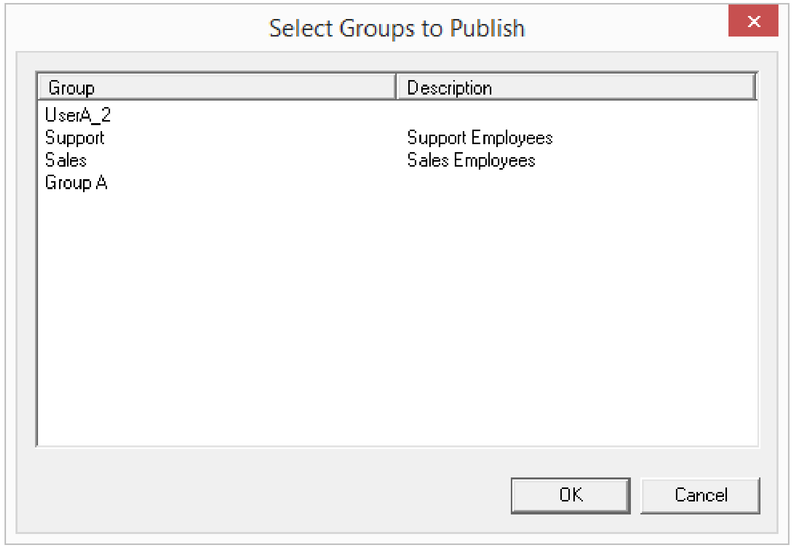
Please note that enough bandwidth is required in order to use the Video and Collaboration (SwyxIt! Meeting) feature. If not enough bandwidth is available, deactivate these check boxes.

Video and SwyxIt! Meeting connections between different SwyxServer locations require a direct connection of the SwyxIt! clients. Existing firewalls between the locations must be opened for the following ports:
Video (RTP, UDP): 50000-50999 (equivalent to the ports for voice transmission) SwyxIt! Meeting: As of port 49152 (dynamic TCP ports)

Group selection

If you have chosen a connection to a SwyxServer of another organization, you can specify individual groups to be visible on the SwyxServer site of the other organization.

Use the "Add" or "Delete" button to select groups, or remove previously added groups.



Select Groups to Publish

Group	Description
UserA_2	
Support	Support Employees
Sales	Sales Employees
Group A	

This is how you define an Intersite connection within your organization

1 Click on "Intersite Settings...".
The "Intersite Settings" window will appear.

2 In the field "Intersite Connection", select "In the same organization".

3 Specify in the "Number synchronization" field whether internal, public or both numbers should be synchronized between the different SwyxServers. See also *10 Numbers and Number Mappings*, Page 146.

4 In the "User Pictures" field you can say whether the user pictures stored by the user should likewise be synchronized between the different servers. To save bandwidth, you can deactivate this option.

5 Choose whether calls and/or presence should be routed via this link.
Calls:

- Deactivate the "Calls" field if calls are to be made via the ISDN trunk rather than this SwyxLink - if you have a flat rate for the PSTN for instance.
  In this case, however, all users will still be shown in the Global Phonebook of linked SwyxServers, and the status will still be sig-

naled according to the relationships configured in the user or group properties.

ℹ If you have deactivated the "Calls" field, you should publish the public numbers. In this case, choose the option "Public numbers" in the number synchronization field!

Presence:

- If you deactivate the "Presence" field, you disable the status signaling. But all users will be displayed in the Global Phonebook of the linked SwyxServers.

6 Click on "OK" to store the Intersite settings for this link.

This is how you define an Intersite connection to another organization

1 Click on "Intersite Settings...".
The "Intersite Settings" window will appear.

2 In the field "Intersite Connection", select "From another organization".

3 Specify in the "Number synchronization" field whether internal, public or both numbers should be synchronized between the different SwyxServers. See also *10 Numbers and Number Mappings*, Page 146.

4 In the "User Pictures" field you can say whether the user pictures stored by the user should likewise be synchronized between the different servers. To save bandwidth, you can deactivate this option.

5 Choose whether calls and/or presence should be routed via this link.
Calls:

- Deactivate the "Calls" field if calls are to be made via the ISDN trunk rather than this SwyxLink - if you have a flat rate for the PSTN for instance.

  In this case, however, all users in the groups selected in step (6) will still be shown in the Global Phonebook of linked SwyxServers, and the status will still be signaled according to the relationships configured in the user or group properties.

ℹ If you have deactivated the "Calls" field, you should publish the public numbers. In this case, choose the option "Public numbers" in the number synchronization field!

Presence:

- If you deactivate the "Presence" field, you disable the status signaling, i. e. the status of all users in the groups selected in step (6) will no longer be displayed on the linked server. However, all users in these groups will still be shown in the Global Phonebook of the linked server.

6 Choose one or more groups that should be visible on the site of the linked SwyxServer. The users in these groups will be visible on the linked server in the Global Phonebook, and their status will be displayed there (if the "Presence" field has been activated).

7 Click on "OK" to store the Intersite settings for this link.

This is how you deactivate the display of status information

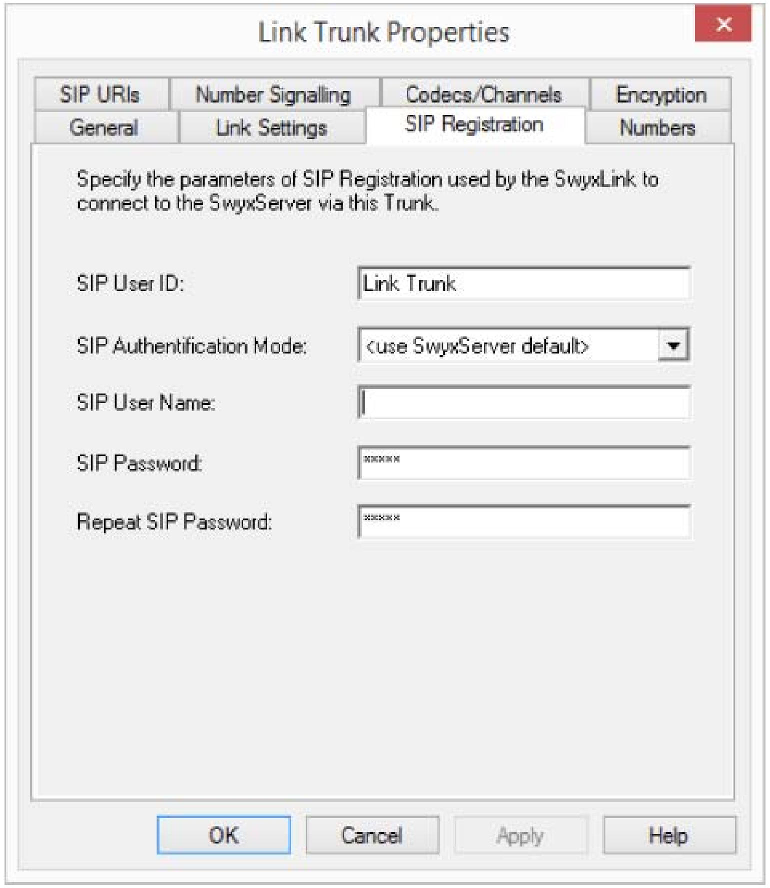
1 Click on "Intersite Settings...".
The "Intersite Settings" window will appear.

2 In the field "Intersite Connection", select "Without any presence interaction".

3 Click on "OK" to store the Intersite settings for this link.
No further data is then visible on the other side of the link.

ℹ If the data of the other SwyxServer site should likewise no longer be visible on your SwyxServer, the display of status information must similarly be deactivated on the other side.

The "SIP Registration" Tab



Specify the parameters of SIP Registration used by the SwyxLink to connect to the SwyxServer via this Trunk.

SIP User ID: Link Trunk

SIP Authentification Mode: <use SwyxServer default>

SIP User Name:

SIP Password: *****

Repeat SIP Password: *****

On this tab you can give the SIP access data with which the LinkManager logs on via this trunk to another SwyxServer. For security reasons, you can also specify that the LinkManager must authenticate itself when logging on to the SwyxServer.

SIP User ID:

A unique SIP user ID is needed for logging on to the SwyxServer. This is identical to the name of the trunk as default, but can be changed.

> The SIP user ID must be identical on both server sides.

SIP Authentication method

Specify here whether the LinkManager must authenticate itself to the SwyxServer or not.

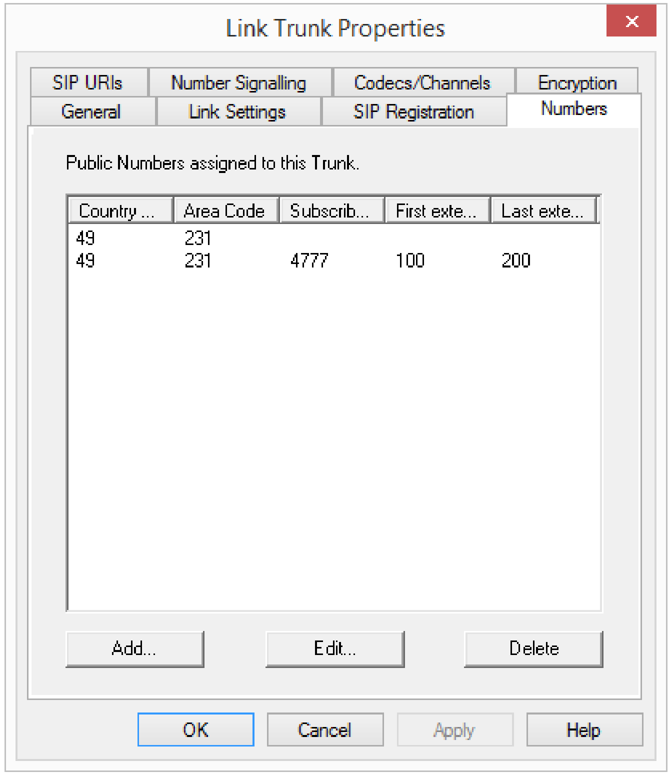
The following options are available for selection:

- <SwyxServer default
  If this option is selected, the authentication method selected in the client settings in the server properties is used here. See *7.5.2 The "Client Preferences" Tab*, Page 88.
- No authentication
  The LinkManager logs on without authentication.
- Always authenticate
  The LinkManager must always authenticate itself.

SIP user name and password

The SIP user name and SIP password are required for authentication.

The "Numbers" Tab



Public Numbers assigned to this Trunk.

Country ...	Area Code	Subscrib...	First exte...	Last exte...
49	231			
49	231	4777	100	200

The following settings can be made:

Public numbers of this trunk

You can specify here which public numbers this trunk uses. External calls to these numbers go over this trunk. Calls with a Calling Party Number that is assigned to this trunk are routed over this trunk.

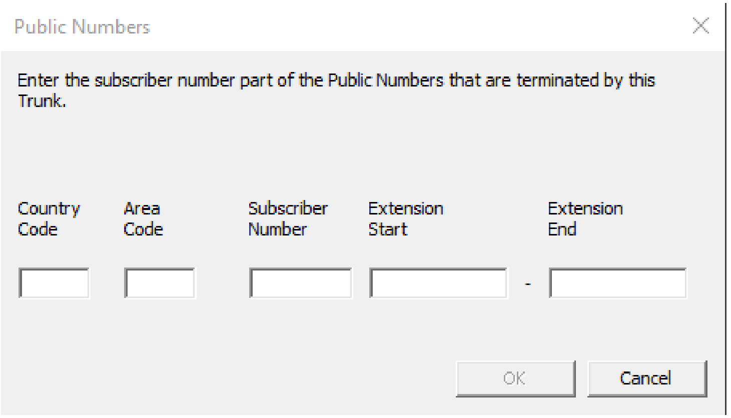
To ensure the unambiguity of the information, you must enter the complete phone number from SwyxWare V.13.20 onwards. In the new "Subscriber number" input field, enter the part of the phone number that follows the area code and precedes the extension (internal phone number).

	Country code	Area code	Subscriber number	First extension	Last extension
e. g.	49	231	4777	100	200

This is how you add numbers for this trunk

The existing phone number entries are automatically extended by the new entry field "Subscriber number" when updating to V.13.20. Make sure that the automatic allocation is correct and adjust the corresponding entries manually as required.

1 Click on "Add...".
The following window appears: "Numbers".



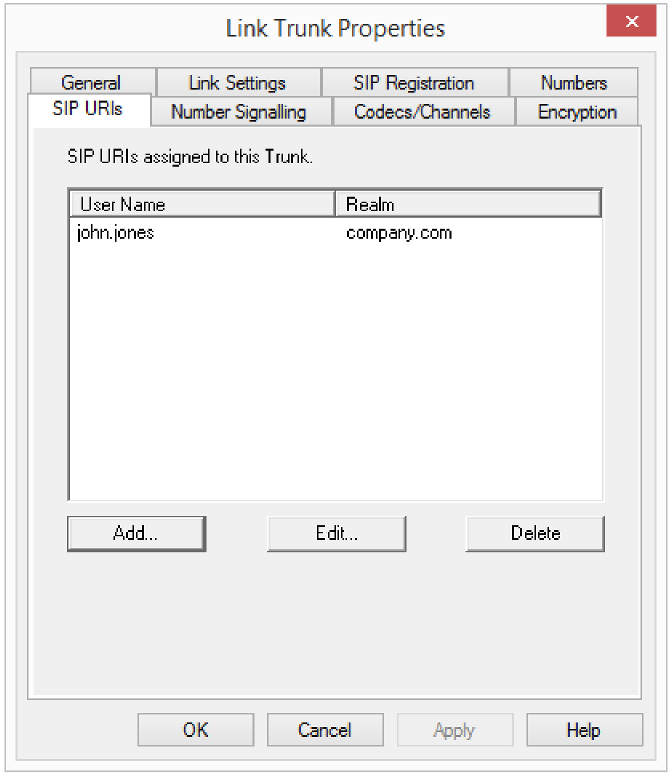
Enter the subscriber number part of the Public Numbers that are terminated by this Trunk.

2 You can add either an individual number or a range of numbers.

3 End your inputs with "OK".

To add several numbers or ranges, simply select "Add" the relevant number of times.

"SIP-URIs"



SIP URIs assigned to this Trunk.

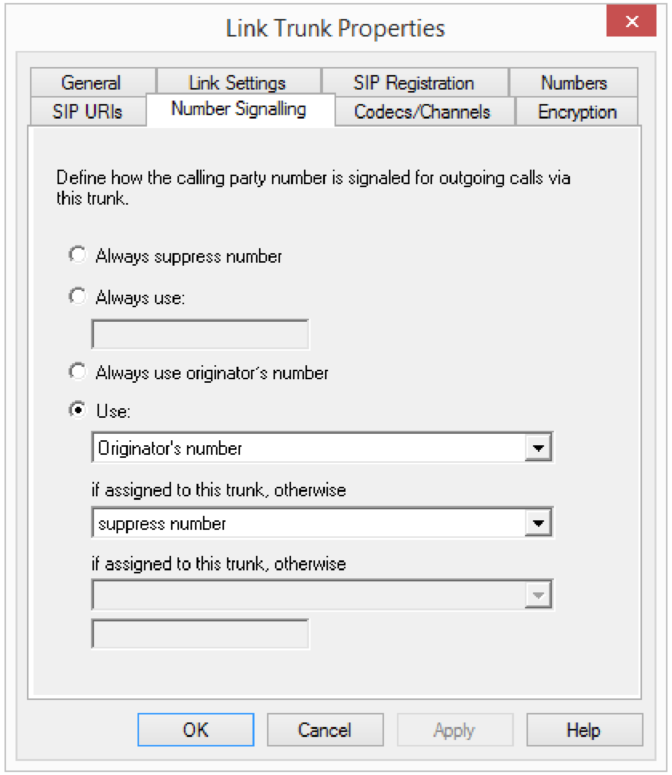
User Name	Realm
john.jones	company.com

The following settings can be made:

A list of SIP-URIs mapped to this trunk appears here. You can enter further SIP-URIs using "Add". To edit or delete a SIP-URI, highlight it in the list.

See *10.1.3 SIP-URIs*, Page 147.

"Number Signaling"



Define how the calling party number is signaled for outgoing calls via this trunk.

○ Always suppress number

○ Always use:

○ Always use originator´s number

● Use:

Originator's number

if assigned to this trunk, otherwise

suppress number

if assigned to this trunk, otherwise

Here you specify whether, and how, the numbers for outgoing calls via this trunk should be signaled.

- Always suppress number
  In this case no number is signaled to the person being called (XXX), regardless of which number was configured for this trunk.

In Germany, the destination numbers 110 and 112 are reserved for emergency calls. The outgoing call number to these destination numbers is always signaled.

- Always Use This Number:
  You can specify a number or SIP-URI here which will always be signaled to the person being called (e.g. the operator's number), regardless of which number was configured for this trunk.

The number must be entered in canonical number format.

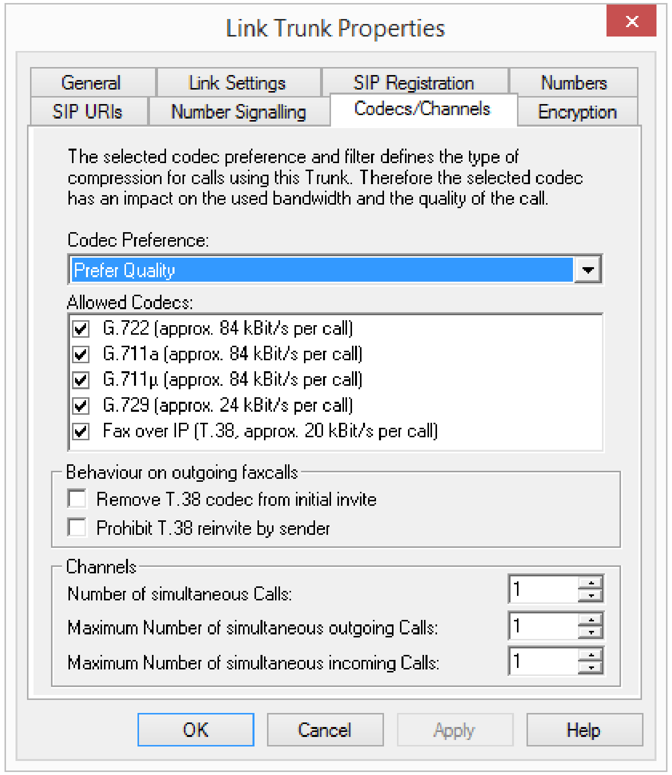
- Signal Caller Number
  Although the caller number is not configured for this trunk, the caller number is signaled to the person being called.

  Example:

  Customer A (number 88 333 44) calls employee B (number 55 666 77). Forwarding to his mobile phone is activated, i. e. an incoming call is routed outwards again. If the customer's number (88 333 44) should also be signaled externally, then this can be allowed here, although this number was not defined for this trunk.
- Use:
  You can specify here which number this trunk uses. You can specify the action for numbers that are assigned to this trunk as well as for numbers which have no assignment.

Use:	If assigned to this trunk, otherwise:	If assigned to this trunk, otherwise:	Entry
Origination Number	Number of the transferor		
	Hide number		
	Don't use this trunk		
	Use the following number		<Number>
Number of the transferor	Origination Number	Hide number	
		Don't use this trunk	
		Use the following number	<Number>
	Hide number		

The "Codecs/Channels" Tab



The selected codec preference and filter defines the type of compression for calls using this Trunk. Therefore the selected codec has an impact on the used bandwidth and the quality of the call.

Codec Preference: Prefer Quality

Allowed Codecs:

☑ G.722 (approx. 84 kBit/s per call)
☑ G.711a (approx. 84 kBit/s per call)
☑ G.711µ (approx. 84 kBit/s per call)
☑ G.729 (approx. 24 kBit/s per call)
☑ Fax over IP (T.38, approx. 20 kBit/s per call)

Behaviour on outgoing faxcalls

□ Remove T.38 codec from initial invite
□ Prohibit T.38 reinvite by sender

Channels

Number of simultaneous Calls: 1
Maximum Number of simultaneous outgoing Calls: 1
Maximum Number of simultaneous incoming Calls: 1

The following settings can be made:

Codecs

Here you can define the type of compression to be used on this connection.

If the Codec priority "Prefer Quality" is selected, the Codecs are provided in the sequence G.722, G.711a, G.711µ, G.729 or Fax over IP. Specify the filter(s) you want:

- Voice, highest bandwidth (G.722)
  HD quality
- Voice, high bandwidth (G.711a, G.711µ)
  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64kbits/s.
- Voice, low bandwidth (G.729)
  High compression. A voice connection requires approximately 24kbits/s.
- Fax over IP
  In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration. A fax connection using T.38 requires approximately 20kbits/s.
- If the Codec priority "Prefer low bandwidth" is selected, the Codecs sequence changes to G.729, G.722, G.711a, G.711µ, Fax over IP. The aim here is to use as little bandwidth as possible. Here too, specify the filter(s).
  Click on "Next>".

If there are several voice codecs selected, SwyxServer will filter voice data according to the current settings. The communicating sides will have to decide which voice codec to use.

It won't be written in the change log, if a Codec was activated or deactivated. See also *7.7 Change log*, Page 117.

Action on fax receipt

When a fax connection is set up, the T.38 protocol is negotiated between the two devices involved. Certain variants of this negotiation may not be supported by some IP adapters. Use the following filter options to establish compatibility with such devices.

- Remove T.38 codec from initial invite
  Some IP adapters cannot correctly interpret an initial connection request which includes T.38 as well as voice Codecs.
  If this option is set, SwyxServer removes T.38 from the initial connection request. The fax devices first set up a voice connection and then switch to the fax protocol T.38 because of the fax tone (CED tone, 2100Hz).
  Prohibit T.38 reinvite by sender
  The receiving fax device switches to T.38 after detecting the fax tone (CED tone, 2100Hz). Alternatively, the switch to T.38 can be carried out by the sending fax device.
  Some IP adapters don't support switching by the sender.
  If this option is set, SwyxServer suppresses a switch to T.38 by the sender.

If the receiving side involves a combined phone/fax device (fax switch), a fax data transmission is impossible when the option "Prohibit T.38 reinvite by sender" is activated.

The filter options can only be set when the Codec "Fax over IP (T.38...)" is activated.

Channels

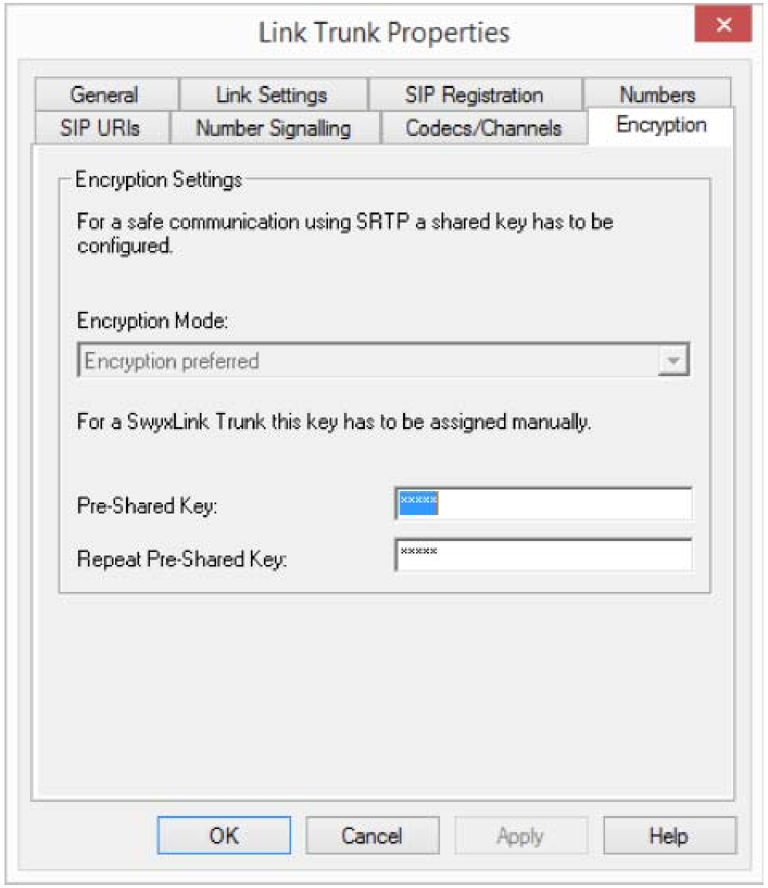
Specify how many channels (connections) should be simultaneously routed over this trunk. You can also determine how many outgoing and/or ingoing connections are established at most.

The maximum number of channels could be calculated from the available bandwidth and the Codec settings.

Please note that all settings made for this SwyxServer at location A for the SwyxLink trunk to location B must correspond with the settings made on the other SwyxServer at location B for the SwyxLink trunk to location A.

If channels were added or removed, you will find these changes in the change log. See also *7.7 Change log*, Page 117.

The "Encryption" tab



Link Trunk Properties

Encryption Settings

For a safe communication using SRTP a shared key has to be configured.

Encryption Mode: Encryption preferred

For a SwyxLink Trunk this key has to be assigned manually.

Pre-Shared Key: *****

Repeat Pre-Shared Key: *****

You can see here how and whether voice data going via this trunk should be encrypted. The settings were selected within the server properties, and apply equally to the SwyxLink trunk. See also *7.5.18 The "Security" tab*, Page 109.

For a SwyxLink trunk, it is advisable to configure both server sides identically in relation to encryption.

Whether a call is established via the SwyxLink trunk, and whether it is correspondingly encrypted from end point to end point (e.g. from SwyxIt! to SwyxIt!), depends on the encryption settings within the user properties on both servers. See also *21 Encryption*, Page 342.

Key (PreSharedKey)

To ensure secure communication by SRTP between two SwyxServers, a common key (PreSharedKey) must be defined between them.

For all components which use the SwyxWare database (e.g. SwyxIt!, PhoneMgr, ConferenceMgr, LinkMgr, Gateway), this key is automatically generated by SwyxServer and distributed to the relevant component, once again encrypted.

It is different for a SwyxLink trunk. In this case the key must be entered manually. Furthermore, the key entered here must likewise be entered in the SwyxLink trunk properties of the linked server.

A key length of less than 10 characters is not advisable. Longer keys offer greater security, and keys can be up to 128 characters long. In order to make brute-force or dictionary attacks more difficult, the key should consist of a combination of letters, numbers and special characters.

See also *21.1 Encryption within SwyxWare*, Page 342.

This is how you specify a key for the encryption of a SwyxLink trunk

1. Start the SwyxWare Administration and log in to the SwyxServer.
2. In the left side of the SwyxWare Administration window, click on "Trunks", and in the right-hand window select the trunk you want to configure.
3. Select "Properties".
4. Select the "Encryption" tab.
5. The encryption configured in the server properties is displayed.
6. Enter the key in the "Key" field. You must also enter this key in the SwyxLink trunk properties of the linked server.
7. Click on "OK".

17.5 PROPERTIES OF THE SWYXLINK CONNECTION

In this version, SwyxWare users are provided with the following features for the SwyxLink connection:

- Call set-up between the locations
- Routing to subscribers at the other location
- Name resolution from the Global Phonebook of each location
- Hold, Call Swap and Call Transfer
- Status signaling between users of the different SwyxServers (Intersite connections)
  Not available:
- Call signaling and the corresponding call pick up (Intersite connection)
- Groups and group calls across servers

18 ENUM LINKS

Setting up and operating ENUM trunks for the connection of the phone system to the ENUM number resolution service

18.1 WHAT IS AN ENUM TRUNK?

ENUM means the application of the Domain Name System to convert telephone numbers to internet addresses.

An ENUM link enables you to make SIP calls with ENUM number resolution via the Internet.

A user of a SIP phone is thus able to investigate the SIP address automatically using only the telephone number of the called party, and to convert the number into the SIP address. The called party can then be reached over the IP network in spite of using a 'normal' phone number. This postulate that the called party is registered at ENUM.

18.1.1 HOW AN ENUM TRUNK WORKS

When a call is made via an ENUM trunk, the system will start by accessing the ENUM registry and attempting to convert the number dialed into a SIP-URI. If the system manages to do this, a standard call will then be made directly via SIP to the opposite terminal with this SIP-URI.

The goal of an ENUM is to make different addresses, numbers and URLs available under a single number. This makes it possible for the user to be reached under the same number in the Internet and in the classical telephone network.

SwyxWare supports the DNS addresses *.e164.arpa (official ITU project) and the alternative project *.e164.org for the ENUM number resolution.

An ENUM trunk directly accepts the SIP messages from the opposite terminal. They are not forwarded via a SIP provider (as is the case with a SIP trunk).

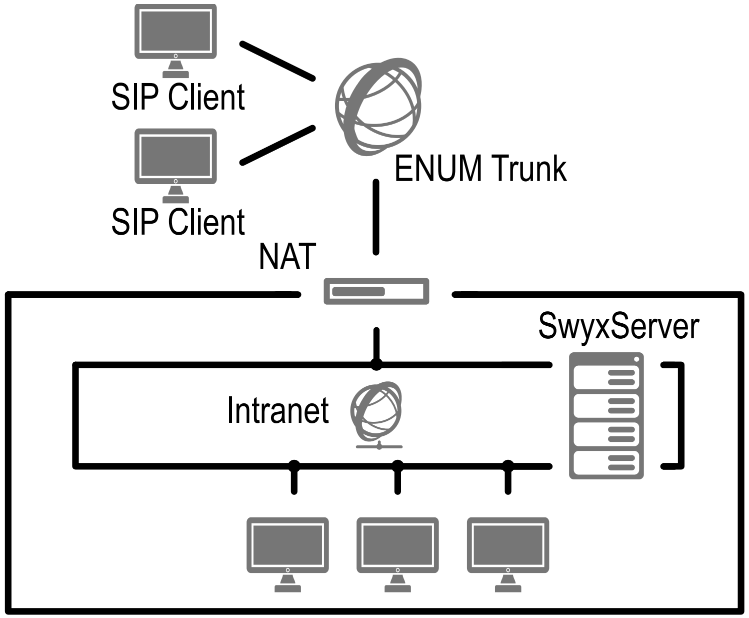


Fig. 18-1: SIP without Internet service provider (ITSP)

To call a SIP client (this can be a terminal device or a software-based telephony system) via an ENUM trunk, the corresponding SIPURI (Uniform Resource Identifier) of the client must be known. If you call a SIP client, for which there is a SIP URI, as usual via the telephone number, the corresponding SIP URI will be queried with the help of the ENUM application and used for creating a connection.

This means that ENUM uses in the case of a call the telephone number dialled (e. g. +1 202 555 1234), transforms it into a domain name (e. g. 4.3.2.1.5.5.5.2.0.2.1.e164.arpa.) and makes a DNS request. As part of this process, records known as NAPTRs (Naming Authority Pointer Records) are sent back. The evaluation of these records results in one or more different types of URI (e.g., SIP:name@domain.com or mailto:name@domain.com, etc.) under which the desired service of the given domain can be contacted.

SwyxWare currently supports the SIP URI type. The use of additional URI types (e.g., mailto, http, etc.) will feature in a later SwyxWare version.

If a SIP URI exists, communication with the SIP client can take place.

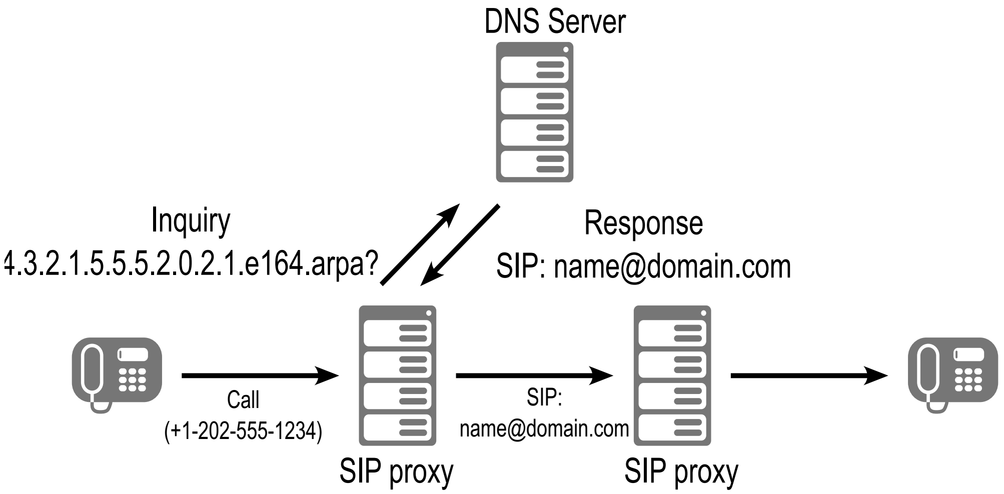


Fig. 18-2: ENUM call process

Please note that communication via an ENUM trunk can only take place with opposite terminals that are able to ensure the existence of a SIP-URI. If the DNS server cannot provide a SIP-URI for the number dialed, it will not be possible to establish a connection.

18.2 CREATION OF AN ENUM TRUNK GROUP

We recommend creating an ENUM trunk group before creating an ENUM trunk.

General parameters such as permissions, location and routings are specified in this group. When creating a trunk, you then simply assign the trunk group to the trunk. As a member of the group, the trunk is thus given the corresponding parameters.

How to create an ENUM trunk group

1. Open the SwyxWare Administration and choose the SwyxServer.
2. In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunk Groups" and select the entry "Add Trunk Group..." in the context menu.
   The "Add Trunk Group..." wizard will appear.
3. Click on "Next>".
4. Name and description of the trunk group:
   Enter the name of the trunk group, and a description.
   Click on "Next>".
5. Type of trunk group:
   Enter the type of trunk group here, in this case "ENUM".
   Only the "ENUM" option appears for selection in the "Profile" field.
   Click on "Next>".
6. ENUM settings:
   To allow incoming calls from the Internet to SIP-URIs to be received via this trunk, enter the dedicated realm here, which must be mapped to the SIP-URIs 'dialed' from outside, e. g., ‘company.com'.
   DTMF method:
   This mode defines a method based on user keyboard entries (DTMF signalize).
   You can choose from a variety of options:
   - None. DTMF signalization is deactivated
   - RFC2833_Event: RFC2833_Event: DTMF signalization, based on the event mechanism described in RFC2833, will be used.
   - Info Method DTMF Relay DTMF signalling as recommended by Cisco (applicationtype DtmfRelay) will be used

   Click on "Next>".
7. Settings for the STUN server

If you wish to use STUN, you can use the free STUN server "stunserver.org" with port "3478".
Click on "Next>".

8. Definition of routing:
   Specify for which calls this Trunk Group should be used. When entering call numbers or URIs you can use placeholders (*), e.g. "+*" for all external numbers or "*" for all internal numbers. Multiple numbers/URIs are separated by a semicolon. You have several different options:
   - for all external calls
   - only for external calls to the following destination number or SIP-URI
   - for all external calls and all unassigned internal numbers
   - For the following internal numbers
   - Create no routing records for the moment

   Click on "Next>".
9. Call Permission
   Specify the Calling Rights profile for the Trunk Group. This Calling Rights profile applies to the incoming calls over this Trunk Group.
   See also *Call permission of a trunk group*, Page 129.
   Click on "Next >".
10. Location profile:
    Define the location. This profile also includes the definition of e.g. country code and public line access.
    Click on "Next>".
11. Click "Finish".
    The new ENUM trunk group is created, and is available for further configuration.

For changing the ENUM Trunk Group properties subsequently, see *13.1 Configure trunk groups*, Page 227.

18.3 CREATING AN ENUM TRUNK

You can now create ENUM trunks.

The service SwyxLinkManager, which is responsible for linking ISDN lines, is automatically installed with the standard version of the SwyxServer software.

The administration of an ENUM trunk is handled with SwyxWare Administration. Please start SwyxWare Administration as described in *7.1 Registration on SwyxWare Administration*, Page 80. If you are not yet connected to this server, please connect now as described in *How to connect to a SwyxServer*, Page 83.

How to create an ENUM trunk

1. Open the SwyxWare Administration and choose the SwyxServer.
2. In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunks" and select the entry "Add Trunk..." in the context menu.
3. An "Add new Trunk Wizard" opens up.
   Click on "Next>".
4. Trunk name:
   Enter a name and a short description for the new trunk here.
   Click on "Next>".
5. Selection of a trunk group:
   Select the trunk group here to which this trunk should be assigned.
   General settings such as routings, rights and location-specific parameters are specified in the trunk group. You can use "New Trunk Group..." to create a new trunk group, and then continue with the creation of a trunk.
   See also *How to create an ENUM trunk group*, Page 310.
   Click on "Next >".
6. Numbers:
   Please enter the Public Numbers to be routed by this Trunk..
   In respect of the generation of SIP-URIs, numbers configured here are also converted into the following format:
   sip:<number>@<realm>
   The realm is the same one defined in the trunk group.

To map several individual numbers or number ranges to this trunk, enter only one number or one range here, and add the others subsequently in the trunk properties (*The "Numbers" Tab*, Page 314).

7 SIP-URI
Enter the SIP addresses (URIs) to be managed by this trunk here. A SIP has the following format:
SIP:<Name 1>@<Name 2>
where <Name 1> represents the user name and <Name 2> the realm. Although the realm is set by default when the trunk group is selected, it can be overwritten individually here.
To make things easier, you can use '*' as a placeholder, e.g., enter '*@company.com' for all users with the realm 'company.com'.

8 Codecs:
With the help of the Codec you select how the voice is compressed for transmission. The following options are available:

If the Codec priority "Prefer Quality" is selected, the Codecs are provided in the sequence G.722, G.711a, G.711µ, G.729 or Fax over IP. Specify the filter(s) you want:

- Voice, highest bandwidth (G.722)
  HD quality
- Voice, high bandwidth (G.711a, G.711µ)
  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64kbits/s.
- Voice, low bandwidth (G.729)
  High compression. A voice connection requires approximately 24kbits/s.
- Fax over IP
  In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration. A fax connection using T.38 requires approximately 20kbits/s.

If the Codec priority "Prefer low bandwidth" is selected, the Codecs sequence changes to G.729, G.722, G.711a, G.711µ, Fax over IP. The aim here is to use as little bandwidth as possible. Here too, specify the filter(s).

Click on "Next>".

If there are several voice codecs selected, SwyxServer will filter voice data according to the current settings. The communicating sides will have to decide which voice codec to use.

It won't be written in the change log, if a Codec was activated or deactivated. See also *7.7 Change log*, Page 117.

9 Voice channels:
Enter how many calls may be routed via this trunk at the same time.
The maximum number of voice channels is calculated on the basis of the bandwidth of the IP connection and terminal used.

10 Computer name:
Enter the name of the computer on which the SwyxLinkManager is managed. Use the name of the computer as it appears in the computer properties.

11 Click "Finish".
The new Trunk is created, and is available for further configuration.

For changing the ENUM Trunk properties subsequently, see *18.4 Configuring an ENUM Trunk*, Page 312.

Please note that when using a NAT router, port forwarding must be configured so that the SIP messages, which are received on the public IP address of the NAT router on port 5060 are also forwarded to the SwyxLinkManager on port 65002 in the internal network.

See also *18.5 Configuring the Firewall/NAT Router for an ENUM Trunk*, Page 319.

18.4 CONFIGURING AN ENUM TRUNK

When you have created an ENUM trunk as described in *18.3 Creating an ENUM Trunk*, Page 311, you can subsequently change the settings of this trunk in the SwyxWare Administration.

When parameters of a trunk are changed, this change takes effect at once. There is no need to halt and restart any services for this.

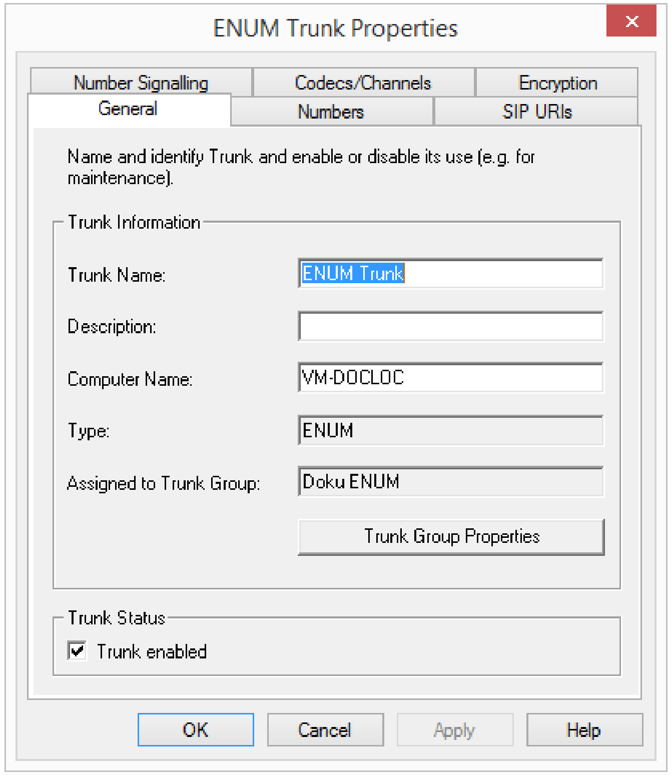
How to configure an ENUM trunk

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click on "Trunks", and in the right-hand window select the trunk you want to configure.

3 In the context menu, select "Properties".
In each case, the "Properties of..." window will appear.

The "General" Tab


ENUM Trunk Properties

Name and identify Trunk and enable or disable its use (e.g. for maintenance).

Trunk Information

Trunk Name: ENUM Trunk

Description:

Computer Name: VM-DOCLOC

Type: ENUM

Assigned to Trunk Group: Doku ENUM

Trunk Status

☑ Trunk enabled

In this tab you can modify the name and description of the trunk.

Trunk information:

In the fields "Trunk Name" and "Description" you will find the descriptive information that is displayed in Administration.

The field "Computer Name" contains the name of the computer in which the service (LinkManager or SwyxGate) is installed.

The "Type" field indicates the type of the trunk, and "Trunk Group" the assigned Trunk Group. Both parameters cannot be retrospectively changed.

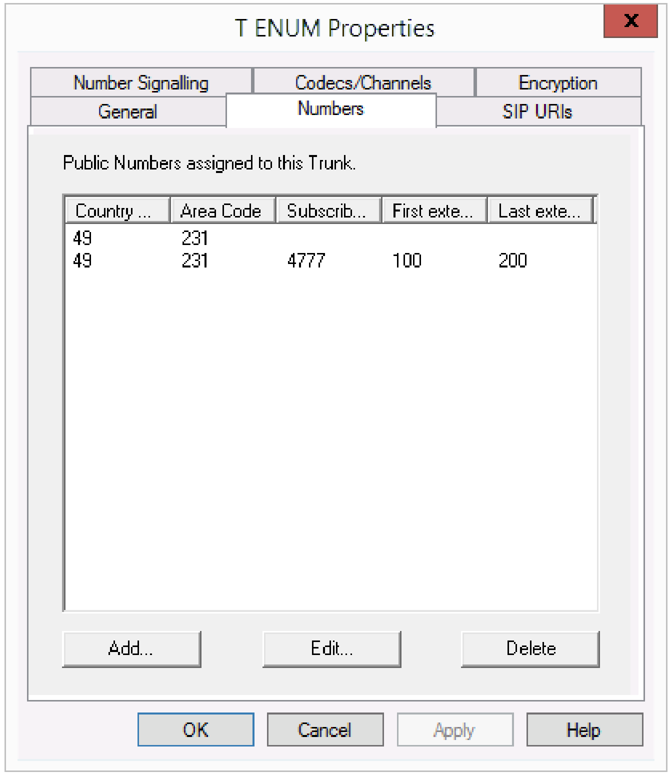
Using "Trunk Group Properties..." You will open the Properties of the according Trunk Group. You can edit the Properties of the Trunk Group directly.

Trunk status:

If you deactivate the checkbox "Trunk enabled", this gateway is blocked for further incoming or outgoing calls.

It won't be written in the change log, if a trunk was activated or deactivated.

The "Numbers" Tab



Public Numbers assigned to this Trunk.

Country ...	Area Code	Subscrib...	First exte...	Last exte...
49	231			
49	231	4777	100	200

The following settings can be made:

Public numbers of this trunk

You can specify here which public numbers this trunk uses. External calls to these numbers go over this trunk. Calls with a Calling Party Number that is assigned to this trunk are routed over this trunk.

To ensure the unambiguity of the information, you must enter the complete phone number from SwyxWare V.13.20 onwards. In the new "Subscriber number" input field, enter the part of the phone number that follows the area code and precedes the extension (internal phone number).

	Country code	Area code	Subscriber number	First extension	Last extension
e. g.	49	231	4777	100	200

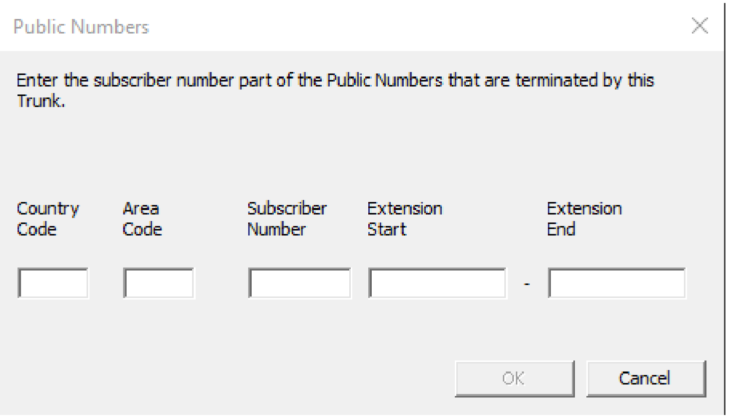
This is how you add numbers for this trunk

The existing phone number entries are automatically extended by the new entry field "Subscriber number" when updating to V.13.20. Make sure that the automatic allocation is correct and adjust the corresponding entries manually as required.

can only be received by this ENUM trunk if these numbers have been registered with ENUM.

This is how you add numbers for this trunk

1 Click on "Add...".
The "Public numbers" window will appear.



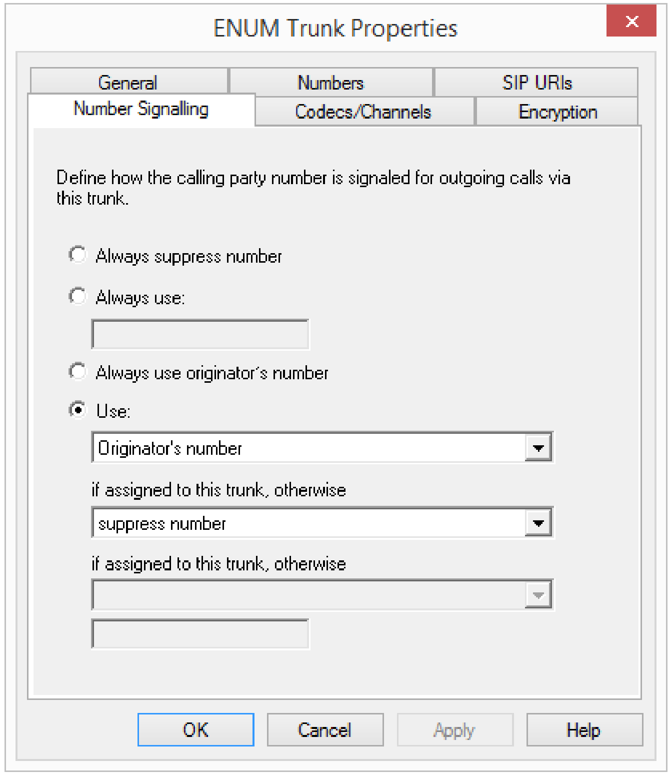
Enter the subscriber number part of the Public Numbers that are terminated by this Trunk.

2 You can add either an individual number or a range of numbers.

3 End your inputs with "OK".

To add several numbers or ranges, simply select "Add" the relevant number of times.

"Number Signaling"



Define how the calling party number is signaled for outgoing calls via this trunk.

○ Always suppress number

○ Always use:

○ Always use originator´s number

● Use:

Originator's number

if assigned to this trunk, otherwise

suppress number

if assigned to this trunk, otherwise

Here you specify whether, and how, the numbers for outgoing calls via this trunk should be signaled.

- Always suppress number
  In this case no number is signaled to the person being called (XXX), regardless of which number was configured for this trunk.

In Germany, the destination numbers 110 and 112 are reserved for emergency calls. The outgoing call number to these destination numbers is always signaled.

- Always Use This Number:
  You can specify a number or SIP-URI here which will always be signaled to the person being called (e.g. the operator's number), regardless of which number was configured for this trunk.

The number must be entered in canonical number format.

- Signal Caller Number
  Although the caller number is not configured for this trunk, the caller number is signaled to the person being called.

  Example:

  Customer A (number 88 333 44) calls employee B (number 55 666 77). Forwarding to his mobile phone is activated, i. e. an incoming call is routed outwards again. If the customer's number (88 333 44) should also be signaled externally, then this can be allowed here, although this number was not defined for this trunk.

- Use:
  You can specify here which number this trunk uses. You can specify the action for numbers that are assigned to this trunk as well as for numbers which have no assignment.

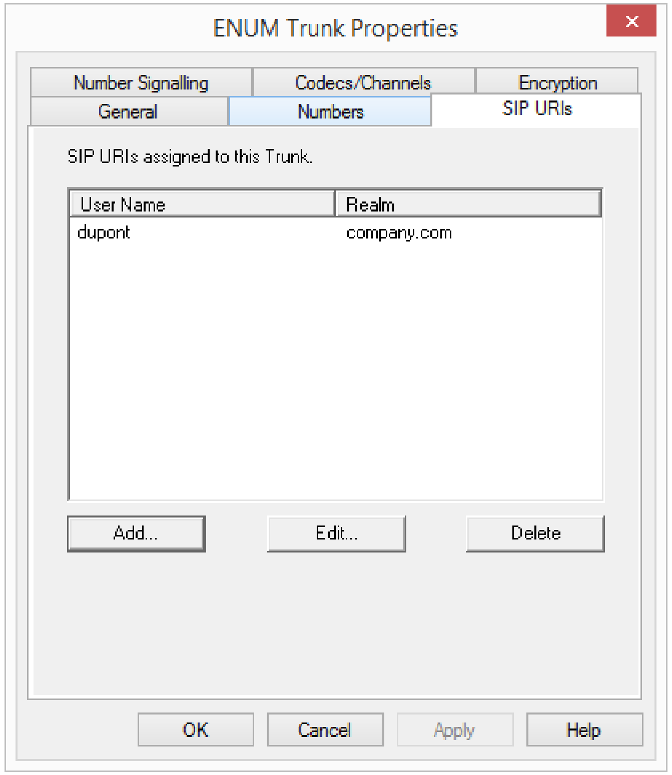
Use:	If assigned to this trunk, otherwise:	If assigned to this trunk, otherwise:	Entry
Origination Number	Number of the transferor		
	Hide number		
	Don't use this trunk		

Use:	If assigned to this trunk, otherwise:	If assigned to this trunk, otherwise:	Entry
	Use the following number		<Number>
Number of the transferor	Origination Number	Hide number	
		Don't use this trunk	
		Use the following number	<Number>
	Hide number		

The caller number signaled on an ENUM trunk combines the number and the configured realm as follows:

sip:<Caller name>@<realm>

The "SIP-URIs" Tab



SIP URIs assigned to this Trunk.

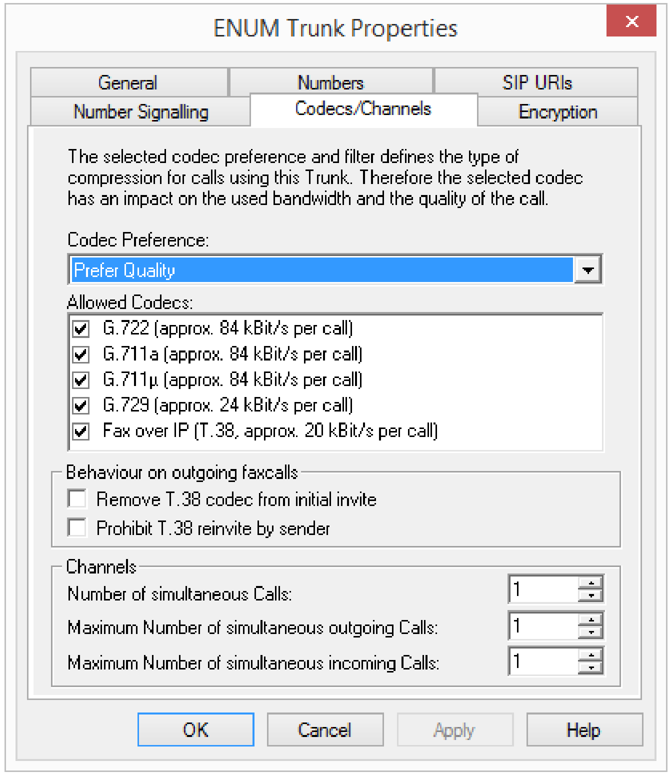
User Name	Realm
dupont	company.com

The following settings can be made:

A list of SIP-URIs mapped to this trunk appears here.

Click on "Add" to enter more SIP-URIs. To edit or delete a SIP-URI, highlight it in the list.

The "Codecs/Channels" Tab



ENUM Trunk Properties

The selected codec preference and filter defines the type of compression for calls using this Trunk. Therefore the selected codec has an impact on the used bandwidth and the quality of the call.

Codec Preference: Prefer Quality

Allowed Codecs:

- ☑ G.722 (approx. 84 kBit/s per call)
- ☑ G.711a (approx. 84 kBit/s per call)
- ☑ G.711µ (approx. 84 kBit/s per call)
- ☑ G.729 (approx. 24 kBit/s per call)
- ☑ Fax over IP (T.38, approx. 20 kBit/s per call)

Behaviour on outgoing faxcalls

- □ Remove T.38 codec from initial invite
- □ Prohibit T.38 reinvite by sender

Channels

Number of simultaneous Calls: 1

Maximum Number of simultaneous outgoing Calls: 1

Maximum Number of simultaneous incoming Calls: 1

The following settings can be made:

Codecs

Here you can define the type of compression to be used on this connection.

If the Codec priority "Prefer Quality" is selected, the Codecs are provided in the sequence G.722, G.711a, G.711µ, G.729 or Fax over IP. Specify the filter(s) you want:

- Voice, highest bandwidth (G.722)
  HD quality
- Voice, high bandwidth (G.711a, G.711µ)
  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64kbits/s.
- Voice, low bandwidth (G.729)
  High compression. A voice connection requires approximately 24kbits/s.
- Fax over IP
  In this case, the special fax protocol T.38 is used, which takes the setup of the IP network into consideration. A fax connection using T.38 requires approximately 20kbits/s.
- If the Codec priority "Prefer low bandwidth" is selected, the Codecs sequence changes to G.729, G.722, G.711a, G.711µ, Fax over IP. The aim here is to use as little bandwidth as possible. Here too, specify the filter(s).
  Click on "Next>".

If there are several voice codecs selected, SwyxServer will filter voice data according to the current settings. The communicating sides will have to decide which voice codec to use.

It won't be written in the change log, if a Codec was activated or deactivated. See also *7.7 Change log*, Page 117.

Action on fax receipt

When a fax connection is set up, the T.38 protocol is negotiated between the two devices involved. Certain variants of this negotiation may not be supported by some IP adapters. Use the following filter options to establish compatibility with such devices.

- Remove T.38 codec from initial invite
  Some IP adapters cannot correctly interpret an initial connection request which includes T.38 as well as voice Codecs.
  If this option is set, SwyxServer removes T.38 from the initial connection request. The fax devices first set up a voice connection and then switch to the fax protocol T.38 because of the fax tone (CED tone, 2100Hz).

- Prohibit T.38 reinvite by sender
  The receiving fax device switches to T.38 after detecting the fax tone (CED tone, 2100Hz). Alternatively, the switch to T.38 can be carried out by the sending fax device.
  Some IP adapters don't support switching by the sender.
  If this option is set, SwyxServer suppresses a switch to T.38 by the sender.

> If the receiving side involves a combined phone/fax device (fax switch), a fax data transmission is impossible when the option "Prohibit T.38 reinvite by sender" is activated.

> The filter options can only be set when the Codec "Fax over IP (T.38...)" is activated.

Channels

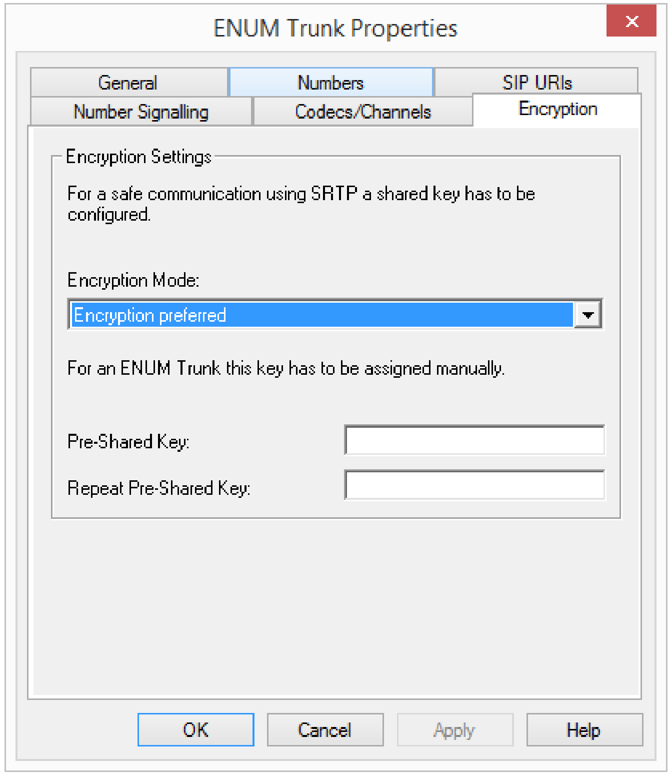
Specify how many channels (connections) should be simultaneously routed over this trunk. You can also determine how many outgoing and/or ingoing connections are established at most.

The maximum number of channels could be calculated from the available bandwidth and the Codec settings.

Please note that as well as the connection for ENUM number resolution, the conversations routed via a SIP connection (Internet) to a directly-dialed terminal are also routed via this trunk.

If channels were added or removed, you will find these changes in the change log. See also *7.7 Change log*, Page 117.

The "Encryption" tab



ENUM Trunk Properties

Encryption Settings

For a safe communication using SRTP a shared key has to be configured.

Encryption Mode: Encryption preferred

For an ENUM Trunk this key has to be assigned manually.

Pre-Shared Key:

Repeat Pre-Shared Key:

You can specify here how and whether voice data going via this trunk should be encrypted.

Encryption mode

This is where you specify the mode of encryption for this trunk. The following encryption modes are available:

- No encryption
  If "No encryption" is selected, the voice data going via this trunk is not encrypted. If the encryption mode was set to "No encryption" within the server properties, the mode is likewise set to "No encryption" here, and cannot be changed. The field is then deactivated.

- Encryption preferred
  When "Encryption preferred" is selected, the voice data is only encrypted if the opposite terminal likewise supports encryption. If this is not the case, the voice data is not encrypted, but phoning is still possible.
- Encryption mandatory
  When "Encryption mandatory" is selected, voice data encryption is obligatory. This means that either encryption always occurs or the call is aborted with the reason "Incompatible encryption settings". This can be the case, for example, if the opposite terminal does not permit any encryption.

> If the encryption mode was set to "No encryption" within the server properties, the mode is likewise set to "No encryption" here; if "Encryption mandatory" was configured there, then the setting "Encryption mandatory" also appears here. In both cases, the mode cannot be changed. The field is then deactivated.

See also *21 Encryption*, Page 342.

Key (PreSharedKey)

To ensure secure communication by SRTP between SwyxServer and the opposite terminal, a common key (PreSharedKey) must be defined and exchanged between them.

For all components which use the SwyxWare database (e.g. SwyxIt!, PhoneMgr, ConferenceMgr, LinkMgr, Gateway), this key is automatically generated by SwyxServer and distributed to the relevant component, once again encrypted.

It is different for the ENUM trunk. In this case the key must be entered manually. The key must also be entered on the opposite terminal.

> A key length of less than 10 characters is not advisable. Longer keys offer greater security, and keys can be up to 128 characters long. In order to make brute-force or dictionary attacks more difficult, the key should consist of a combination of letters, numbers and special characters.

See also *21.1 Encryption within SwyxWare*, Page 342.

This is how you specify the encryption mode for an ENUM trunk

1. Start the SwyxWare Administration and log in to the SwyxServer.
2. In the left side of the SwyxWare Administration window, click on "Trunks", and in the right-hand window select the trunk you want to configure.
3. Select "Properties".
4. Select the "Encryption" Tab.
5. In the field "Encryption mode", choose from:
   - No encryption
   - Encryption preferred
   - Encryption mandatory
6. Enter the key in the "Key" field. The key must also be entered on the opposite terminal.
7. Click on "OK".

18.5 CONFIGURING THE FIREWALL/NAT ROUTER FOR AN ENUM TRUNK

The ENUM trunk does not need a SIP provider to log on. An ENUM trunk directly accepts the SIP messages from the opposite terminal. In order to support this scenario, the NAT router must have port forwarding configured so that the SIP messages, which are received on the public IP address of the NAT router on well-known port 5060 are also forwarded to the SwyxLinkManager on port 65002 in the internal network. To do this, create a rule on the NAT router that forwards all messages received on the public IP address an the port 5060 from the NAT router to the internal network to the IP address of the SwyxLinkManager and the port 65002.

This will ensure that the SIP messages are also received by the SwyxLinkManager.

Example:

Port: 5060 on the external side of the NAT router
= ">" IP: 192.168.100.5, Port: 65002

Placing the SwyxLinkManager in a DMZ (Demilitarized Zone) is not recommended because the clients must contact the SwyxLinkManager directly for voice transmission and a real DMZ cannot usually be accessed by LAN clients.

19 SIP GATEWAY LINKS

19.1 WHAT IS A SIP GATEWAY TRUNK?

SIP gateway trunks are used for activating gateways which are themselves reached by SwyxServer via an SIP connection. This allows e.g. telephones in small branch offices to be operated with a local gateway in each case and with a local direct connection to the PSTN. In this way, sophisticated requirements of a company network can also be met when there are numerous small sites (e.g. many shops in a chain of stores).

Generally, gateways support extensive functions for routing, firewalls, security, VPN and intrusion detection; in other words, they provide an end device for branch offices that is tailored to meet company requirements.

You can obtain more information about this subject from your specialist dealer.

19.2 APPLICATION SCENARIOS

A gateway connected directly to SwyxServer via SIP, can be used in a variety of scenarios. In applications of this type, the purpose is usually to connect a small to medium-sized branch office. An example scenario is described below.

If you need to link two locations, each of which has its own SwyxServer, please use SwyxLink trunks. See also *17 SwyxLink (Server-Server Connection)*, Page 292.

Branch office with central SwyxWare

Under normal circumstances, communication between the branch office and headquarters takes place via VPN using a DSL/ADSL IP broadband connection, whereby the communication devices in the branch office have full access to the functions of the SwyxWare in the headquarters.

A wide selection of terminals can be used in the branch office. These include analog phone and fax devices, digital phones, SwyxPhone, computer clients, and SIP phones. All functions of SwyxWare are used.

SwyxIt! as a computer client and SwyxPhone can be integrated seamlessly into the branch office environment alongside existing analog, ISDN and SIP phones. This means that all employees can benefit from the advantages of SwyxWare, without having to work in isolation from the existing infrastructure.

19.3 CREATING A SIP GATEWAY TRUNK GROUP

We recommend creating a SIP gateway trunk group before creating a SIP gateway trunk.

General parameters such as permissions, location and routings are specified in this group. When creating a trunk, you then simply assign the trunk group to the trunk. As a member of the group, the trunk is thus given the corresponding parameters.

How to create a SIP gateway trunk group

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunk Groups" and select the entry "Add Trunk Group..." in the context menu.
The "Add Trunk Group..." wizard will appear.

3 Click on "Next>".

4 Name and description of the trunk group:
Enter the name of the trunk group, and a description.
Click on "Next>".

5 Type of trunk group:
Enter the type of trunk group here, in this case "SIP gateway".

6 Enter the profile for this trunk group in the lower field "Profile".
Here: "SIP Gateway Profile"
See also *19.4 Creating a SIP Gateway Trunk*, Page 322.
Click on "Next >".

7 Definition of routing:
Specify for which calls this Trunk Group should be used. When entering call numbers or URIs you can use placeholders (*), e.g. "+*" for all external numbers or "*" for all internal numbers. Multiple numbers/URIs are separated by a semicolon. You have several different options:

- for all external calls
- only for external calls to the following destination number or SIP-URI
- for all external calls and all unassigned internal numbers
- For the following internal numbers
- Create no routing records for the moment

Click on "Next>".

8 Call Permission
Specify the Calling Rights profile for the Trunk Group. This Calling Rights profile applies to the incoming calls over this Trunk Group.
See also *Call permission of a trunk group*, Page 129.
Click on "Next>".

9 Location profile:
Define the location. This profile also includes the definition of e.g. country code and public line access.
Click on "Next>".

10 Click "Finish".
The new SIP gateway trunk group is created, and is available for further configuration.

For changing the SIP Trunk Group properties subsequently, see *13.1 Configure trunk groups*, Page 227.

19.4 CREATING A SIP GATEWAY TRUNK

Once you have created a SIP gateway trunk group, you can proceed to create individual trunks to this SIP gateway.

> The SwyxLinkManager service, which is responsible for linking SIP lines, is automatically installed with the standard version of the SwyxServer software.

The administration of a SIP gateway trunk is handled with the SwyxWare Administration. Please start SwyxWare Administration as described in *7.1 Registration on SwyxWare Administration*, Page 80. If you are not yet connected to this server, please connect now as described in *How to connect to a SwyxServer*, Page 83.

How to create a SIP gateway trunk

1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click with the right mouse button on "Trunks" and select the entry "Add Trunk..." in the context menu.

3 An "Add new Trunk Wizard" opens up.
Click on "Next>".

4 Trunk name:
Enter a name and a short description for the new trunk here.
Click on "Next>".

5 Selection of a trunk group:
Select the trunk group here to which this trunk should be assigned.
General settings such as routings, rights and location-specific parameters are specified in the trunk group. You can use "New

Trunk Group..." to create a new trunk group, and then continue with the creation of a trunk.
See also *How to create a SIP gateway trunk group*, Page 321.
Click on "Next >".

6 SIP registration:
Enter the parameters the SIP gateway needs to log on to SwyxServer via this trunk.
SIP User ID:
The user ID is combined with the realm to create the SIP address (URI).
SIP Authentication method:
Indicate whether or not the gateway needs to authenticate itself.
SIP user name and password:
The user name and password are required for authentication.
This logon data must be entered in the same format as when was configured.

7 Numbers:
Please enter the Public Numbers to be routed by this Trunk..
To map several individual numbers or number ranges, enter only one number or one range here, and add the others subsequently in the trunk properties (*The "Numbers" Tab*, Page 325).

8 Codecs:
With the help of the Codec you select how the voice is compressed for transmission. The following options are available:
Specify which Codecs should be permitted for this trunk.
- Voice, low bandwidth (G.729)
  High compression. A voice connection requires approximately 24 kbits/s.
- Voice, highest bandwidth (G.722)
  HD quality
- Voice, high bandwidth (G.711a, G.711μ)
  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64 kbits/s.
- Fax over IP
  In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration. A fax connection using T.38 requires approximately 20 kbits/s.

9 Number of channels:
Enter how many calls may be routed via this trunk at the same time. The maximum number of channels available is determined by the codec used and the bandwidth of the connection between the headquarters and branch office.

10 Computer name:
Apply the default computer name.

11 Click "Finish".
The new Trunk is created, and is available for further configuration.

For changing the SIP Trunk properties subsequently, see *19.5 Configuring a SIP Gateway Trunk*, Page 323.

19.5 CONFIGURING A SIP GATEWAY TRUNK

When you have created a SIP gateway trunk as described in *19.4 Creating a SIP Gateway Trunk*, Page 322, you can subsequently change the settings of this trunk in the SwyxWare Administration.

When parameters of a trunk are changed, this change takes effect at once. There is no need to halt and restart any services for this.

How to configure a SIP gateway trunk

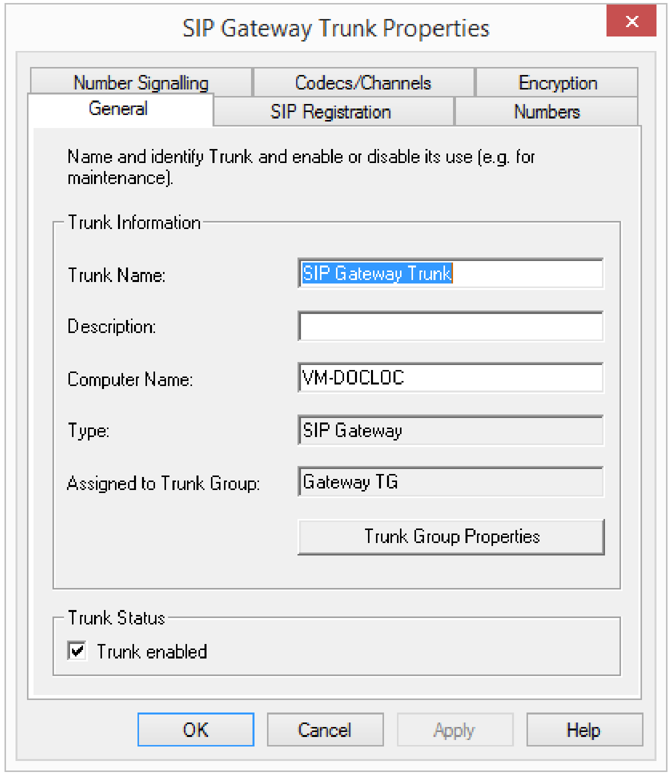
1 Open the SwyxWare Administration and choose the SwyxServer.

2 In the left side of the SwyxWare Administration window, click on "Trunks", and in the right-hand window select the trunk you want to configure.

3 In the context menu, select "Properties".
In each case, the "Properties of..." window will appear.

Any changes to the configuration of a SIP gateway trunk must also be made in the configuration of the gateway.

The "General" Tab



SIP Gateway Trunk Properties

Name and identify Trunk and enable or disable its use (e.g. for maintenance).

Trunk Information

Trunk Name: SIP Gateway Trunk

Description:

Computer Name: VM-DOCLOC

Type: SIP Gateway

Assigned to Trunk Group: Gateway TG

Trunk Status

☑ Trunk enabled

In this tab you can modify the name and description of the trunk.

Trunk information:

In the fields "Trunk Name" and "Description" you will find the descriptive information that is displayed in Administration.

The field "Computer Name" contains the name of the computer in which the service (LinkManager or SwyxGate) is installed.

The "Type" field indicates the type of the trunk, and "Trunk Group" the assigned Trunk Group. Both parameters cannot be retrospectively changed.

Using "Trunk Group Properties..." You will open the Properties of the according Trunk Group. You can edit the Properties of the Trunk Group directly.

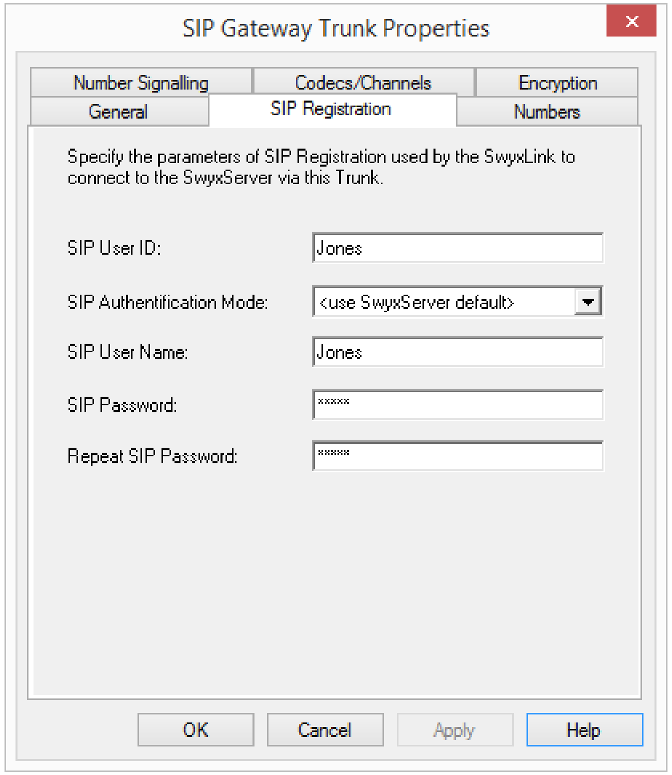
Trunk status:

If you deactivate the checkbox "Trunk enabled", this gateway is blocked for further incoming or outgoing calls.

It won't be written in the change log, if a trunk was activated or deactivated.

The "SIP Registration" Tab

The SIP access parameters of the gateway, which the latter will use to establish a connection to the SwyxServer, appear on this tab.



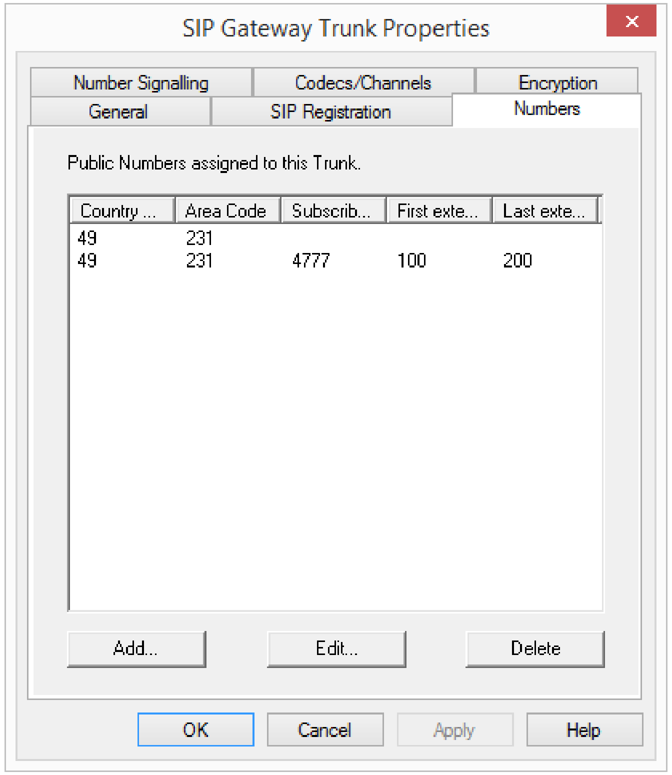
Specify the parameters of SIP Registration used by the SwyxLink to connect to the SwyxServer via this Trunk.

SIP User ID:	Jones
SIP Authentification Mode:	<use SwyxServer default>
SIP User Name:	Jones
SIP Password:	*****
Repeat SIP Password:	*****

Enter the parameters the SIP gateway needs to log on to SwyxServer via this trunk.

- SIP User ID:
  The user ID is combined with the realm to create the SIP address (URI).
- SIP Authentication method:
  Indicate whether or not the gateway needs to authenticate itself.
- SIP user name and password:
  The user name and password are required for authentication.

The "Numbers" Tab



Public Numbers assigned to this Trunk.

Country ...	Area Code	Subscrib...	First exte...	Last exte...
49	231			
49	231	4777	100	200

The following settings can be made:

Public numbers of this trunk

You can specify here which public numbers this trunk uses. External calls to these numbers go over this trunk. Calls with a Calling Party Number that is assigned to this trunk are routed over this trunk.

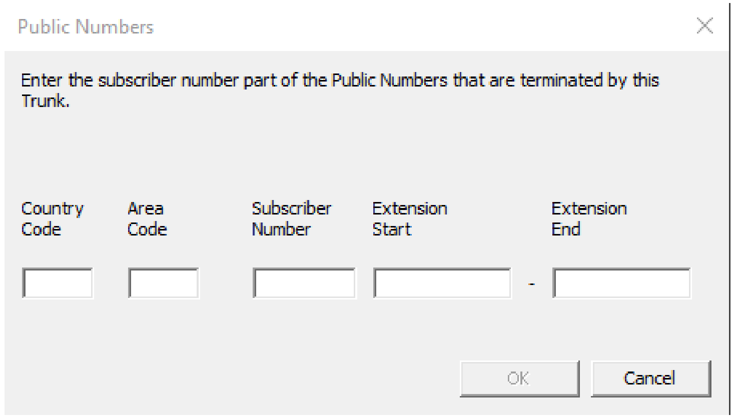
To ensure the unambiguity of the information, you must enter the complete phone number from SwyxWare V.13.20 onwards. In the new "Subscriber number" input field, enter the part of the phone number that follows the area code and precedes the extension (internal phone number).

	Country code	Area code	Subscriber number	First extension	Last extension
e. g.	49	231	4777	100	200

This is how you add numbers for this trunk

The existing phone number entries are automatically extended by the new entry field "Subscriber number" when updating to V.13.20. Make sure that the automatic allocation is correct and adjust the corresponding entries manually as required.

1 Click on "Add".
The "Public numbers" window will appear.



Public Numbers

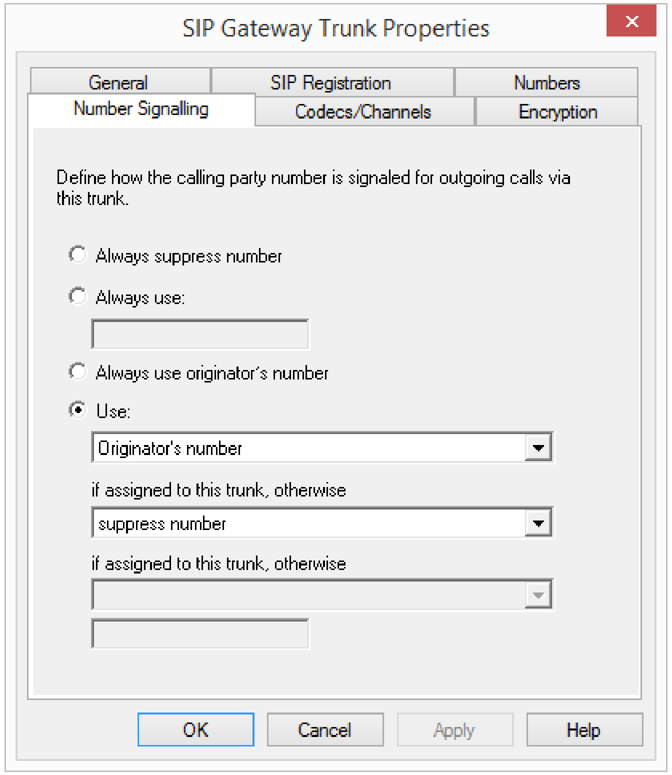
Enter the subscriber number part of the Public Numbers that are terminated by this Trunk.

2 You can add either an individual number or a range of numbers.

3 End your inputs with "OK".

To add several numbers or ranges, simply select "Add" the relevant number of times.

"Number signaling" tab



SIP Gateway Trunk Properties

Define how the calling party number is signaled for outgoing calls via this trunk.

○ Always suppress number

○ Always use:

○ Always use originator's number

● Use:

Originator's number

if assigned to this trunk, otherwise

suppress number

if assigned to this trunk, otherwise

The following settings can be made:

- Always suppress number
  In this case no number is signaled to the person being called (XXX), regardless of which number was configured for this trunk.

In Germany, the destination numbers 110 and 112 are reserved for emergency calls. The outgoing call number to these destination numbers is always signaled.

- Always Use This Number:
  You can specify a number or SIP-URI here which will always be signaled to the person being called (e.g. the operator's number), regardless of which number was configured for this trunk.

The number must be entered in canonical number format.

- Signal Caller Number
  Although the caller number is not configured for this trunk, the caller number is signaled to the person being called.

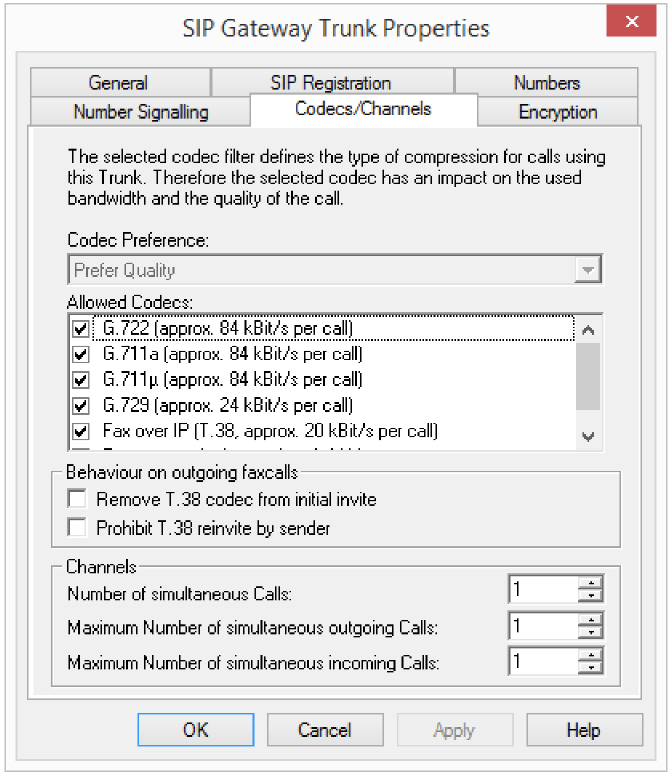
  Example:

  Customer A (number 88 333 44) calls employee B (number 55 666 77). Forwarding to his mobile phone is activated, i. e. an incoming call is routed outwards again. If the customer's number (88 333 44) should also be signaled externally, then this can be allowed here, although this number was not defined for this trunk.
- Use:
  You can specify here which number this trunk uses. You can specify the action for numbers that are assigned to this trunk as well as for numbers which have no assignment.

Use:	If assigned to this trunk, otherwise:	If assigned to this trunk, otherwise:	Entry
Origination Number	Number of the transferor		
	Hide number		
	Don't use this trunk		
	Use the following number		<Number>
Number of the transferor	Origination Number	Hide number	
		Don't use this trunk	
		Use the following number	<Number>
	Hide number		

For Number Signalling, the line characteristic "Clip no Screening" must be enabled on the line, otherwise the number is suppressed.

The "Codecs/Channels" Tab



SIP Gateway Trunk Properties

The selected codec filter defines the type of compression for calls using this Trunk. Therefore the selected codec has an impact on the used bandwidth and the quality of the call.

Codec Preference: Prefer Quality

Allowed Codecs:
☑ G.722 (approx. 84 kBit/s per call)
☑ G.711a (approx. 84 kBit/s per call)
☑ G.711µ (approx. 84 kBit/s per call)
☑ G.729 (approx. 24 kBit/s per call)
☑ Fax over IP (T.38, approx. 20 kBit/s per call)

Behaviour on outgoing faxcalls
□ Remove T.38 codec from initial invite
□ Prohibit T.38 reinvite by sender

Channels
Number of simultaneous Calls: 1
Maximum Number of simultaneous outgoing Calls: 1
Maximum Number of simultaneous incoming Calls: 1

The following settings can be made:

Codecs

Here you can define the type of compression to be used on this connection.

Specify which Codecs should be permitted for this trunk.

- Voice, low bandwidth (G.729)
  High compression. A voice connection requires approximately 24 kbits/s.
- Voice, highest bandwidth (G.722)
  HD quality
- Voice, high bandwidth (G.711a, G.711µ)
  The voice data is slightly compressed. This keeps the packet delay time in the LAN (Local Area Network) to a minimum. A voice connection requires approximately 64 kbits/s.
- Fax over IP
  In this case, the special fax protocol T.38 is used, which takes the set-up of the IP network into consideration. A fax connection using T.38 requires approximately 20 kbits/s.
  Click on "Next>".

If there are several voice codecs selected, SwyxServer will filter voice data according to the current settings. The communicating sides will have to decide which voice codec to use.

It won't be written in the change log, if a Codec was activated or deactivated. See *7.7 Change log*, Page 117.

Action on fax receipt

When a fax connection is set up, the T.38 protocol is negotiated between the two devices involved. Certain variants of this negotiation may not be supported by some IP adapters. Use the following filter options to establish compatibility with such devices.

- Remove T.38 codec from initial invite
  Some IP adapters cannot correctly interpret an initial connection request which includes T.38 as well as voice Codecs.
  If this option is set, SwyxServer removes T.38 from the initial connection request. The fax devices first set up a voice connection and then switch to the fax protocol T.38 because of the fax tone (CED tone, 2100Hz).
- Prohibit T.38 reinvite by sender
  The receiving fax device switches to T.38 after detecting the fax tone (CED tone, 2100Hz). Alternatively, the switch to T.38 can be carried out by the sending fax device.
  Some IP adapters don't support switching by the sender.
  If this option is set, SwyxServer suppresses a switch to T.38 by the sender.

If the receiving side involves a combined phone/fax device (fax switch), a fax data transmission is impossible when the option "Prohibit T.38 reinvite by sender" is activated.

The filter options can only be set when the Codec "Fax over IP (T.38...)" is activated.

Channels

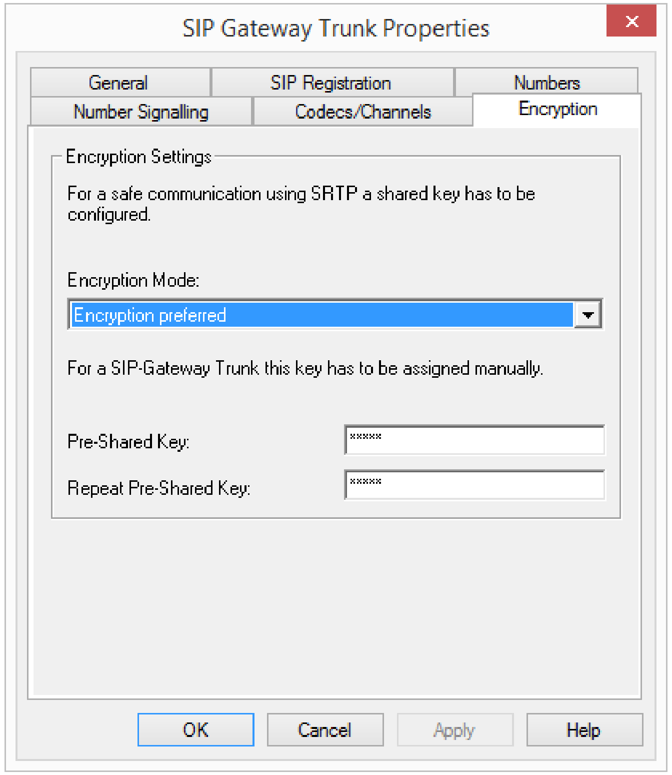
Specify how many channels (connections) should be routed simultaneously via this trunk and forwarded from there to the public network. You can also determine how many outgoing and/or ingoing connections are established at most.

The maximum number is determined by the gateway used.

If channels were added or removed, you will find these changes in the change log.

See also *7.7 Change log*, Page 117.

The "Encryption" tab



Encryption Settings

For a safe communication using SRTP a shared key has to be configured.

Encryption Mode: Encryption preferred

For a SIP-Gateway Trunk this key has to be assigned manually.

Pre-Shared Key: *****

Repeat Pre-Shared Key: *****

You can specify here how and whether voice data going via this trunk should be encrypted.

Encryption mode

This is where you specify the mode of encryption for this trunk. The following encryption modes are available:

- No encryption
  If "No encryption" is selected, the voice data going via this trunk is not encrypted. If the encryption mode was set to "No encryption" within the server properties, the mode is likewise set to "No encryption" here, and cannot be changed. The field is then deactivated.
- Encryption preferred
  When "Encryption preferred" is selected, the voice data is only encrypted if the gateway likewise supports encryption. If this is not the case, the voice data is not encrypted, but phoning is still possible.
- Encryption mandatory
  When "Encryption mandatory" is selected, voice data encryption is obligatory. This means that either encryption always occurs or the call is aborted with the reason "Incompatible encryption settings". This can be the case, for example, if the gateway does not permit any encryption.

> If the encryption mode was set to "No encryption" within the server properties, the mode is likewise set to "No encryption" here; if "Encryption mandatory" was configured there, then the setting "Encryption mandatory" also appears here. In both cases, the mode cannot be changed. The field is then deactivated.

See also *21 Encryption*, Page 342.

Key (PreSharedKey)

To ensure secure communication by SRTP between SwyxServer and gateway, a common key (PreSharedKey) must be defined between them.

For all components which use the SwyxWare database (e.g. SwyxIt!, PhoneMgr, LinkMgr, ConferenceMgr,), this key is automatically generated by SwyxServer and distributed to the relevant component, once again encrypted.

It is different for the SIP gateway trunk. In this case the key must be entered manually. In addition, the key stored here must also be entered on the gateway.

> A key length of less than 10 characters is not advisable. Longer keys offer greater security, and keys can be up to 128 characters long. In order to make brute-force or dictionary attacks more difficult, the key should consist of a combination of letters, numbers and special characters.

See also *21.1 Encryption within SwyxWare*, Page 342.

This is how you specify the encryption mode for a SIP link trunk

1. Start the SwyxWare Administration and log in to the SwyxServer.
2. In the left side of the SwyxWare Administration window, click on "Trunks", and in the right-hand window select the trunk you want to configure.
3. Select "Properties".
4. Select the "Encryption" Tab.
5. In the field "Encryption mode", choose from:
   - No encryption
   - Encryption preferred
   - Encryption mandatory
6. Enter the key in the "Key" field. The key must also be entered on the gateway.
7. Click on "OK".

19.6 CONNECTING THE GATEWAY TO SWYXWARE

For information on how to connect a gateway with a SwyxWare, see

HOW TO: SwyxON: How to connect a LANCOM 1783 VA to a UC Tenant (VPN information) (kb5069)

INFO: SwyxON: IPsec VPN parameters for VPN clients (kb5073)

INFO: SwyxON: Configuration of Swyx with gateways for connection to SIP providers

(You may need to be logged in to view the content)

20 CONNECTION OF SWYXPHONE AND SWYXIT!

Requirements and configuration of SwyxServer for the operation of SwyxIt! and SwyxPhone

Depending on the telephony device (SwyxPhone Lxxx or SwyxIt!) and its use, you will need different licenses, see *3 Licensing via license key*, Page 28 or *2 Online Licensing*, Page 21. All of these licenses are entered in the SwyxWare Administration, see *7.5.5 The "Licenses" Tab*, Page 91.

Licenses for System Phones

When using SwyxWare, you can also make calls with SIP telephones and so-called system telephones in addition to a telephony client. Valid system phones here are desk phones from third-party manufacturers.

A separate system phone license is required for each system phone that is to be operated using SwyxWare. If telephones are purchased as part of a SwyxWareinstallation (SwyxPhone), this single license is included, i.e. either SwyxServer recognizes the SwyxPhone automatically (whitelist), see *Install and update Whitelist*, Page 331, or a single license must be entered for the system telephone, see *7.5.5 The "Licenses" Tab*, Page 91.

> If a system telephone cannot register due to missing licenses and you do not have any licenses, please contact the supplier of this system telephone.

> A telephone license does not include a user license, it only serves to authorize the system phone to SwyxServer.

> If a user is logged on to SwyxServer with a SwyxIt! and a system telephone at the same time, they only need a user license for this, but also a license for the system telephone if it is not a SwyxPhone.

Install and update Whitelist

If SwyxPhone displays the error message "No license available" during logon, check the number of user licenses.

If sufficient user licenses are present, but the logon fails, download the current Whitelist.

You will find the most up-to-date SwyxPhone Whitelist on the download page in the Support area or on the Enreach FTP server:

ftp://ftp.swyx.com/pub/phonewhitelist/phonewhitelist.msi

To install the Whitelist, start the .msi file.

Automatic Updates

For automatic updating of the whitelist you should create a task in the SwyxServerConfiguration Wizards. See also *5.4.2 Configuring SwyxWare*, Page 54 step (31).

> In SwyxON the whitelist is updated automatically by default.

The task appears in the Windows task planning (under the name "PhoneWhitelistUpdate") and is executed via presetting daily at 2 a.m.. The precise starting time is moved using random time delay in order to hinder overburdening the update server.

> Your own settings for the "PhoneWhitelistUpdate" task are reset to the preset SwyxServer next time the configuration wizard is executed.

The task replaces the existing whitelist with a new one which is downloaded from the update server.

You will find information on the (successful) actions in the Windows event display under "Windows logs | Application". Look for the line marked in the "Source" column as "Phone Whitelist Update".

Licenses for SwyxIt!

The number of telephony clients who can log on to SwyxServer is limited to four per user. This means that a user can e.g. log on simultaneously to a SwyxIt!, additional SwyxPhones at the workstation and a further SwyxPhone in the conference room.

SwyxWare

The purchased user numbers limit the number of different users logging in simultaneously to SwyxServer; it is possible to configure more users than the number licensed.

SwyxWare for DataCenter and SwyxON

All configured or ordered users are recorded in the usage report and thus licensed. (*11.4 Activate/deactivate or delete users*, Page 207).

20.1 GENERAL NETWORK CONFIGURATION (DHCP/DNS/WINS SERVICES)

This chapter describes the various ways a SwyxPhone and SwyxIt! used in a company can get the necessary network information.

To run SwyxWare there must be three services available:

- DHCP (Dynamic Host Configuration Protocol)
  Distribution of the IP addresses to the telephony clients
- WINS (Windows Internet Name Service)
  Resolution of the NetBIOS name to the IP addresses
- DNS (Domain Name System)
  Resolution of the FQDN (Fully Qualified Domain Name) to the IP addresses

20.1.1 DHCP-SERVER (DYNAMIC HOST CONFIGURATION PROTOCOL)

A DHCP server should be used for distributing unique IP addresses to the telephony clients. The following clients are suitable for this:

- SwyxPhone L6xx
- SwyxIt! (not from Windows Vista on)

The DHCP server is a component of the Windows Server operating system and it offers the following advantages:

- Unique and specific assignment of IP addresses
- Automatic transmission of the SwyxServer IP address to the telephony clients
- The DHCP server offers you the option forwarding changes to the IP address of the client directly to the DNS server. This is important in order to keep the assignment of the IP address to FQDN (Fully Qualified Domain Name) of the computer consistent.

If there is no DHCP server in the network, install a DHCP server on the SwyxServer computer.

How to install a DHCP server

1. Click on "Start | Settings | Control Panel."
2. Double click on "Software" and then select "Add/Remove Windows Components".
3. In the wizard for Windows components, select "Components | Network Services | Details".
4. Activate the checkbox DHCP (Dynamic Host Configuration Protocol) in the "Network Services" dialog field.
5. Then click on "OK".
6. Click in the wizard for Windows components on "Next" in order to execute the installation.
7. After the completion of the setup, click on "Finish".
8. The Windows DHCP server is installed and is then available to you.

The DHCP server offers you the option forwarding changes to the client IP address directly to the DNS server. This is important in order to keep the assignment of the IP address to FQDN (Fully Qualified Domain Name) of the computer consistent.

This is how you configure the DHCP server for dynamic update

1. Start the DHCP Administration in Windows under "Start | Administration".
2. Click with the right mouse button on the server and select "Properties".
3. Click on the "DNS" tab.
4. Activate the checkbox "Automatically update DHCP client information in DNS".

In order for the Windows client computers to receive the IP address of the WINS and DNS servers, these must be entered on the DHCP server as DHCP options:

- 006 DNS Server
- 044 WINS/NBNS Server

Please note that the query of server information via DHCP is only possible for clients with Windows2000 or later.

20.1.2 WINS (WINDOWS INTERNET NAME SERVICE)

The service WINS resolves NetBios names into IP addresses and is therefore an elementary component of a Windows network. Given this fact, this service should already be installed on the Windows Server located in the network.

This is how you install WINS (Windows Internet Name Service)

1. Click on "Start | Settings | Control Panel."
   Double click on "Software" and then select "Add/Remove Windows Components".
2. In the wizard for Windows components, select "Components | Network Services | Details".
3. Activate the checkbox "WINS (Windows Internet Name Service)" in the dialog field "Network Services".
4. Then click on "OK".

The WINS server can update the resource entries in the DNS server.

A more extensive configuration of the WINS is not necessary.

20.1.3 DNS (DOMAIN NAME SERVICE)

The service DNS resolves the names of the client FQDN, domains, locations and services in the Active Directory in an IP address. If there is no DNS server in the network, install it on the SwyxServer PC.

How to install the DNS server

1. Click on "Start | Settings | Control Panel."
2. Double click on "Software" and then select "Add/Remove Windows Components".
3. In the wizard for Windows components, select "Components | Network Services | Details".
4. In the dialog field "Network Services", activate the checkbox DNS (Domain Name System).
5. Then click on "OK".
6. Click in the wizard for Windows components on "Next" in order to execute the installation.
7. After the completion of the setup, click on "Finish".
8. The Windows DNS server is installed and is then available to you.

Dynamic update must be enabled on the DNS server. Dynamic updates makes it possible for important client computer changes, such as IP address, to be registered on a DNS server and to be dynamically updated there. This reduces the manual administration particularly in the case of client computers, which have been assigned an IP address based on DHCP.

Please note that the query of server information via DNS is only possible for clients with Windows2000 or later.

This is how you configure the DNS server for dynamic update

1. Open the DHCP Administration in Windows under "Start | Administration".
2. Select the appropriate zone in the console structure.
3. Select "Properties" in the "Action" menu.
4. Check on the "General" tab whether "Active Directory integrated" is selected as zone type.
5. Click in the Allow Dynamic updates? list on "Yes".

The WINS resolution for DNS must be activated on the DNS server. In this case, the WINS server will be queried if a client name cannot be resolved per DNS.

This is how you activate the WINS resolution for the DNS server

1. Open the DHCP Administration in Windows under "Start | Administration".
2. Click on the appropriate zone in the console structure.
3. Click on "Properties" in the "Action" menu.
4. Click on the corresponding tab "WINS" or "WINS-R".
5. Activate the checkbox "Use WINS Forward Lookup" in order to enable the use of WINS resolution.
6. Enter the IP address of a WINS server, which is to be used for the further resolution of names that could not be found by the DNS server.
7. Click on "Add" in order to add the IP address of the WINS server to the list.
8. If necessary, activate the checkbox "Do not replicate this record" for the WINS entry.
9. Close the DNS administration.

When using dynamic update, the resource entries are automatically added when computers are started in the network. In some cases these are not automatically deleted if the computers are removed from the network. If a computer e.g. registers its own resource entry for the host (A entry) while starting and if this computer is later disconnected from the network improperly, its resource entry for the host (A entry) can no longer be deleted. If there are e.g. mobile computers in the network, this may occur more frequently. A DNS server which loads the obsolete resource entry, will then sent obsolete information as an answer to queries. This will result in name resolution problems in the network. In order to avoid these problems, the DNS server provides the "Aging" mechanism for resource entries. Please see the Microsoft documentation for more detailed information on this topic.

20.2 USE OF SWYXPHONE LXXX

The SwyxPhone Lxxx series includes the following telephones:

- SwyxPhone L62, SwyxPhone L64, SwyxPhone L66, SwyxPhone L615, SwyxPhone L640, SwyxPhone L660.

If you use SwyxPhone Lxxx in your SwyxWare scenario, you can find detailed operating information here for SwyxPhone Lxxx.

- Distribution of the PhoneManager IP address to the SwyxPhone Lxxx
- Initial operation of the SwyxPhone Lxxx
- Automatic Firmware Update for a SwyxPhone Lxxx

20.2.1 DISTRIBUTION OF THE PHONEMANAGER IP ADDRESS TO THE SWYXPHONE LXXX

The PhoneManager distributes its IP address to the SwyxPhones from a central location, so that they log on to the PhoneManager when started. You must configure the necessary parameters in the SwyxWare Administration and then start the scan, i.e. the search for the SwyxPhone Lxxx, in the IP address ranges configured there (*7.5.14 The "Search SwyxPhones" Tab*, Page 105).

The IP address of the responsible PhoneManager remains permanently intact in the SwyxPhone. For this reason, this process only needs to be started if new SwyxPhones are to be operated in the network.

20.2.2 CORRECT TIME TO CONNECT TO SWYXSERVER

For connections to the SwyxServer, the correct time has to made available to all SwyxPhones.

Time differences between SwyxServer and SwyxPhones may result in errors during logon to SwyxServer and during call setups.

The correct time should thus setup at all SwyxPhones by means of a time server (NTP).

A Windows domain controller can be used as a NTP server.

The IP address of the NTP server should be distributed via DHCP (option 42). Alternatively you can configure the NTP server via the web interface of the phone.

The time of the NTP server will only be internally used by the phone.
The time appearing in the display depends on the assigned location of the SwyxWare user.

SwyxPhones require the correct time for connections to the SwyxServer
service.swyx.net/hc/en/articles/360000014639

20.2.3 INITIAL OPERATION OF THESWYXPHONE LXXX

When the phones are set up at the workstations and connected to the network, SwyxWare Administration is used to search for the new phones and distribute the IP address of the PhoneManager.

Please note that for a successful assignment of the user account, the automatic log in must be enabled and the field for the MAC address must be empty. This will be the case for both when dealing with a newly created user. See *11.2.1.6 The Tab "SwyxPhone Lxxx"*, Page 171.

See also the SwyxPhone documentation.

How to install SwyxPhone Lxxx with display

1. Start SwyxWare Administration.
   In the Server Properties open the "SwyxPhone Search" tab.
2. Enter the IP address range from which the IP addresses (per DHCP) will be assigned.
3. Begin the search by clicking on "Start".
   The PhoneController stops the search automatically after an hour.
4. Connect one or more SwyxPhones on to the LAN and the power supply.
   SwyxPhone is found by the PhoneController and logs on to the PhoneManager using the assigned IP address.
5. On the display of the SwyxPhone Lxxx the prompt for PIN entry will appear.
   If the user enters his PIN and confirms this with "OK", the SwyxPhone is then logged in.

20.2.4 AUTOMATIC FIRMWARE UPDATE FOR A SWYXPHONE LXXX

Firmware is the software installed on SwyxPhone itself. It can be updated automatically, i.e. the update is controlled by SwyxServer.

It may happen that the PhoneManager requests an Update of the SwyxPhone firmware. The menu of the SwyxPhone points out if the automatic updates is not activated.

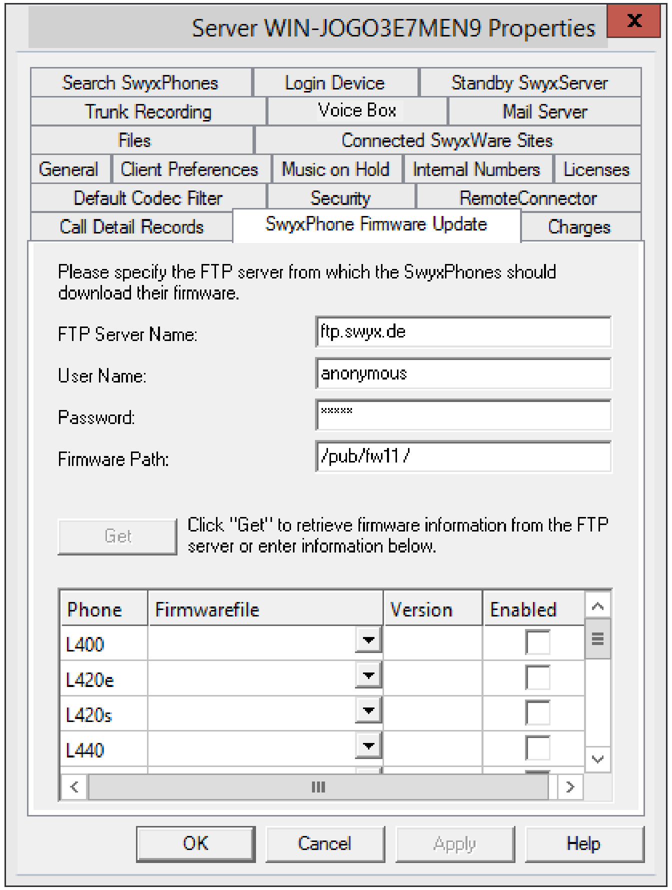
On every start, SwyxPhone Lxxx compares its own firmware with that configured on the server. If these versions differ, the user is requested on the SwyxPhone Lxxx to confirm the software update with OK. During the update SwyxPhone downloads the current firmware version from an FTP server. You can use an FTP server from your network, or you can use the FTP server provided by Enreach on the Internet for this purpose.

This is how you set up the automatic firmware update on the SwyxPhone Lxxx

1 Open the SwyxWare Administration.

2 In the context menu, select "Properties".
The "Properties of..." window will appear.

3 Switch to the "SwyxPhone firmware update" tab:



Please specify the FTP server from which the SwyxPhones should download their firmware.

FTP Server Name: ftp.swyx.de

User Name: anonymous

Password: *****

Firmware Path: /pub/fw11 /

Click "Get" to retrieve firmware information from the FTP server or enter information below.

Phone	Firmwarefile	Version	Enabled
L400			☐
L420e			☐
L420s			☐
L440			☐

4 Enter the corresponding data in the tab.

- Name of the FTP server
- User name, e.g. ‘anonymous’
- password (you have to enter your own password)
- Directory on the FTP server under which the files containing the current firmware version can be found (e. g. /pub/fw11).

The firmware path and the file name should each not exceed 80 characters.

5 Indicate which software should be used for the update.
You can get the current firmware information from the FTP server listed by clicking on "Get". Then you can select the appropriate firmware version for the SwyxPhone from the drop-down list.

6 Activate the automatic update for the telephone model to be updated.

7 Confirm your entries by clicking on "OK" and close the SwyxWare Administration.

When you restart a SwyxPhone, and after a user logs off from SwyxPhone, the firmware version is compared and if necessary you will be prompted to update your firmware. If you want the firmware query to be displayed on all SwyxPhones, restart the SwyxPhoneManager service.

Please verify that the firmware version in the SwyxWare Administration is the same as the version of the files on the FTP server. Otherwise the user will always be asked to update.

20.3 USE OF SWYXIT!

If you use SwyxIt! in your SwyxWare scenario, you can find detailed operating information here for SwyxIt!.

- Distribution of the SwyxServer IP address to SwyxIt!
- Using SwyxIt! from home office
- SwyxIt! installation from the Command Line
- Customer-specific context menu for Speed Dials
- SwyxIt! Web Extension
- Use of System Variables
- Automatic distribution of SwyxIt! in a network

When uninstalling SwyxIt!, please note that some data can only be deleted manually from the respective directory. This includes the trace files in the temp folder (%temp%\Swyx\Traces\SwyxIt!.log), the files stored in the user directory of the operating system (C:\Users\[User]\AppData\Local\Swyx) and the credentials of the SwyxIt! user in the Windows-registry (Computer\HKEY_CURRENT_USER\Software\Swyx\CommonLogin\CurrentVersion\Options\).

20.3.1 DISTRIBUTION OF THE SWYXSERVER IP ADDRESS TO SWYXIT!

SwyxIt! receives the required IP address of the SwyxServer via DHCP/ DNS.

Windows does not support the manufacturer-specific DHCP option 43. Please use the DNS method for distributing the SwyxServer addresses (*Configuration of DNS Server for SwyxIt!*, Page 337).

SwyxIt! needs the following information for the IP configuration:

- IP Address of the SwyxServer

DHCP Configuration of SwyxIt!

This information is transferred to SwyxIt! via DHCP:

ID (dec)	Name	Meaning
43	Vendor Specific Info	IP Address of the SwyxServer

Example:

If the IP address of SwyxServer is e. g. 10.20.30.40,

and the IP address of the standbySwyxServer 60.70.80.90 (obsolete)

The following byte sequence must then be entered:

decimal	73	80	80	66	88	83	82	86	10	20	30	40	60	70	80	90
hexadecimal	49	50	50	42	58	53	52	56	0a	14	1e	28	3d	48	50	5a

The beginning of the byte sequence (73, 80, 80, 66, 88, 83, 82, 86 which is equivalent to the string "IPPBXSRV") serves an identification purpose and it helps to prevent a misconfiguration if this option is used elsewhere.

Please note that the byte sequence for identification (73, 80, 80, 66, 88, 83, 82, 86 corresponds the string "IPPBXSRV") must always have eight bytes defined.

Configuration of DNS Server for SwyxIt!

In order for the terminal devices to contact the DNS server, they must know the IP address of the DNS server and the domain name for the request to the DNS server. This can be transmitted to the telephone per DHCP using the standard DHCP options or it can be entered into the telephone manually. The latter has the disadvantage that the DNS server IP address must be configured individually for each device in the network.

The SwyxIt! query of the DNS server is made via the DNS A record "ippbxsrv. <domain>", where <domain> stands for the Internet domain name (analog: "ippbxsrvfallback.<domain>" for FallbackSwyxServer). The answer of the DNS server then contains its IP address.

The DHCP options required for the use of the DNS server:

ID (dec)	Name	Meaning
6	DNS Option	DNS Server IP Address
15	Domain Name Option	Domain name of the Subnet

The dynamic query of the server information is supported by the clients in Windows 2000 or higher.

20.3.2 AUTOMATIC DISTRIBUTION OF SWYXIT! IN A NETWORK

Automatic installation or updating of SwyxIt! can be implemented in various ways:

You will find detailed information in the Knowledgebase:

Distribution of SwyxIt! via Swyx Control Center

Distribution of SwyxIt! via logon script

Distribution of SwyxIt! through group guidelines of the Active Directory

(You may need to be logged in to view the content)

20.3.3 USING SWYXIT! FROM HOME OFFICE

If SwyxIt! is going to be used from the field or a home office outside the company network, then it is recommendable to use a direct connection to SwyxServer via SwyxRemoteConnector.

See also *26.1 Internet connection via RemoteConnector*, Page 385.

20.3.4 SWYXIT! INSTALLATION FROM THE COMMAND LINE

You can also start the installation of SwyxIt! by opening it via the command line. For this type of installation it is always advisable to create a log file (msiexec /l). Start the installation with the command "msiexec /i". You can control the scope and the progress of the installation with certain parameters.

Example 1:

You want to install SwyxIt! without additional functions, along with the Quickstart documentation. The installation should take place without user intervention (silent installation):

```
msiexec /i "SwyxIt!EnglishUK64.msi" /qb+
ADDLOCAL="PhoneClient,Quickstart"
```

Example 2:

You want to install SwyxIt! with all available functions, in a specified directory. SwyxIt! Should be installed in CTI mode, in a silent installation, and a log file should be written.

```
msiexec /i "SwyxIt!EnglishUK64.msi" /qb+ ADDLOCAL=ALL
INSTALLDIR="C:\Program Files\SwyxIt!" REGCTISETTING=#1
/l*v %temp%\SwyxIt!_install.log
```

Example 3:

You want to install SwyxIt! with all available functions, along with the Quickstart documentation. The user should have the chance to alter these parameters through the installation wizard's interface during installation:

```
msiexec /i "SwyxIt!EnglishUK64.msi" ADDLOCAL="All"
```

Example 4:

You would like to install SwyxIt! with deactivated status signaling. The checkboxes on the "Extended Status Information" tab under "Settings | Local Configuration"are deactivated:

```
msiexec /i "SwyxIt!EnglishUK64.msi"/qb `
RP_IDLE=0 `
RP_IDLE_TIME=120000 `
RP_LOCKED=0 `
RP_SCREEN=0 `
RP_APPOINTMENT=0 `
RP_APPOINTMENT_STATUS=0;
```

You can use the following parameters

:

Parameter	Explanation
msiexec /i	Start of installation
SwyxIt!EnglishUK32.msi or SwyxIt!EnglishUK64.msi	Name of installation file Please select the MSI installation file according to your operating system (32bit or 64bit). Please verify the correct designation.

Parameter	Explanation
/qb+	**Silent installation** The installation of SwyxIt! does not require any user entries. If you don't use this parameter, the installation wizard is started as for the normal installation. Each separate step must then be confirmed with the "Next" button, and the predefined options can be changed.
ADDLOCAL	**Definition of the functions** You will find the available features and components in the following table.
/l*v	**Generation of a detailed log file during the installation** A log file (*.log) enables you to detect errors during the installation. The directory to which the log file will be written must already exist.
REGCTISETTING	**Specification of the CTI setting (REGCTISETTING=#1)** With this option you can define whether SwyxIt! is executed directly after installation in the CTI mode. The user can also change this setting later via the SwyxIt! interface.
INSTALLDIR	**Specification of the installation directory** This option allows you to set the directory in which SwyxIt! is to be installed.
/help	**Help function** This option displays further parameters of the Windows Installer, which you may be able to use.

The following table contains the functions valid for ADDLOCAL:

Parameter	Component name
All	All available options are installed (see note after the table).
PhoneClient	SwyxIt!
ScriptEditor	Graphical Script Editor (Subfunction of PhoneClient)
OfficeUCSupport	Office Communication Add-In (Subfunction of PhoneClient)
Outlook2007Support	Outlook Add-In (2007 or later) (Subfunction of PhoneClient)
EstosAccess	Swyx VisualContacts (Subfunction of PhoneClient)
DatevIntegration	Swyx Connector for DATEV (Subfunction of PhoneClient)
NotesAccess	Lotus/IBM/HCL Notes Plugin (Subfunction of PhoneClient)
Video	Video function in SwyxIt!
TeamViewer	TeamViewer function for Collaboration (Subfunction of PhoneClient)
NetViewer	Netviewer function for Collaboration (Subfunction of PhoneClient)
ClientMeeting	SwyxIt! Meeting function for Collaboration (Subfunction of PhoneClient)
CLMgrTSP	TAPI Service Provider (Subfunction of PhoneClient)
DesktopShortcut	Desktop link for SwyxIt! (Subfunction of PhoneClient)
StartupShortcut	Add SwyxIt! to Startup group (Subfunction of PhoneClient)
Quickstart	Quickstart documentation for SwyxIt! (Subfunction of PhoneClient)
FaxClient	SwyxFax Client
DesktopShortcutFaxClient	Desktop link for SwyxFax Client (Subfunction of FaxClient)
StartupShortcutFaxClient	Add SwyxFax Client to Startup group (Subfunction of FaxClient)
SwyxMeeting	Swyx Meeting – Internal and external
FAnalytics	Swyx Analytics: Extension for the analysis of corporate communication on the basis of the generated call data

Parameter	Component name
MsTeamsIntegration	Integration with Microsoft Teams
MsTeamsIntegration-Settings	SwyxIt! default settings for the Swyx Connector for Microsoft Teams
DiscoveryService	Service for Swyx Connector for Microsoft Teams Support on Terminal Servers
Auth0Client	Auth0 Authentication

20.3.5 CUSTOMER-SPECIFIC CONTEXT MENU FOR SPEED DIALS

For better integration of external applications (3rd party), SwyxIt! has been enhanced with a function that allows the customer's own entries to be added to the context menu of the Speed Dials. Applications are started with parameters of this Speed Dial, or of the current or last call of the currently selected Line button.

In order to add individual entries to the context menu of the Speed Dials, corresponding keys must be created in the Windows registry. The entries are later displayed in the context menu under the existing entry "Send email...".

Any number of keys can be created on the following registration path, which then represent the new context menu entries along with the associated command line and the working directory.

```
HKLM\SOFTWARE\Swyx\SwyxIt!\CurrentVersion\Options\SpeedDialMenus
HKCU\SOFTWARE\Swyx\SwyxIt!\CurrentVersion\Options\SpeedDialMenus
```

Such an entry has the following structure:

Key "Key1"

```
String "MenuLabel" (e.g. "Video_conference")
String "CommandLine" (e.g. "c:\test.exe %SpeedDialPeernumber%")
String "WorkingDirectory" (e. g. "c:\")
```

In this example, an entry named "Video_conference" is added to all Speed Dials. If this new entry is selected, then the program "c:\test.exe" is started with the configured parameters in relation to the selected Speed Dial.

As soon as the menu item is selected, the variables are replaced by the real values. The values used always relate to the chosen Speed Dial or the selected line. If the selected line is not being used at the time or is even deactivated, the information from the last call is used.

In "CommandLine", any program that can be executed by Windows can be used, for example

- notepad
- c:\test.doc
- c:\windows\notepad.exe
- enreach.de/en

In both "CommandLine" and "WorkingDirectory", the inputs can be entered in quotes (e.g. "c:\Programme\test\test.exe" %SelLinePeernumber%).

To start a VB script via a context menu entry, the command line entry must be constructed as follows

```
wscript.exe "C:\CallTo.vbs" %SelLinePeernumber%
```

The working directory is then "C:\". Variable names are not case-sensitive.

The values for variable replacement do not contain inverted commas, so it is advisable to include these already in the command line entry.

```
"c:\Programme\test\test.exe" "%SelLinePeername%"
```

for example, is converted into

```
"c:\Programme\test\test.exe" "Jones, Tom"
```

20.3.6 SWYXIT! WEB EXTENSION

SwyxIt! Web Extension offers the option of displaying a website within the SwyxIt! skin.

See also the SwyxIt! documentation.

It is possible to use special variables in the website address (URL) or HTML code in the websites. These variables are exchanged for their current value (content) during the website loading process. These variables can be used flexibly and effectively in web applications. It is possible, e.g. to resolve the number of an incoming call into an address by using an Internet phonebook service. Information, such as in this case the address, can then be displayed directly in the SwyxIt! skin.

Example - Variables in a URL

With the help of the following URL, it is possible to resolve the numbers of incoming calls using the Internet phonebook service "www.dastelefonbuch.de":

http://www.dastelefonbuch.de/?kw=%SelLinePeernumberPublicFormat%&cmd=search

In this example the variable "%SelLinePeernumberPublicFormat%" is used, which contains the caller number of the last (or the active) call in "non-canonical" format.

For further variables, please refer to *20.3.7 Use of System Variables*, Page 341.

SwyxIt! Web Extension supports Microsoft Edge WebView2

When you create or edit a SwyxIt! skin, you can configure the Web Extension to use Microsoft WebView2 instead of the old Internet Explorer control. WebView2 is a runtime environment that uses the Microsoft Edge Engine to integrate web content into applications. Existing skins and all VisualContacts and VisualGroups skins shipped with Swyx 14 will continue to use the legacy control. VisualContacts and VisualGroups are not yet compatible with Microsoft Edge WebView2.

20.3.7 USE OF SYSTEM VARIABLES

In SwyxIt!, program calls can be started at various points, e.g.

- Program call on shortcuts
- Program call using the context menu of a Speed Dial
- Composition of a web link as part of the SwyxIt! Web Extension

Windows system variables can be used, but also SwyxWare variables:

Variable	Content
%SelLinePeernumber%	Number of the conversation partner (both call directions)
%SelLinePeername%	Name of the conversation partner (both call directions)
%SelLinePeeraddress%	Name and number of the conversation partner (%SelLinePeername%, %SelLinePeernumber%), if both are available, otherwise just name or number
%SelLineCallednumber%	Internal number of the person being called blank for outgoing calls
%SelLineCalledname%	Name of the person being called blank for outgoing calls
%SelLineCalledaddress%	Name and number of the person being called (%SelLineCalledname%, %SelLineCallednumber%), if both are available, otherwise just name or number
%OwnName%	Own SwyxWare user name as displayed in SwyxIt!
%ActiveServerName%	SwyxServer Name as displayed in SwyxIt!
%SpeedDialPeernumber%*	Number configured on the Speed Dial
%SpeedDialLabel%*	Label configured on the Speed Dial
%SpeedDialUserbitmap%*	File name of the image configured on the speed Dial
%SpeedDialState%*	Signals the status of the user configured on the Speed Dial ● 0: Unknown ● 1: Logged off ● 2: Available ● 3: Currently talking ● 4: Call signaling/pickup possible

*. *Only usable in context menu of a Speed Dial* (20.3.5 Customer-specific context menu for Speed Dials, Page 340)

21 ENCRYPTION

Encryption of call data with SRTP

from SwyxWare on, SwyxWare supports the encryption of call data via "Secure Real Time Transport Protocol" (SRTP). The protocol, designed for real-time communication, means security for voice data transmission. The data is encrypted, making listening to calls impossible.

The following encryption modes are available:

- No encryption
- Encryption preferred
- Encryption mandatory

You can specify this setting individually per user, or globally for SwyxServer. It must be remembered that the selection of SwyxServer in the global settings has an influence on the configuration options in the user and trunk properties within the "Encryption" tab:

On selection within the server properties of...	...the following selection options are available within the trunk* and user properties:
No encryption	No encryption
Encryption preferred	No encryption
	Encryption preferred
	Encryption mandatory
Encryption mandatory	Encryption mandatory

Exceptions

SwyxLink-Trunk

In the SwyxLink trunk, the encryption mode is taken from the server settings and cannot be changed. Only one key must be assigned. See *The "Encryption" tab*, Page 307.

SIP Trunk

The setting of the encryption mode which was set within the server properties has no influence on the encryption mode within the SIP trunk. Voice data encryption on SIP trunks requires TLS as transport protocol and must be supported by the SIP provider. The corresponding configuration is defined in the properties of a SIP trunk group. See also *13.1.4 The "Encryption" tab of the SIP Trunk Group*, Page 233.

In a new installation of SwyxWare, the encryption mode is set by default to "Encryption preferred". When an older version is updated to Version 2011, the encryption mode is preconfigured to "No encryption".

See also *This is how you specify the encryption mode globally for SwyxServer*, Page 345.

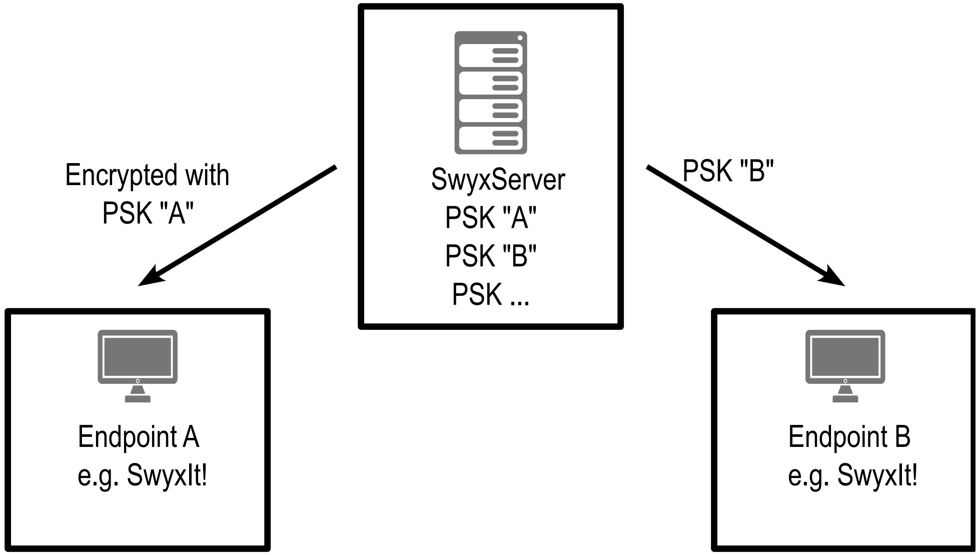
21.1 ENCRYPTION WITHIN SWYXWARE

For the actual media data transfer between two end points, the RTP (Real-Time-Transport Protocol) has previously been used. Within the encryption scenario, an end point can be a SwyxIt!, SwyxPhone, ConferenceMgr, LinkMgr, Gateway or a device from another manufacturer. With SRTP it is now possible to transfer media data encrypted and authenticated. SRTP is based on RTP and encrypts the data stream with the encryption algorithm AES (Advanced Encryption Standard).

To enable secure communication by SRTP, a common key (the so-called "PreSharedKey" (PSK)), must be defined between SwyxServer and the respective end point.

Assignment of the keys (PreSharedKeys) by SwyxServer

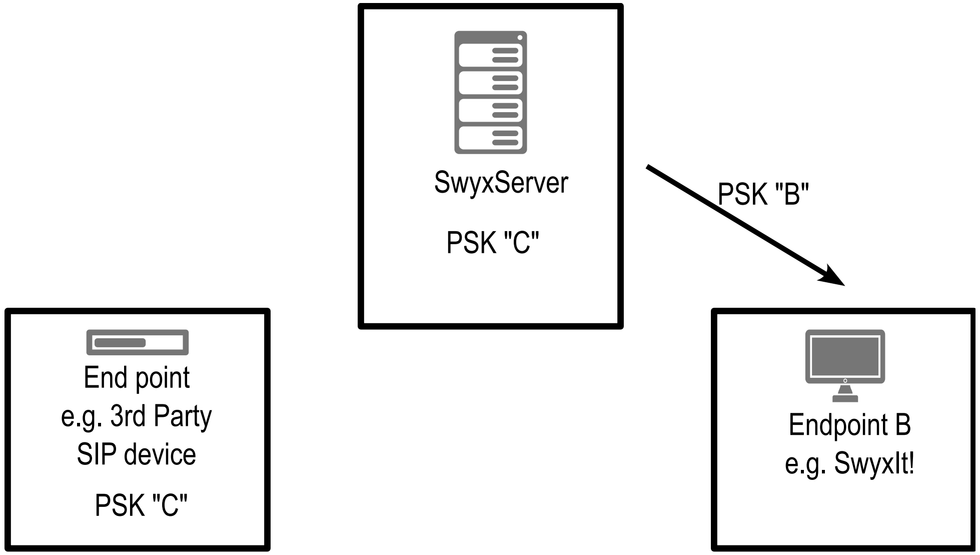
SwyxServer distributes a key (PSK) to each end point logging on. End point A is given PSK "A" and end point B PSK "B".



For all end points which use the SwyxWare database (e.g. , SwyxIt!, PhoneMgr, ConferenceMgr, LinkMgr, Gateway), SwyxServer automatically creates and distributes a PreSharedKey. On each successful logon of an end point, another key is generated and distributed encrypted to the end point.

Manual key assignment

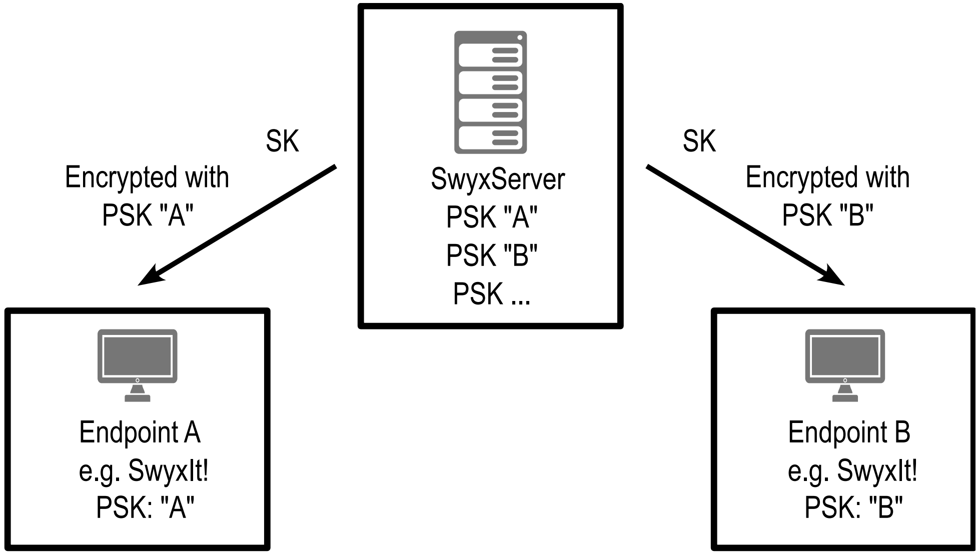
Exceptions to the automatic PSK distribution are devices from third party manufacturers. The key is not automatically assigned to these by SwyxServer. In such cases the key must be stored manually in the device (e.g. via a web interface). Furthermore, it must be configured in the properties of the user who uses this device. See also *11.2.1.9 The "Encryption" Tab*, Page 174.



The keys for a SwyxLink trunk and a SIP link must also be created manually. For a SwyxLink trunk this must be set correspondingly on both SwyxServer sides; for a SIP link, on the SwyxServer side and on the provider side.

The subsequent exchange of keys by MIKEY and the SRTP connection proceed in exactly the same way for the end points which are given a key manually as for the end points which receive a PSK automatically.

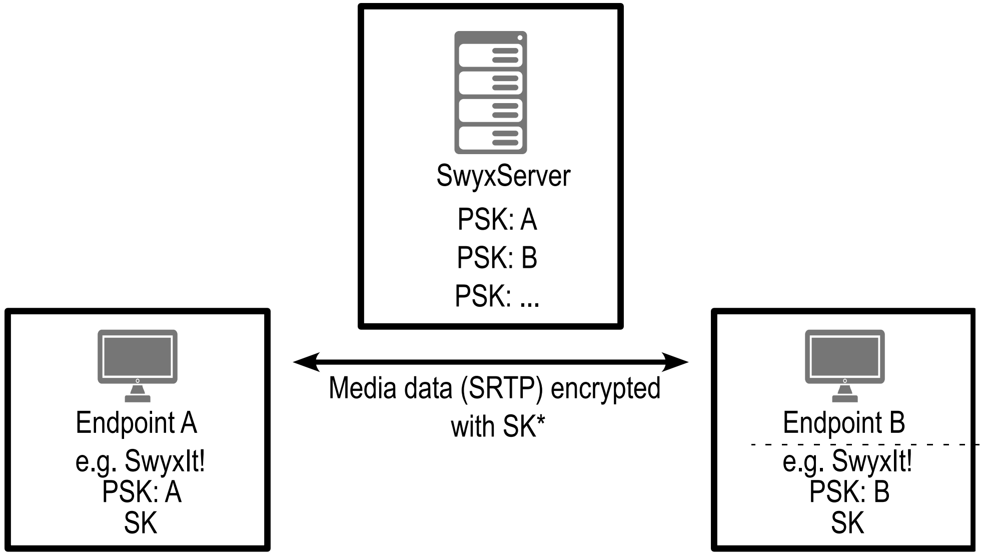
Exchange of keys by MIKEY



End point A...	SwyxServer...	End point B...
generates a session key SK (random key), encrypts this with PSK "A" and sends it to SwyxServer.	decodes SK with PSK "A" and encrypts SK once again with PSK "B". It then sends SK encrypted with PSK "B" to end point B.	decodes SK with PSK "B".

The end point from which the call is outgoing (here end point A) generates a session key (SK). The secure exchange of the session key is ensured by the protocol MIKEY (Multimedia Internet KEYing). This session key is used by SRTP to encrypt the data stream.

Connection by SRTP



The media data is encrypted with SRTP. This means that calls can no longer be listened to or recorded..

Encryption is dependent on settings of the end points

Whether a call is established, and whether it is correspondingly encrypted from end point to end point (e. g. from SwyxIt! to SwyxIt!), is ultimately dependent on the encryption settings within the user properties:

		If configured for end point A:		
		No enctyption	Encryption preferred	Encryption mandatory
If configured for end point B:	No enctyption	+ 🔓⚠	+ 🔓⚠	-
	Encryption preferred	+ 🔓⚠	+ 🔒✓ *	+ 🔒✓ *
	Encryption mandatory	-	+ 🔒✓ *	+ 🔒✓ *

- = Telefony is not possible	+ = Telefony is possible
🔒✓	data is encrypted
🔓⚠	data is not encrypted

** It is assumed that the endpoint supports encryption.*

21.2 CONFIGURE ENCRYPTION MODE GLOBALLY FOR SWYXSERVER

The encryption mode can be set globally for SwyxServers at user and trunk level.

This is how you specify the encryption mode globally for SwyxServer

1. Start the SwyxWare Administration and log in to the SwyxServer. Click the SwyxServer entry with the right mouse button to open the context menu.
2. Select "Properties".
3. Select the "Security" tab.
4. In the field "Encryption mode", choose from:

No encryption

The voice data is not encrypted. The selection of "No encryption" affects the configuration of the encryption within both the user and the trunk properties (*Exceptions*, Page 342). Here the mode is likewise set to "No encryption", and cannot be changed by the user. The field is deactivated within the user and trunk properties.

Encryption preferred

If "Encryption preferred" is selected, encryption only occurs if both call partners have configured either "Encryption preferred" or "Encryption mandatory". If this is not the case, the voice data is not encrypted, but phoning is still possible. With this encryption mode, the user is allowed to change the mode within his settings. The encryption mode can also be changed within the trunk properties.

Encryption mandatory

When "Encryption mandatory" is selected, voice data encryption is obligatory. This means that either encryption always occurs or the call is aborted with the reason "Incompatible encryption settings". This is the case, for example, when the other party has configured "No encryption". The selection of "Encryption mandatory" affects the configuration of the encryption within both the user and the trunk properties (*Exceptions*, Page 342). Here the mode is likewise set to "Encryption mandatory", and cannot be changed by the user. The field is deactivated within the user and trunk properties.

22 SCRIPTS

Swyx-Scripting for intelligent call routing; explanation of special scripts such as "standard voice box" or "automatic call center"

Some scripts, which complete the functions of SwyxWare, are installed during the installation. At this time, the following scripts are available:

- *22.2 Default call handling*, Page 348
- *22.3 Voice Box*, Page 348
- *22.4 Remote Inquiry*, Page 349
- *22.5 Operator (AutoAttendant)*, Page 352
- *22.6 Dial by Name*, Page 353

These scripts can be activated or altered by the administrator. For more information on script editing, see help.enreach.com/cpe/latest.version/CRM/Swyx/en-US/index.html#context/help/scripting_$.

22.1 CALL ROUTING MANAGER AND GRAPHICAL SCRIPT EDITOR

The Call Routing Manager is an intelligent module for handling incoming calls. The Call Routing Manager manages a list of rules which describe what should happen to an incoming call and under which circumstances this should take place. Each rule is made up of two basic components; the condition and the sequence of actions. When a call is received, the rule list is examined and a check is run for each rule to see whether the condition applies to the call. A sequence of actions is carried out as soon as a rule can be applied. Once a rule has been applied, all further rules in the list are ignored for this call.

Condition

A rule condition consists of the following components:

- The situation of the person called (e.g. "Logged off", "Speaking", "Available")
- Other conditions (e.g. time of the call, number of the caller, extension of the person called)
- Exceptions (e.g. except Mondays, except for a specific caller)

Sequence of Actions

A sequence of actions consists of a list of sub-actions which are carried out sequentially. Actions include, for example:

- Exit
- Connect To
- Connect Via DTMF
- Send email
- FollowMe
- Record Message
- Connect To Loop
- Play sound
- Voice Box
- Remote Inquiry

Each of these individual actions has parameters which can be assigned when they are added to the sequence of action. Sequences of actions can be defined and managed independent of the rule definition.

Graphical Script Editor provides a graphic presentation option, which allows you to create and edit complex sets of rules. See also help.enreach.com/cpe/latest.version/GSE/Swyx/en-US/index.html#context/help/GSE_$. The following text includes information necessary for administration.

The rules themselves, as well as the sub-conditions and actions available for the construction of rules, are defined and stored in the so-called Rule Book.

Each user also has a personal Rule Book with the rules he/she has defined in the SwyxServer user directory. The Call Routing Manager creates a script file called 'callrouting.vbs' which is based on the rules currently activated. This script is analyzed by SwyxServer when a call is received for the corresponding user. This script file can also be found in the user data directory of the user called.

The public Rule Book can be found in the server data directory in the sub-directory 'PhoneClient /Scripts'. This is used if no Rule Book exists for this user (*22.2 Default call handling*, Page 348).

Please remember that the use of the Call Routing Manager must be approved for the user (*11.2.8 The "Properties..." Dialog: The "Relationships" Tab*, Page 202). To use the rules created with the use of the Graphical Script Editor., the licenses for the option package 'SwyxECR' or 'SwyxProfessional' must have been added (*3 Licensing via license key*, Page 30).*2 Online Licensing*, Page 21

Signing Scripts

If you have purchased the "Extended call routing" option pack, you can create your own scripts using use of the Graphical Script Editor.. You can sign these scripts so that they can only be run on SwyxServers whose serial numbers are explicitly given in the script.

See also help.enreach.com/cpe/latest.version/GSE/Swyx/en-US/index.html#context/help/serial_number_restriction_$.

22.2 DEFAULT CALL HANDLING

If an incoming call can be associated with a user but not transferred, because no rule of the user’s Rule Book is applicable, the caller hears a busy signal. Internal callers also see the message "Subscriber not available" in the display.

If a user has no rules defined, and no Call Forwarding is set, it is attempted to connect the call to the original number for 60 seconds. If the destination does not answer the call, the caller hears a busy signal. Internal callers also see the message "Subscriber not available" in the display.

If a number cannot be assigned, i.e. neither to a user nor to a gateway connection (e.g. to a sub PBX), the call is rejected.

22.3 VOICE BOX

Every SwyxWareuser and every group has a personal answering machine (voice box). Voice messages can be called up in the call journal and can optionally also be sent to an e-mail address. For this purpose, an e-mail system that uses SMTP (Simple Mail Transfer Protocol) as the mail transport protocol is used. Incoming calls can be forwarded to Voice Box with the Call Forwarding function.

The Voice Box Process

- The caller hears an announcement recorded by a member of the group.
- The caller can then leave a message.
- If the caller does not end the call after recording a message, but stays on the line without saying anything or pressing '#' for 10 seconds, he will reach a tone selection menu:

Button	Explanation
1	Saving the recorded voice message
2	Listening to the recorded voice message
3	Re-starts the recording of the voice message
#	Ends the recording and starts the menu announcement

- The caller's message is recorded as an OPUS file and optionally sent to the SwyxWareuser or group by e-mail.

  The calling party number, the calling party name, if available, and the length of the voice message are written in the subject of the Email. The name of the attachment is composed in the following way:

  Voicemail-<date using the format yymmdd-hhmmss>-<Calling party number>-<Calling party name>

  Each user and each group can individually set the e-mail address to which the voice messages are sent. The e-mail contains the date, time, number, and name of the caller (if available) in text form. The recorded message is included as a file attachment.

  The files sent contain the voice message in a compressed form. The compression to be used for this can be indicated as the server standard or it can be individually set for the user.

  See also *11.2.1.8 The "Advanced" Tab*, Page 173.

Voice Box announcement

If a user starts SwyxIt! for the first time and if the user has been assigned the standard configuration (CompanyWelcome.wav (template)), he will be prompted to record an announcement. Both announcements, e.g. the name announcement (name.wav) and the Voice Box announcement ("My welcome message.wav") will be saved in the database. If none of the announcement files ("default welcome.wav", "default welcome without recording.wav", "default welcome_with_menu.wav") is available, the user will be prompted to record the announcement again, regardless of whether he uses this announcement. If the announcement file "name.wav" is missing, the Recording Wizard will prompt again.

It is also possible for every user to record an individual announcement with SwyxIt! at a later point.

If SwyxIt! is started in a terminal session or as a CTI-SwyxIt!, the user will not be prompted to record his announcement. The same is true if the administrator has configured a company-specific announcement when creating the user.

The user can also listen to and edit these voice messages from another telephone connection. See also *11.8.1 Remote Inquiry*, Page 213.

If the user or group has not defined any rules or detour, the standard call handling is activated. See also *22.2 Default call handling*, Page 348.

22.4 REMOTE INQUIRY

Remote Inquiry allows the user to listen to his voice messages and to change Call Forwarding Unconditional from any telephone line. When a user is called at the or her own SwyxWare number, he or she identifies him/herself to SwyxWare with a Remote access PIN; only then can he or she listen to, repeat, or delete new voice messages and afterwards all existing voice messages.

When configuring the Voice Box, you must specify that you can access the remote query by pressing the * button. After entry and verification of the PIN, the caller has several options to choose from. These can be selected from the menus.

To change the Call Forwarding, follow the instructions in the Remote Inquiry menu. SwyxIt! Users can configure the remote inquiry within the Call Forwarding themselves. The administrator must set up this remote inquiry functionality for the SwyxPhone users. See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/remote_inquiry_$.

This is how you set up Remote Inquiry for a user

1 Open the user properties and select the "Call Forwardings" dialog.

2 Set the default voice box and activate the option "Start remote inquiry using the * key"
See also *11.2.5.4 Standard Voice Box" tab*, Page 183.
The announcement of the Standard Voice Box provides the option of going to the Remote Inquiry menu using the * key.

3 Then set the PIN for remote access, see *11.2.5.5 Tab "Standard Remote Inquiry"*, Page 184.

4 Make certain that it is possible to reach the Remote Inquiry menu with a phone call.

Call Forwarding Configuration for Remote Inquiry

To listen to voice messages remotely, the call forwarding must be set up so that you can access the remote access menu by making a call:

- If no other call routing rules have been activated yet, set up "Delayed call forwarding" so that a call is forwarded to the standard voice box. To ensure access to Remote Inquiry even after changes to Call Forwarding Unconditional, open the Call Routing Manager and prioritize the Call Forwarding rule "Call Forwarding No Reply" by putting this rule at the beginning. During the welcome announcement the caller can use the *- key to reach the Remote Inquiry menu.
- If call routing rules are enabled, please make sure to include the remote inquiry option. See also help.enreach.com/cpe/latest.version/CRM/Swyx/en-US/#context/help/remote_inquiry_$.
- If no call routing rules are enabled, and the **immediate** call forwarding is changed, (e.g. from the Standard Voice Box to another number), the caller can no longer perform a remote inquiry, i.e. he/she can no longer change or disable the immediate call forwarding remotely. To avoid this, create a call routing rule and place it before the immediate call forwarding in the list of rules. Such a rule could be, for example, always forward calls to Voice Box that are made from your mobile phone. In this manner, you will always be forwarded to your Voice Box and thus to Remote Inquiry when you call from your mobile phone.

If you configure a Remote Inquiry within a Call Forwarding or system rule, you will always be asked for your user PIN. There is no checkbox for this. If a user is calling from his own extension number, for which this Call Forwarding was configured, he will not be asked for his PIN.

Overview of the Remote Inquiry Menus

If a user calls the remote inquiry function, they will hear the main menu announcement after the announcement of how many new voice messages they have received. Here you can listen to the old voice messages or undertake further configurations.

Main Menu

Button	Explanation
0	End Remote Inquiry (=Hook on)
1	Querying voice messages
4	Change the Call Forwarding Unconditional
7	Delete all voice messages Deletions must be confirmed with the # key.
#	Help

During the output of a voice message, the following options are available:

Button	Explanation
1	Back to the beginning of the voice message
3	Forward to the end of the voice message
4	10 seconds backward
5	Stops or starts the output of the voice message
6	10 seconds forward
7	Switch to the previous voice message
8	Switch to the next voice message
9	to the main menu
*	Switches to the next information of the voice message (date, time, number, content)
#	Help

After each voice message has been played, you have the choice of the following options:

But-ton	Explanation
0	Create connection to caller (if the number is known)
1	Repeat the message played
3	Delete the played voice message. The deleting procedure must be confirmed with the * key.
9	to the main menu

Configuration Menu for Call Forwarding Unconditional

But-ton	Explanation
0	Activate the Call Forwarding Unconditional to the number from which you are currently calling You will only be provided with this option if SwyxWare has recognized the number.
1	Activate the Call Forwarding Unconditional to a destination number. The Call Forwarding Unconditional to the saved destination number will be activated. If no destination number is saved, you will be prompted to enter a number.
2	Activate the Call Forwarding Unconditional to Voice Box The Call Forwarding to your Standard Voice Box will be activated.
3	Deactivate Call Forwarding Unconditional Call Forwarding Unconditional is switched off. Please note that in this case other rules of the Call Routing Manager can be applied.
4	Save a new destination number for Call Forwarding Unconditional Here you can enter a new destination number and end with '#'. Call Forwarding Unconditional to this number is then activated.
5	Display the current status of Call Forwarding The current status of Call Forwarding Unconditional will be given.
6	Record a new announcement for the Standard Voice Box The current announcement will be played. You can change this (1). The recording can then 1: be saved 2: be listened to 3: be re-recorded. 9. Back to the Main menu If the new announcement is not saved, the previous announcement will continue to be used.
9	End remote configuration The remote configuration of Call Forwarding Unconditional is ended and you return to the main menu.
#	Help

Name Announcement

In order to play both the number and the name of the caller for other internal subscribers, the first time SwyxIt! is started with the help of the announcement wizard, a file called 'name.wav' is recorded and saved in the database. Before the voice message is played, the internal caller is identified based on the number, and the file 'name.wav' will be played from his personal files. Alternatively, the administrator can create a WAV file for every user in the database, which contains the spoken name of the user and which has this name as a file name.

Example:

For the user "John Smith", a file labeled "John Smith.wav" is saved in this directory and this file contains the spoken name "John Smith". If Otto Müller has left a voice message for another user Meier, Mr. Meier is not only announced the number when the voice message is requested, but "Otto Müller.wav" is played.

The name announcement also functions for incoming external calls if the number is signaled for such a call and if a corresponding entry has been made in the global or personal phonebook.

Example:

> *A caller from 00123456789 leaves a voice message for user Baker. In the global phonebook, there is an entry for the number 00123456789 under the name "Sample Company (Ms. Schmidt)". If you then save a WAV file with the name "Sample Company (Ms. Schmidt).wav" in the aforementioned directory, this will be played when Mr. Baker listens to his voice message by Remote Inquiry.*

See also https ://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/recording_wizard_$.

22.5 OPERATOR (AUTOATTENDANT)

There is the option of directly configuring users and groups which are required within the company structure, during the SwyxWare installation.

The script "Operator" serves as the automatic forwarding option: You may e.g. receive any general calls to your company via an operator desk. Similar to all other users, an internal and an external number may be assigned to the operator desk.

Script Process

First the announcement is played:

> "Please enter the extension number or the 7 for Sales, the 8 for Support, the 9 for automatic dial by name or stay on the line to be connected to an operator." The groups Sales and Support were chosen as an example. You can change these at any time (*22.5.3 Change Operator Script*, Page 353).

Afterwards the caller can make a selection per DTMF entry.

- If no entry is made, the caller will be connected to an operator after 5 seconds.
- If the caller enters an internal or external number directly, he will be put through to this number. This is also true for extension numbers that begin with 7, 8 and 9 as long as the caller enters the first two numbers of the extension number within 2 seconds.

STOP To prevent misuse (e.g. unauthorized dialing in to the telephone system followed by transfer to chargeable service numbers), the default setting only permits an operator to dial internal calls. If transfer to external numbers is nevertheless required, be sure to protect the script e.g. with the help of a PIN.

22.5.1 INSTALLATION OF THE AUTOATTENDANT

During the SwyxWare installation you can indicate whether the AutoAttendant should be installed.

The installation includes the following steps:

- A SwyxWare user is generated with the name "Operator".
- Two groups are created as examples, "Support" and "Sales".
- The Call Routing script for the operator desk is then installed.
  This call routing script is installed in the SwyxWare directory under \data\defaults\operator. This can be changed later (*22.5.3 Change Operator Script*, Page 353).

If the operator is not installed during the main installation, you can also create this and the groups "Support" and "Sales" at a later time. The assignment to the script takes place via the name of the user or group.

In order to log in as Operator using SwyxIt!, you must assign a Windows user account or a password to Operator. To do this, open the administration for the user "Operator" in the SwyxWare Administration.

See also *11.2.1.2 The "Authentication" Tab*, Page 165.

The first time you log in as Operator using SwyxIt!, the Recording Wizard will start and assist you in recording the necessary announcements. You can start this wizard once again at any time from the menu bar of SwyxIt! (under Settings | Recording Wizard...).

22.5.2 OPERATOR AND SWYXWARE UPDATE

The update of SwyxWare will be performed in a way that your existing configuration remains unchanged.

The following situations can occur during the update:

The user "Operator" already exists

If there is already a user with the name "Operator", this will not be changed and the Call Routing remains the same. The "Operator" function provided by the "Operator" script will then not work.

The groups "Sales" and "Support" already exist

In this case these will be used by the Call Routing of the user "Operator".

The names "Sales", "Operator" or "Support" already exist

If other objects (users, SwyxLinks, Phonebook entries, etc) with the names "Sales" or "Support" already exist, these groups will not be created and the operator will not function.

Before beginning the update, make certain that there are no user names, gateway names, link names or global Phonebook entries with the names "Operator", "Support" or "Sales".

You can also create the groups "Sales" and "Support" later using the SwyxWare Administration.

22.5.3 CHANGE OPERATOR SCRIPT

If the "Extended call routing" or "SwyxProfessional" option pack has been installed, you can edit the operator script.

This is how you change the settings in the operator script

1. To do this, open the Call Routing Manager for the user "Operator" in SwyxIt! or in the SwyxWare Administration.
2. Select the rule "Auto Attendant".
3. Click on the link "Auto Attendant Action" in the description field. The dialog "Sequence of Actions" opens.
4. Click with the right mouse button on the action "Operator" in the list on the left and select "Edit Editor Action" in the context menu. Graphical Script Editor will start.
5. There you can change the action according to your needs.

For more information, see help.enreach.com/cpe/latest.version/GSE/Swyx/en-US/index.html#context/help/scripts_$.

22.6 DIAL BY NAME

This action e.g. is part of the operator script. This gives the caller the option of being put through to a user, assuming he knows the user's name. It uses the files 'name.wav' in the user files.

Script Process

An announcement is played first:

> *"Hello! You have reached the automatic dial by name. Please type the name of the desired subscriber on the telephone keyboard." Here the letters A, B and C correspond to the 2 button, the letters D, E and F correspond to the 3 button, etc.*

This announcement will be cancelled upon entry of a DTMF tone. The list of user names is searched after each entry:

- If more than three users with the entered letters are found, an additional letter entry will be prompted.
- If two or three users are identified, the caller can select from these per DTMF.
- If only one entry is found, the caller will be directly connected to this user.
- If no entry is found, the dial by name function will be discontinued.
- The caller can cancel the name search at any time with ‘#’ and return to the dial by name menu.

22.7 THE GROUP "EVERYONE"

SwyxWare creates a group with the name "Everyone" during installation and adds all users (except for the user "Conference") to this group. Each new user created using the SwyxWare Administration will also be added to this group. This allows status signaling to be set up between all members of this group (*11.2.8 The "Properties..." Dialog: The "Relationships" Tab*, Page 202).

Updating

If a group called "Everyone" already exists at the time of an update, this group will remain unchanged. All new users created using the SwyxWare Administration will also be added to this group.

22.8 STANDARD SCRIPTS IN THE DATABASE

The call routing scripts for the call handling are stored in the database. You can display them in the server properties under Files (*7.5.10 The "Files" Tab*, Page 97).

After an installation, the following script files can be found in the database:

System standard files

These files are standard in every system. When a user is created, the examples could e.g. be made accessible to the user. As soon as a user opens and alters such a rule (e.g. saves it again with his parameters), the changed script is transferred to the user's rule set (user_book.srb).

Name	Explanation
System_V4.3.srb	Settings for Rule assistants in the Call Routing Manager
System_Resource_V4.3.srb	Texts for the script examples: ● Employee absent, ● Employee vacation, ● Secretariat - no business hours Texts for describing the system functions
User_Default_V4.3.srb	Default rule set for new users This is adopted when a new user is created.
Templates_V4.3.vbs	contains the functions for use of the Graphical Script Editor.
Functions.vbs	contains the system functions used by Graphical Script Editor.

User files

These files are user-specific. As soon as the user draws up his own call routing rules, or sets his call forwarding, a new 'set of rules' is saved for this user (user_book.srb).

Name	Explanation
user_book.srb	Contains the rule set for the user. This consists of all activated and deactivated rules (*.rse) and actions (*.ase) which are displayed to this user in Call Routing Manager.
callrouting.vbs	will be executed by SwyxServer and contains the executable script which will be generated from the rule set (user_book.srb) when Call Routing Manager is closed. This script contains all rules and actions generated with the Call Routing Manager. The rules created with use of the Graphical Script Editor. are stored in the file 'ruleXXX.rse', the corresponding executable script in 'ruleXXXe.vbs'. If actions have been created with use of the Graphical Script Editor., the files 'actionXXX.ase' and 'actionXXX.vbs' have been created. All these VBS files are included when call routing is executed.
crmhst.dat	Contains the last selected parameters which are then available in the drop-down lists of Call Routing Manager.

22.9 PIN QUERY FOR CONFERENCE ROOM (GSE) (KB2377)

In SwyxWare v4.10 and higher, there is the "Conference" function, with the so-called virtual conference rooms. This article describes how you can restrict access to a conference room with a PIN query.

0PIN query for conference room (GSE) (kb2377) enreach.com/products/support/knowledge-database/article-details/swyxknowledge/kb2377.html

22.10 FUNCTION CODES

Within SwyxWare, certain functions can also be started by entering a function code. The character string is interpreted and executed as a command by SwyxServer.

A differentiation is made between

- Template Script Code
  These character strings are detected and interpreted by the user's script template.
  Note that these codes can only be used within SwyxWare, and not externally.
- CTI+ Code
  These DTMF strings are being used in connection with CTI+ (control of Third Party devices and control of phones via your phone number). Certain SwyxWare functions can be executed via DTMF function codes, independently of SwyxIt!, directly at the connected devices.
- Call Intrusion
  These function codes are only used in the context of intrusion on external calls (SwyxMonitor option pack required). They are only possible in block dialing, i.e. before the handset is lifted (e.g. with an abbreviated dialing button).
- Feature Codes
  These character strings relate to remote inquiries of external voice-messages. They are only possible in block dialing, i.e. before the handset is lifted (e.g. with an abbreviated dialing button).

The following function codes are available:

Template Script Code (internal only)

Code	Function	Description
##	-	Initial sequence, which routes a call directly to the user. Additional characters are processed by the user's script (template.vbs).
##10	Remote Inquiry	The remote inquiry for the user is activated; the PIN is not queried since the user himself is calling (from his own device)! Sub-menus of the remote inquiry can be reached directly by suffix.
##20nnn#	Call Forwarding Unconditional to nnn	● Enable Call Forwarding Unconditional to nnn* . ● If a * is entered instead of nnn, immediate forwarding to the Voice Box is activated. ● Without nnn, Call Forwarding Unconditional is deactivated.
##21nnn#	Call Forwarding Busy to nnn	● Enable Call Forwarding Busy to nnn*. ● If a * is entered instead of nnn, call forwarding to the Voice Box is activated when busy. ● Without nnn, Call Forwarding Busy is deactivated.
##22nnn#	Call Forwarding No Reply to nnn	● Enable Call Forwarding No Reply to nnn*. ● If a * is entered instead of nnn, delayed forwarding to the Voice Box is activated. ● Without nnn, Call Forwarding No Reply is deactivated.
##23	Deactivate Call Forwarding Unconditional	Deactivate Call Forwarding Unconditional
##24	Deactivate Call Forwarding Busy	Deactivate Call Forwarding Busy

Code	Function	Description
##25	Deactivate Call Forwarding No Reply	Deactivate Call Forwarding No Reply
##70*	Call All Devices	Regardless of the redirection rules, all logged-on terminal devices of the calling user will ring.
##71*	Connecting to the Voice Box	Regardless of all forwarding settings, the calling user is connected to their own Voice Box. He can then leave himself a voice message.
##8nnn*ppp #	Call Forwarding Unconditional from nnn	For the user with the number nnn, Call Forwarding Unconditional to the calling line is activated. The given PIN ppp is checked.
##9nnn#	Remote Inquiry from nnn	The remote inquiry of the user with the number nnn is called. The PIN is queried in the Remote Inquiry menu.

*. <nnn> stands for extension or external number with public line access or in format **44231123456

<ppp> stands for the PIN

CTI+

Code	Function	Description
*0	Disable DTMF recognition	The DTMF recognition is disabled. This can be necessary in order to send DTMF signals to the call partner. Please use the sequence ## for # here.
#0	Enable DTMF recognition	The DTMF recognition is enabled.
##	Send single #	Sends a # as a DTMF code to the caller (transparent), when the DTMF recognition is disabled.
*3	Starting a conference	A conference is started with active callers and those put on hold.
*7	Hold/Call Swap/Activate	The active call is put on hold. A switch is made to a free line or to another line on hold. If a call has already been put on hold, it can be re-activated by pressing *7.
*8	Exit	The currently active call is terminated.
*9	Call Transfer	The active call is connected to the call on hold.
*9nnn#	Blind Call Transfer	The active call will be connected to nnn without inquiry. Requirement: You have only one call. If the connection with the destination subscriber cannot be established within 20 seconds, the originally received call will be displayed in your SwyxIt! as a call on hold. By pressing *7, the call on hold can be re-activated.
*0	Disable DTMF recognition	The DTMF recognition is disabled. This can be necessary in order to send DTMF signals to the call partner. Please use the sequence ## for # here.
#0	Enable DTMF recognition	The DTMF recognition is enabled.

In order to use DTMF in connection with SwyxCTI+, the SIP termial devices must support DTMF via SIP-INFO.

The following applies for using DTMF in connection with : SwyxCTI+ If there is an active call on hold and a second call needs to be aborted before being connected, then the DTMF code cannot be used. In this case, hang up on the controlled device. You'll now receive a call back for the line still on hold, and a second call can be initialized again by entering *7.

Call Intrusion (only possible as block dialing)

Code	Function	Description
nnn*24*1#	Call Intrusion (listening only)	A call that the agent is making with the number nnn is intruded in 'listening only' mode.
nnn*24*2#	Call Intrusion (speak with agent)	A call that the agent is making with the number nnn is intruded on; the agent can hear the intruder.
nnn*24*3#	Call Intrusion (Conference)	The call that the agent is making with the number nnn becomes a conference.

Feature Code (only possible as block dialing)

Code	Function	Description
nnn[*] 71*	Voice Box	Calls the Voice Box of user nnn, regardless of the selected call forwarding. You can leave a voice message directly.
nnn*72*	Direct Call	Calls the user nnn as a direct call (Intercom), i.e. a device of the called person is switched at once to output.
nnn*ppp*8*	Call Forwarding Unconditional from nnn	For the user with the number nnn, Call Forwarding Unconditional to the calling line is activated. The given PIN ppp is checked.
nnn*9*	Remote Inquiry from nnn	The remote inquiry of the user with the number nnn is called. The PIN is queried in the Remote Inquiry menu.

[*] *<nnn> stands for extension or external number with public line access or in format **44231123456*

<ppp> stands for the PIN

23 STANDBY SWYXSERVER

As of SwyxWare 13, the standby functionality is not available.
Enreach will be happy to assist you in selecting a suitable high-availability solution, see *App. L: High Availability Solution for SwyxWare*, Page 457

23.1 CONVERT MASTER OR STANDBY SYSTEM TO A STAND-ALONE SYSTEM

An existing standby installation with a master system and a standby system can be converted into an installation with only one SwyxServer.

Please convert only the master system into a stand-alone SwyxServer, since the hardware dependency means that new permanent licenses have to be requested for the conversion of a standby system.

This is how you convert an existing standby installation

1. Deactivate the database replication.
   You need to have administrator rights on the host system to do this.
2. Master System
   On the system with the master SwyxServer, open an input prompt under "Start | Run... | cmd", and execute:
   ```
   osql -E -Q "EXEC sp_replicationdboption 'ippbx', 'merge
   publish', false"
   ```
   If you use a named SQL Server instance, then please use
   ```
   osql -S <master-host>\<master-instance-name> -E -Q
   "EXEC sp_replicationdboption 'ippbx', 'merge publish',
   false"
   ```
   where
   - master-host = host name (NETBIOS name) of the master SwyxServer
   - master-instance-name> - name of the SQL Server instance on the master SwyxServer
3. Standby System
   Open an input prompt on the standby system and execute:
   ```
   osql -E -d ippbx -Q "EXEC sp_mergesubscription_cleanup
   '<master-host>', 'ippbx', 'ippbx_merge_publ'"
   ```
   If you use a named SQL Server instance, then please use
   ```
   osql -S <standby-host>\<standby-instance-name> -E -d
   ippbx -Q "EXEC sp_mergesubscription_cleanup '<master-
   host>\<master-instance-name>', 'ippbx',
   'ippbx_merge_publ'"
   ```
   where
   - <master-host> - host name (NETBIOS name) of the master SwyxServer
   - <master-instance-name> - name of the SQL Server instance on the master SwyxServer
   - <standby-host> - host name (NETBIOS name) of the standby SwyxServer
   - standby-instance-name = name of the SQL Server instance on the standby SwyxServer.
4. Delete the content of the registry keys "StandbyType" and "StandbyServer" in the path "HKEY_LOCAL_MACHINE\SOFTWARE\Swyx\IpPbxSrv\CurrentVersion\Options"
5. Start the configuration wizard on the former master system that you now want to configure as the standard SwyxServer. For the selection of the server type, choose the option "Standard SwyxServer".

24 SWYXFAX SERVER

Option Pack SwyxFax to send and receive faxes from every workstation.

This makes it possible to use the central fax service from any Windows computer in a Windows network, in which SwyxWare is installed. Each user can be assigned his or her own fax number. Once the SwyxFax Client has been installed on the computer, the user can send, receive, forward and manage documents both internally and externally by fax.

It is also possible to send the fax documents you have received to another user per email (Faxmail).

SwyxFax Server is a component of SwyxServer. It can be installed on the same computer together with SwyxServer, or as a separate service within the network. After the installation, a connection to SwyxServer will be established to exchange the user parameters, to verify the existing licenses, and to send or receive faxes. SwyxFax uses the same connection as SwyxServer to public network. If SwyxFax is installed, the number of licensed SwyxFax users can use this fax service.

Incoming faxdocuments are received by SwyxFax Server and assigned to the corresponding user. If a fax is received on a number, which has not been assigned to any user, this document will be forwarded to a central distributer, e.g. the system administrator. Each user has a personal fax inbox, in which the received documents are shown.

Furthermore, it is possible to create a personal telephone book for each user. Frequently used fax numbers and recipients can be saved here. Alternatively, you can also use Outlook Contacts or the fax addresses can be taken directly from a file.

The Advantages of Using SwyxFax Server with SwyxServer

SwyxFax Server is integrated in SwyxServer from Version 7.0. This provides you with all of the advantages of SwyxWare for SwyxFax users as well:

- Installation of the SwyxFax Server together with the SwyxServer installation
- Configuration of SwyxFax Server within the SwyxWare Administration
- Observation of fax dispatch in the SwyxWare Administration
- Call detail records, even for fax connections
- Call Routing, even for fax connections (e.g. forwarding)
- Internal telephone number substitution and therefore the use of routing records (Least Cost Routing)
- Fax connections via SwyxLink
- Connections to and from fax devices via VoIP adapters without the use of the public telephone network (e.g. via SwyxLink or SIP provider)

24.1 SYSTEM REQUIREMENTS

SwyxFax is a component of SwyxServer. You will find the current matching client version (SwyxIt!) on the SwyxWare DVD.

> Please always install the appropriate matching (identical) server and client versions.

System requirements for SwyxServer and other components, see *4 System Requirements*, Page 40.

SwyxFax Client

SwyxFax Client is a component of the telephony client SwyxIt!. The computer must accordingly satisfy the same requirements as for SwyxIt!. See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/requirements_$.

24.2 THE BASICS

SwyxFax is a component of SwyxWare and expands the PBX with the option of a central fax service. SwyxFax represents a client/server solution and it includes the following components:

- SwyxFax Server as central fax server. It receives the fax documents and forwards them accordingly. SwyxFax Server is started as a service, just like SwyxFax Printer Gateway is started for central print.

> Please note that within a SwyxWare installation only one SwyxFax Server may be present .

- SwyxFax Client for the individual users together with the corresponding printer driver.

SwyxFax Server

The SwyxFax Server is installed as a component of SwyxServer together on one computer, or as a separated service. All SwyxFax parameters are configured in the SwyxWare Administration.

SwyxFax Server is implemented as a service and is automatically started when Windows is started. The service is permanently available on the machine, even if no user is logged on to SwyxFax Server.

The SwyxFax Server is only contacted by the SwyxFax Client. In doing so, the SwyxFax Client can run on the same computer as the server or on any other Windows computer in the network. This makes transparent network operation possible using a central SwyxFax Server and any number of distributed SwyxFax Clients.

All faxes sent and received are managed by SwyxFax Server. SwyxFax Client calls the user-specific data from SwyxFax Server, whereby the data continue to be stored on the server. Therefore, it is only possible to operate SwyxFax Client if the SwyxFax Server is available in the network.

SwyxFax Server automatically provides its services throughout the entire network in LAN environments. No other special supplementary software is required.

SwyxFax Client

SwyxFax Client is the corresponding client software for SwyxFax Server. SwyxFax Client is installed as a component of the telephony client SwyxIt!.

The SwyxFax Client logs on to the SwyxServer. The authentication uses the Windows user account or user name and password.

A printer driver is included in SwyxFax Client. This driver enables you to easily send faxes from other applications.

Fax Transmission

SwyxFax uses different ways to transmit fax documents, e.g. via a SwyxLink to other branch offices or to a terminal adapter within the network.

The ISDN cards and licensed voice channels, which are used by SwyxServer, are also used by SwyxFax Server during a transmission.

Some service providers also offer fax transmission over SIP according to the T.38 standard. You can find details about this in the Knowledgebase under

SIP provider
enreach.com/products/sip-provider.html

Forward Inbound Faxes

Received fax documents are always in a page-oriented DCX format (multi-page PCX format).

The associations between fax numbers and local recipients (SwyxFax Client), users' email addresses (Faxmail) or printers are defined in the forwarding table. The forwardings are specified in the properties of the individual user. See *11.2.2.3 The "SwyxFax Numbers" Tab*, Page 179.

When a fax is received for a specific fax number, the table is used to assign the fax to a recipient. The user will then see the received document either in the fax inbox of his SwyxFax Client or he will receive a

Faxmail or will receive the document as a printout from a defined printer.

Please note that document printing is only available within a domain environment.

Faxmail

The fax documents you receive can also be delivered as a file per email. This requires that a corresponding SMTP mailserver is permitted for forwarding emails of the SwyxFax Server. SwyxFax Server takes the relevant parameters from the SwyxServer.

Fax stack

From SwyxWare Version 12.40 onwards, the existing fax stack will be replaced by a new stack by default in order to offer a future-proof Swyx Fax solution. The SpanDSP library from www.soft-switch.org is then used.

However, if you want to continue using the old fax stack, you can set this via the Windows registry. To do this, you must create the corresponding keys under "HKEY_LOCAL_MACHINE\SOFTWARE\Swyx\IpPbxFaxSrv\CurrentVersion\Options" and set them to true.

Key (Reg_DWORD value 32-bit) (set if value ≠0)	Description	Default value
DisableSpanDspG711Rx	SpanDSP is not used for receiving faxes via G.711 protocol	false
DisableSpanDspG711Tx	SpanDSP is not used for receiving faxes via G.711 protocol	false
DisableSpanDspT38Rx	SpanDSP is not used for receiving faxes via T.38 protocol	false
DisableSpanDspT38Tx	SpanDSP is not used for receiving faxes via T.38 protocol	false
DisableSpanDsp	Master key: If this key is set to true, it overwrites internally all keys mentioned here with true, so that SpanDSP is no longer used	false

24.3 LICENSES

SwyxFax is an optional component for SwyxWare. The licensing of SwyxFax takes place centrally on the SwyxServer with the help of SwyxWare Administration. In doing so, the following are licensed:

- the number of SwyxFax users to whom fax documents are delivered and
- The number of fax channels, i.e. the number of documents to be sent or received simultaneously.

If you would like to add further fax channels or SwyxFax users to your original SwyxFax installation, you will need a new license key. This license key is added in the SwyxWare Administration (*For information on Online Licensing, see 2 Online Licensing, Page 21.*, Page 361).

If more SwyxFax users are configured than there are licenses for SwyxFax users, then the SwyxFax Server no longer starts. The message will be added to the eventlog "SwyxFax Server failed to start within 3 minutes. It keeps trying to start. Last error message was: License check failed (FaxChannel Licenses X/Y; FaxUser Licenses: X/Z)".
In such a case, remove the extra user fax numbers.

For information on Online Licensing, see *2 Online Licensing*, Page 21.

.

24.4 INSTALL SWYXFAX SERVER

SwyxFax Server is installed / uninstalled as a component of SwyxServer. See *5.4.1 SwyxWare - Run Setup*, Page 53.

The SwyxServer Configuration Wizards undertakes an initial configuration of the necessary parameters for SwyxFax Server. See *5.4.2 Configuring SwyxWare*, Page 54.

Please note that local administrator privileges are required for the installation. If SwyxFax Server is installed as SwyxServer on some other computer, the installation and configuration must be carried out under a user account which is a member of the group "SwyxWare administrators" on the SwyxServer computer.

24.5 CONFIGURING SWYXFAX SERVER

If SwyxFax Server is installed, you can use SwyxWare Administration to change the SwyxFax settings, to display a list of the fax documents on the server and to observe the state of the fax channels.

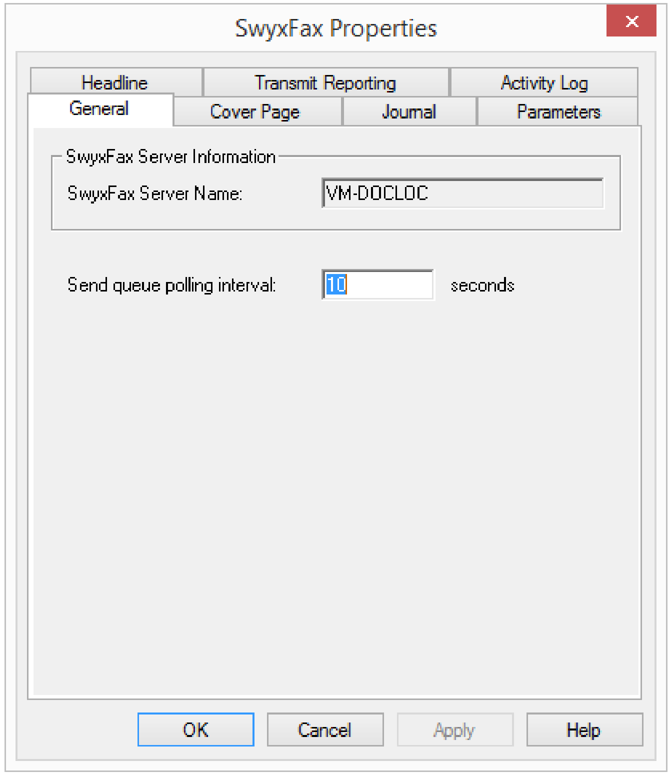
This is how you start the configuration of SwyxFax

1. Open the SwyxWare Administration and establish the connection to the SwyxServer.
   See *7.1 Registration on SwyxWare Administration*, Page 80.
2. Click the SwyxFax entry with the right mouse button to open the context menu.
3. Select "Properties".
   You can now configure the settings for SwyxFax as described below.

By clicking on "OK", any changes made will be implemented after closing the settings. There is no need to halt or restart the SwyxFax Server service.

In order nonetheless to restart SwyxFax or other services after a configuration, you can prevent new calls and logins. Existing connections can be completed without disturbance. See *How to prevent new logins and new calls*, Page 86. You can then halt the service in the administration of the services (e.g. likewise in the MMC application).

24.5.1 THE "GENERAL" TAB



SwyxFax Server Information

SwyxFax Server Name: VM-DOCLOC

Send queue polling interval: 10 seconds

General settings for SwyxFax are made on this tab.

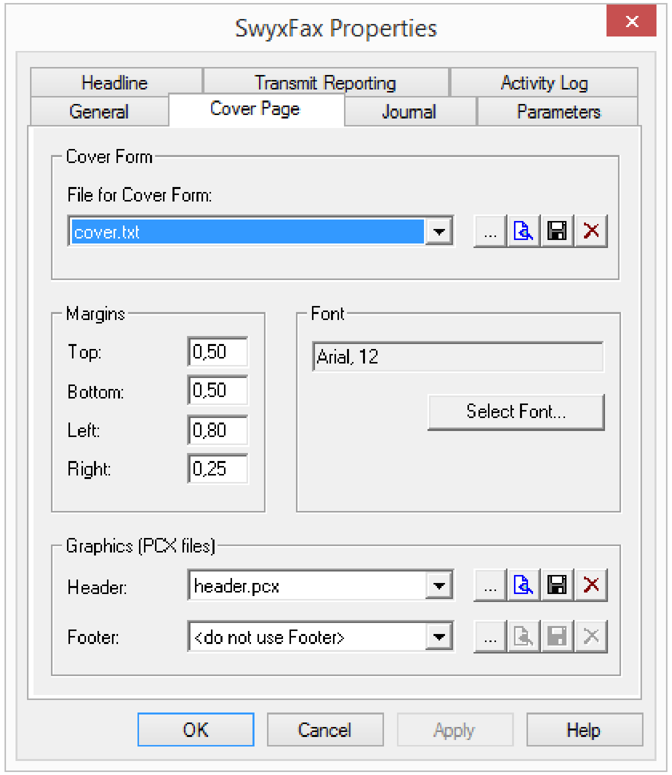
SwyxFax Server information

The name of the computer running the "SwyxFax Server" service is entered here. The name is only displayed if SwyxFax Server is active.

Send Queue Polling Interval

Here you define the time range after which the SwyxFax Server updates the queue of fax documents. Thus, if a SwyxFax Client sends a fax document, it will be added to the queue and processed by SwyxFax Server after the next refresh interval at the very latest.

24.5.2 TAB "COVER PAGE"



Cover Form
File for Cover Form: cover.txt

Margins
Top: 0,50
Bottom: 0,50
Left: 0,80
Right: 0,25

Font
Arial, 12

Graphics (PCX files)
Header: header.pcx
Footer: <do not use Footer>

With the help of this dialog, you can set the page format, font and font size, and the headers and footers for the cover page.

Cover Page Template

The provided 'cover.txt' file is a template for the cover page and will be saved in the database.

By selecting 🔍, the file is saved and then displayed, provided a suitable program has been specified in the Windows configuration. You can also just store the cover page in the file system 💾, or delete the file in the database ✕.

To save a new cover page in the database, you can search here for an existing TXT file .... The TXT file will be saved into the database (category "Fax Cover Pages") and can be used as cover page by all users. See *7.5.10 The "Files" Tab*, Page 97.

When creating the cover page, you can enter information concerning the sender, the recipient, as well as other information such as the page number or the date as variables. This information is then replaced by the appropriate data. You can use the following variables:

Variable	Explanation
<From.Company>	Sender's company
<From.Name>	Sender's name
<From.Postal>	Sender's address
<From.Dept>	Sender's department
<From.Email>	Sender's email address
<From.Voice>	Sender's phone number
<From.Fax>	Sender's fax number
<To.Company>	Recipient's company
<To.Name>	Recipient’s name
<To.Postal>	Recipient's address
<To.Dept>	Recipient's department
<To.Email>	Recipient's email address
<To.Voice>	Recipient's phone number
<To.Fax>	Recipient's fax number
<Date>	Date
<Pages>	Number of pages
<Message>	Short message

Margins

Here you can define the width of the margins in centimeters for the cover page. This setting is applied for the display of the title page.

Font

"Select Font..." is used to define the font, the size and the typeface. This setting is applied for the display of the title page.

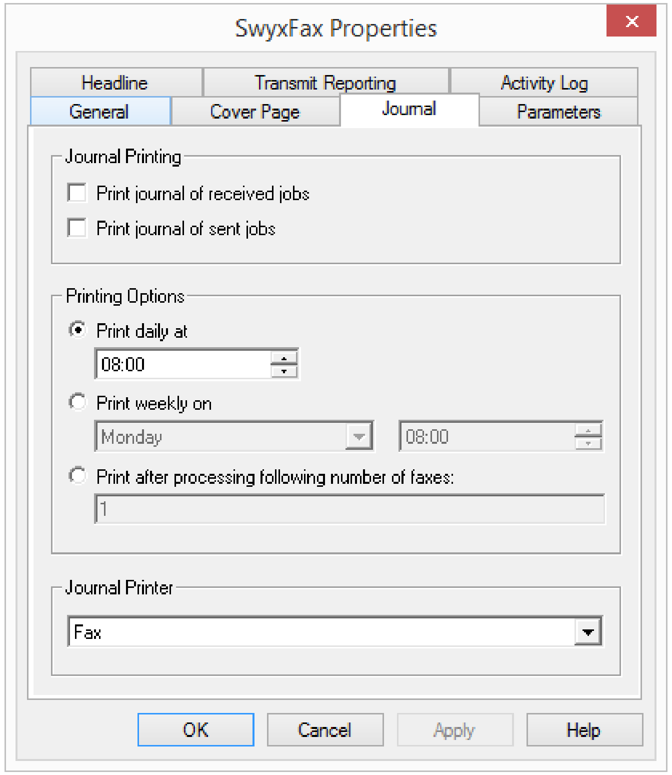
Graphic (PCX files)

You can insert graphics such as the company logo in the header or the footer of the cover page. In order to do this, you must have a PCX file in black-white display (monochromatic) with a maximum pixel size of 1768 x 2200 pixels (breadth x height). In our experience, the best size is 800 x 200 pixels.

By selecting 🔍, the file is saved and then displayed, provided a suitable program has been specified in the Windows configuration. You can store the graphic in the file system 💾 , or delete the file in the database ✕ .

To save a new graphic in the database, you can search here for an existing PCX file ... . The PCX file will then be saved into the database (category "Fax Cover Graphics") and can be used as footer or header for the cover page. See *7.5.10 The "Files" Tab*, Page 97.

24.5.3 THE "JOURNAL" TAB



Journal Printing

☐ Print journal of received jobs

☐ Print journal of sent jobs

Printing Options

● Print daily at: 08:00

○ Print weekly on: Monday 08:00

○ Print after processing following number of faxes: 1

Journal Printer: Fax

You also have the option of creating an automatic report on all incoming and/or outgoing faxes.

Print Journal

Here you can define whether an overview of all received and sent faxes should be created and on which journal printer they should be printed.

Please note that document printing is only available within a domain environment.

Print Options

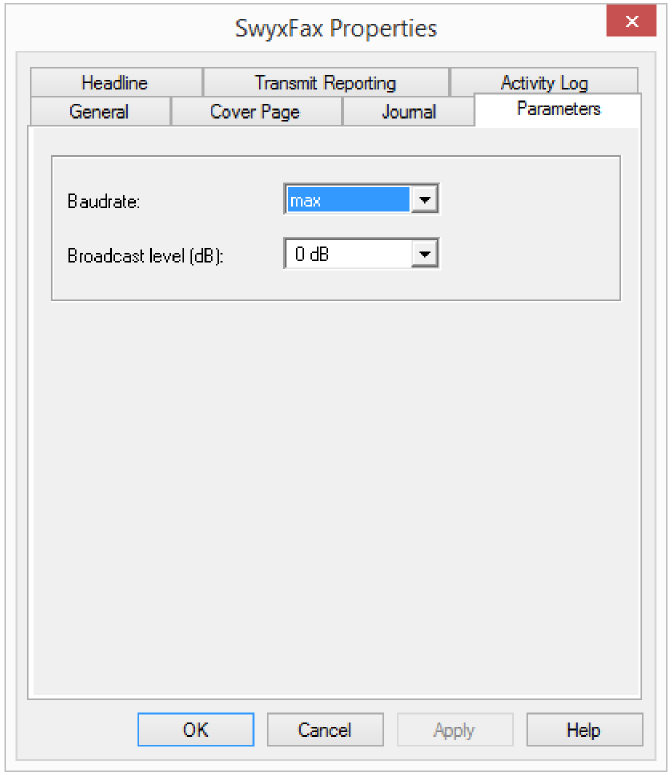
Define the time of the journal printout. The following options are available:

- Daily printout upon entry of a specific time.
- Weekly printout upon entry of a day of the week and a specific time.
- Printout after transmission/receipt of the number of fax documents entered here

Journal Printer

Here you select the printer to be used to print the journal reports.

24.5.4 THE "PARAMETERS" TAB



Baudrate: max

Broadcast level (dB): 0 dB

Here you can more specifically define the transmission parameters of SwyxFax Server.

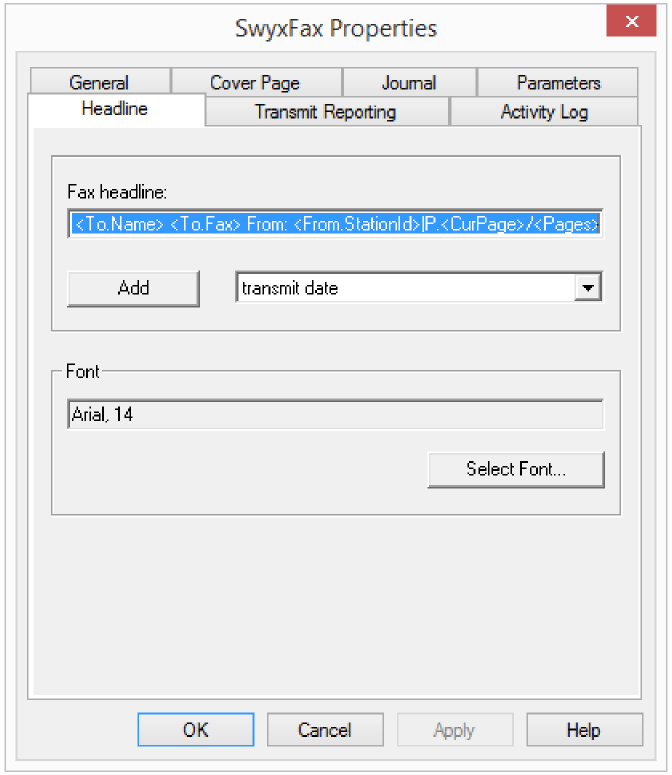
Speed

Define the transmission speed (Bps) either the maximum possible or a low rate, which you can select from the dropdown list. SwyxFax supports transmission rates of up to 14400 bits/second.

Broadcast Level (dB)

Furthermore, you can also select the broadcast level from a dropdown list.

24.5.5 THE "HEADLINE" TAB



Fax headline: <To.Name> <To.Fax> From: <From.StationId>|P.<CurPage>/<Pages>

transmit date

Font: Arial, 14

Define the header for the fax documents. This will appear each time a fax is sent and on each faxed page.

In the default setting this line has the following format:

> <CurDate> <CurTime>|To: <To.Name> <To.Fax> From: <From.Station-Id>|S.<CurPage>/<Pages>

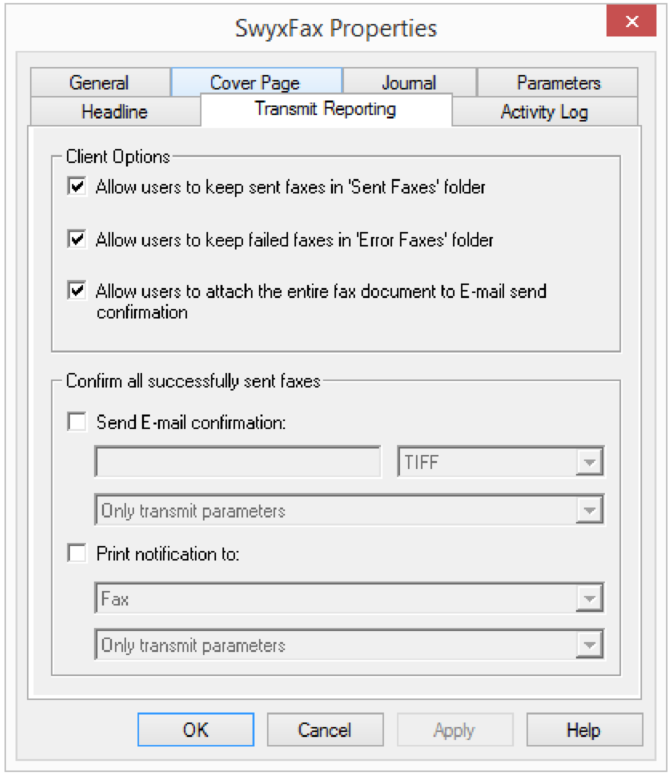
You can add a text here and make use of additional fields, which will be substituted with the current value during transmission. Select these fields from the drop-down list:

Variable	Explanation
<CurDate>	current date
<CurTime>	Current Time
<To.Name>	Recipient’s name
<To.Fax>	Recipient's fax number
<From.Name>	sender's name
<From.Fax>	Sender's fax number
<From.StationId>	Sender's Faxstation ID
<CurPage>	Current page
<Pages>	page number

Font

"Select Font..." is used to define the font, the size and the typeface to be used on the cover page. This setting is applied for the display of the header.

24.5.6 THE "TRANSMIT REPORTING" TAB



Client Options

☑ Allow users to keep sent faxes in 'Sent Faxes' folder

☑ Allow users to keep failed faxes in 'Error Faxes' folder

☑ Allow users to attach the entire fax document to E-mail send confirmation

Confirm all successfully sent faxes

□ Send E-mail confirmation: TIFF; Only transmit parameters

□ Print notification to: Fax; Only transmit parameters

Here you define whether the user should receive a transmission confirmation after each successful fax transmission. In addition, you define whether the user may decide to manage successfully transmitted faxes in the "Sent Faxes" folder and failed fax transmissions in the "Error Faxes" folder.

Client Options

If you activate the fields "Allow user to keep sent faxes in "Sent Faxes" folder" and "Allow user can keep failed faxes in "Error Faxes" folder", you give the user the option to decide whether successful or faulty fax transmissions should be managed in the folders available in SwyxFax Client.

When the field "Allow user to attach entire fax to the email send confirmation" is activated, you allow the user to decide whether he or she would like to attach the entire fax to an email transmit confirmation.

Transmit Confirmation of Error-Free Fax Transmissions

Here you define whether a transmit confirmation should be sent per email after a successful fax transmission or if a printout should be generated.

Transmit Confirmation via E-mail

Activate the checkbox "Send E-mail confirmation:". Enter the email address to which the transmit confirmation should be sent. Define the content of the e-mail. Decide whether just the transmission parameters, the transmission parameters and the first page of the fax or the transmission parameters and the entire fax should be sent.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

Transmission parameters include:

- Sender ID
- Recipient ID
- Recipient’s name
- Send Time
- Number of Pages
- Attempts
- Duration of Transmission
- Remote Station ID
- Resolution
- Speed
- Transmission Status

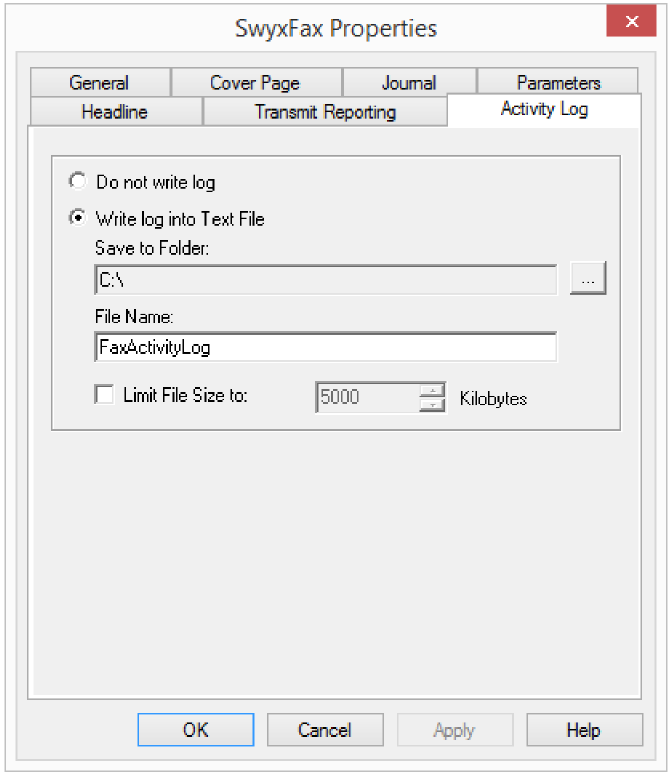
If you select "Transmission parameters and the first page" or "Transmission parameters and the entire fax", the first page or the entire fax will be attached to an email as a file. You can define the format for the file attachment. Formats include:

- TIFF or
- PDF and
- TIFF and PDF (2 attachments)

Fax Transmit Confirmation per Print

Activate the checkbox "Print confirmation to:" and select the printer. Define the content of the printout. Decide whether just the transmission parameters, the transmission parameters and the first page of the fax or the transmission parameters and the entire fax should be printed. Confirm your selection with "OK".

24.5.7 TAB "PROTOCOL"



○ Do not write log

● Write log into Text File

Save to Folder: C:\

File Name: FaxActivityLog

□ Limit File Size to: 5000 Kilobytes

SwyxWare Saves information about established connections (itemized call records) in a similar format as the "Call Detail Records" into a text file.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

While SwyxFax Server is active, and after activation in administration, information concerning all activities of SwyxFax Server (similarly to the call detail records) is written to the file 'activity.log'.

If you don't want any recordings, please enable "no protocol".

If you choose the option "Write log into Text File", you specify here the file name and the directory in the file system for saving the call detail records for SwyxFax Server. If necessary, you can limit the file size (100 – 32000 Kbyte). If the maximum file size is exceeded, a new file with the same name plus a counter will be created and filled.

For an overview of all files that are written by the fax components during operation, see 24Traces, Page 378.

24.6 FAX DOCUMENTS ON THE SERVER

Fax documents can be stored in the file system or in the database. The memory location is specified by the Configuration Wizards during the configuration of SwyxFax Server (see step (27), "Memory location for the files" in the installation).

If you want to change this memory location later, please start the Configuration Wizards again (*This is how you configure SwyxWare*, Page 54).

When saving and processing personal data, observe the respective applicable legal data protection regulations.

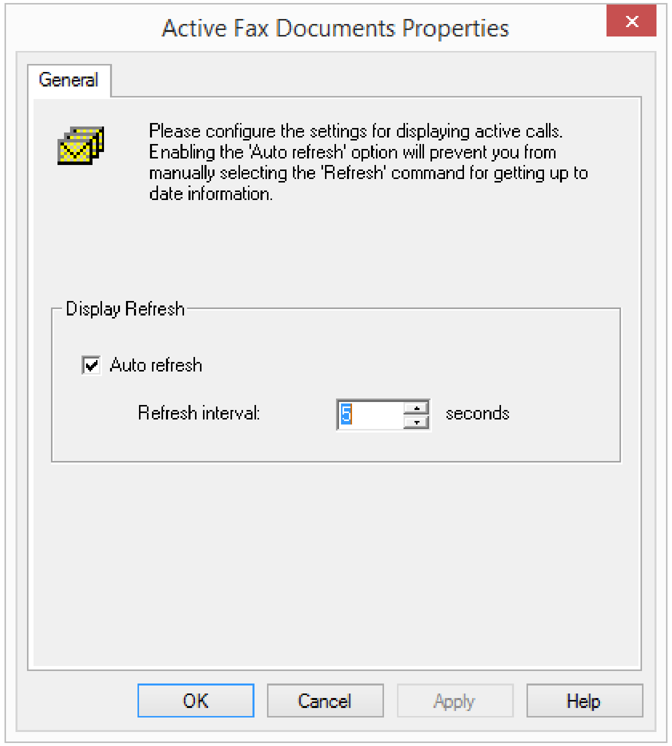
Personal data cannot be deleted automatically from the data base. In order to meet the valid data protection regulations, it may be necessary to delete the corresponding entries manually.

If the first send attempt for a fax fails, SwyxFax Server can make multiple attempts to transmit the fax. The number of repeats is set by the sending user in the SwyxFax Client.

Updating

To update the view of the faxes in SwyxFax Administration, please select "Refresh" in the context menu.

Properties of the list "Active Fax Documents"



Please configure the settings for displaying active calls. Enabling the 'Auto refresh' option will prevent you from manually selecting the 'Refresh' command for getting up to date information.

Display Refresh

☑ Auto refresh

Refresh interval: 5 seconds

You can adapt the refresh interval for the list display here to suit your needs.

Refresh View

If you would like to change the refresh interval, select "View | Options..." and enter the time interval between two updates in seconds.

The periodic update of the "Active fax documents" view will be disabled in more than one thousand active documents.

24.6.1 STORED FAX DOCUMENTS

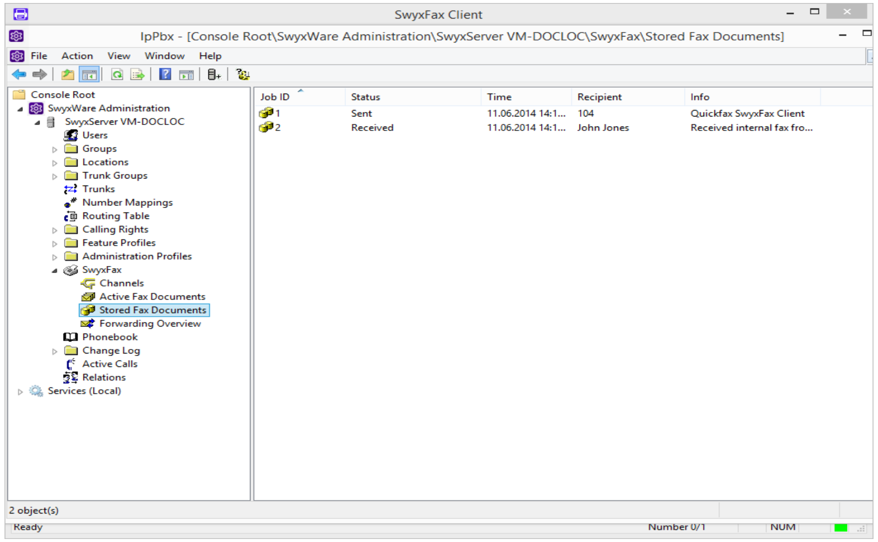
In the SwyxWare Administration under "SwyxFax | Stored Fax Documents", you have an overview of all faxes which

- were received
- were sent or
- could not be sent after a given number of repeats.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

If the first send attempt for a fax fails, SwyxFax Server can make multiple attempts to transmit the fax. The number of repeats is set by the sending user in the SwyxFax Client.

All fax jobs can be removed or reactivated here. Furthermore, you can also open detail information for each fax document.



Job ID	Status	Time	Recipient	Info
1	Sent	11.06.2014 14:1...	104	Quickfax SwyxFax Client
2	Received	11.06.2014 14:1...	John Jones	Received internal fax fro...

24.6.2 EDITING FAX DOCUMENTS

The fax documents in the lists can be further edited. To do so, open the document's context menu (right mouse button) and choose the relevant entry.

Depending on the status and processing state, you can suspend, resume, delete or reactivate documents.

Delete fax documents

To delete fax jobs, highlight the entries in the list. Then, open the context menu and click on "Delete". A single job will be deleted; for multiple documents, the delete will have to be confirmed again.

> Please remember that faxes that are deleted in SwyxFax Server are no longer available to the associated user in SwyxFax Client.

Pause

If you want to pause a fax, highlight the relevant job in the list and click in the context menu on "Pause". The highlighted fax will be stopped.

You can only pause fax documents, which are in the "Active fax documents" list and have not been sent yet.

Resume

To reactivate a paused fax (status: "Paused"), highlight the corresponding fax in the list "Active Fax Documents" and click in the context menu on "Resume". The highlighted fax will be sent once again.

You can only resume fax jobs that are in the "Active fax documents list" and have been paused.

Reactivate

To re-send a fax, highlight the corresponding fax in the "Stored Fax Documents" list. In the context menu of the highlighted fax document, click on "Reactivate".

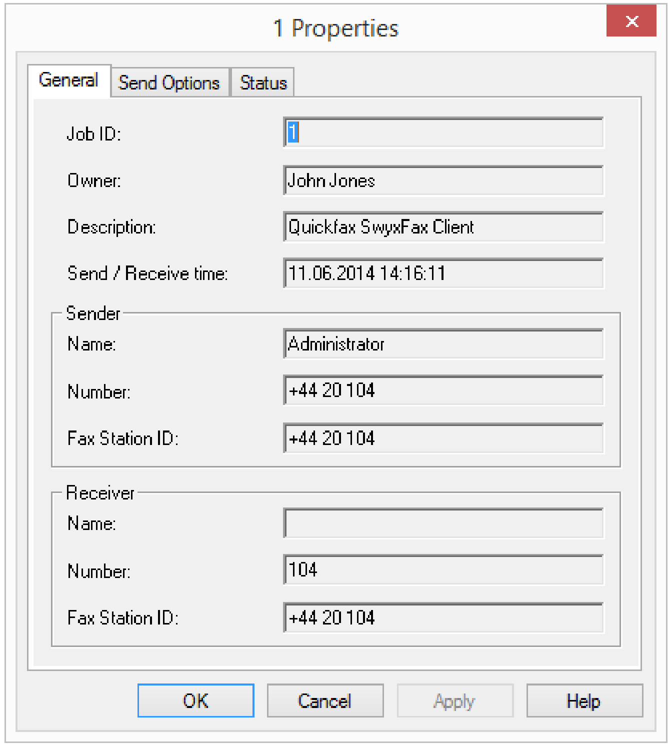
24.6.3 PROPERTIES OF A FAX JOB"

To obtain details about an individual job, highlight a job and choose "Properties" in the context menu.

> These details provide information only. You do not have the option of changing the listed parameters.

The corresponding tabs will be described below.

24.6.3.1FAX DOCUMENT "PROPERTIES": "GENERAL" TAB



1 Properties

General | Send Options | Status

Job ID: 1

Owner: John Jones

Description: Quickfax SwyxFax Client

Send / Receive time: 11.06.2014 14:16:11

Sender

Name: Administrator

Number: +44 20 104

Fax Station ID: +44 20 104

Receiver

Name:

Number: 104

Fax Station ID: +44 20 104

Here you will find information on the sender and recipient of the highlighted fax job.

The Job ID, owner (SwyxWare user name), a description and the time of sending or receiving are displayed.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

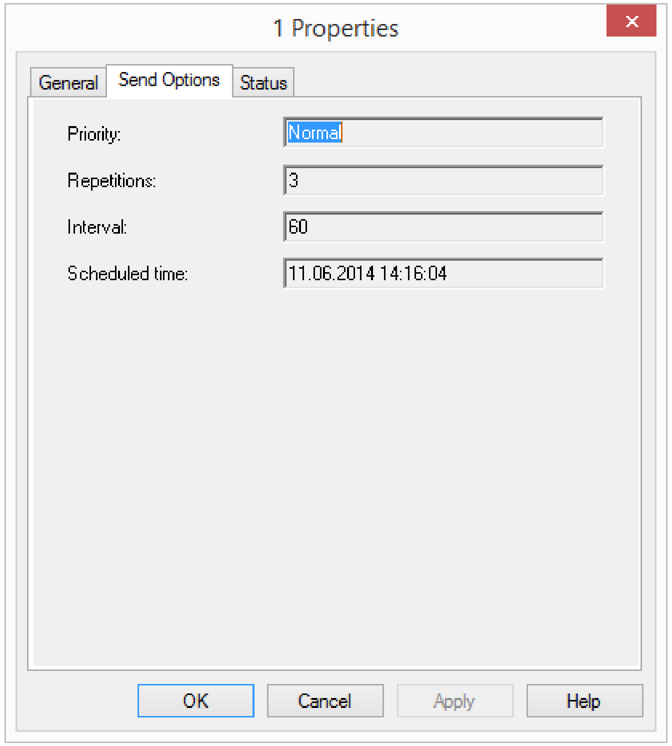
Sender / Receiver

Here you will find information on both the sender and the recipient:

- Name
- Number
- Fax Station ID

This information cannot be changed.

24.6.3.2FAX DOCUMENT "PROPERTIES": "SEND OPTIONS" TAB



1 Properties

General | Send Options | Status

Priority: Normal

Repetitions: 3

Interval: 60

Scheduled time: 11.06.2014 14:16:04

This information is only available for sent documents or those to be sent.

Priority

You can assign different priorities when creating a fax job. The priority levels 1 (high) and 0 (normal) are available.

Repetitions

If it was not possible to transmit a fax, you will see the number of retry attempts undertaken if a transmission error occurred.

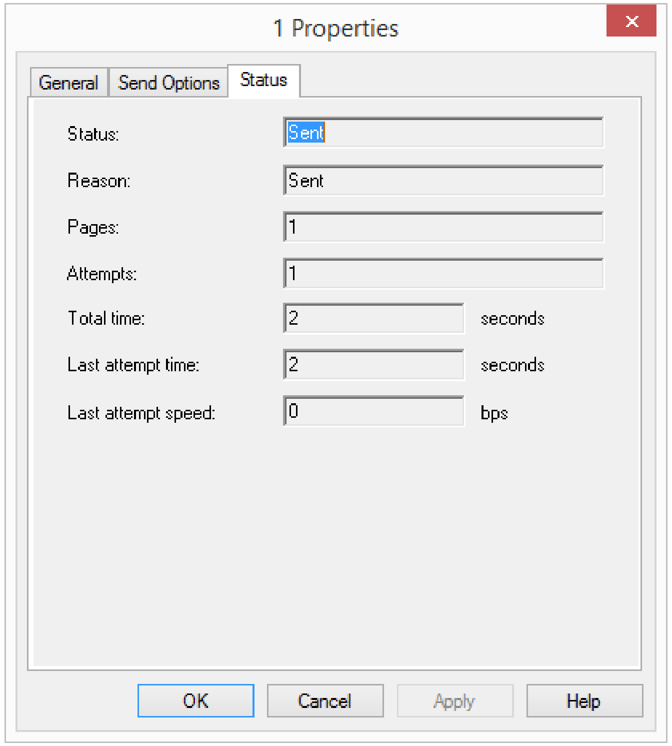
Interval

The interval (in seconds) is the time period between a failed transmission attempt and the next transmission attempt.

Scheduled time

Scheduled time for sending a fax.

24.6.3.3FAX DOCUMENT "PROPERTIES": "STATUS" TAB



Status: Sent
Reason: Sent
Pages: 1
Attempts: 1
Total time: 2 seconds
Last attempt time: 2 seconds
Last attempt speed: 0 bps

In this dialog you can check the status of the highlighted fax document.

Status

Here you will see whether a fax has already been read (email delivery also counts as read), has already been sent, whether it is waiting to be sent or whether an error has occurred.

If problems during transmission or the reception of the fax occured, the field "Info" will provide more detailed information.

Pages

Displays the number of pages in this fax.

Attempts

Lists the number of send attempts.

Duration

Lists the total transmission time or the time to the next send attempt.

Last attempt time

When the last transmission attempt was started.

Last attempt speed

This gives the Bps with which the last transmission attempt was started.

24.7 FAX CHANNELS

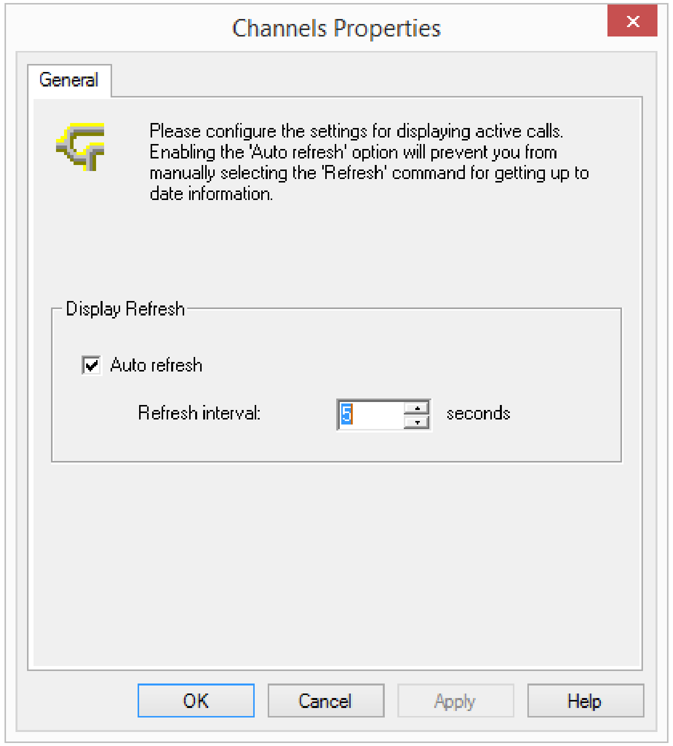
Fax channels are created and configured in the SwyxWare Administration. You can create the channels individually or several together and afterwards change the corresponding properties.

Please remember that you can only create as many fax channels as are licensed in SwyxServer (fax channel = voice channel + fax channel license). The fax channel license is simply the expansion of an existing voice channel into a fax channel, and does not offer a license for an independent additional channel.

Updating

To update the view of the faxes in SwyxFax Administration, please select "Refresh" in the context menu.

Parameters of the list "Fax Channels"



Channels Properties

General

Please configure the settings for displaying active calls. Enabling the 'Auto refresh' option will prevent you from manually selecting the 'Refresh' command for getting up to date information.

Display Refresh

☑ Auto refresh

Refresh interval: 5 seconds

You can adapt the refresh interval for the list display here to suit your needs.

Add

Start the SwyxWare Administration and enter all of the license keys for the fax channels in SwyxServer (24Licenses, Page 361). Then add the appropriate number of fax channels. A fax channel wizard will appear which will help you to install the fax channels, and which will prompt you to enter parameters, such as the fax station ID. After you have made all settings, all fax channels appear in the "Channels" list.

This is how you create a new fax channel

1. In the SwyxWare Administration tree structure, open the entry SwyxFax.
2. In the context menu of "Channels", select "Add Channel...".
   The fax channel wizard appears.
   Click on "Next>".
3. Operating steps:
   Indicate whether this channel should only receive or send faxes or both.
   Click on "Next>".
4. Faxstation ID:
   Enter the number, which should be transmitted to the sending fax device as identification when a fax is received. The canonical format is usually selected here, e.g. +44 1234 567890.
   Click on "Next>".
5. Channel Reservation:
   Enter the numbers to which the SwyxFax Server should react. You can enter several numbers or number ranges separated by a semicolon. (e.g. 100-199; 356; 401).
   Alternatively, enable the "Use channel for all calls" option.
   Click on "Next>".
6. Internal default number
   Select here an internal fax number that will be used for outgoing calls if the SwyxFax Client has configured "Use channel default".
7. Number of fax channels:
   Enter how many fax channels you would like to create with the given parameters. The fax channel wizard offers you the maximum possible number of licensed channels.
   Click "Finish".

The desired number of fax channels will be created. A corresponding list will appear in the "Channels" window.

You can still change all parameters of a fax channel later (*24.7.1 Fax channel properties*, Page 374).

Remove

If you would like to remove a fax channel, highlight the corresponding fax channel in the "Channels" window and select "Remove" in the context menu. The highlighted channel will be removed from the list.

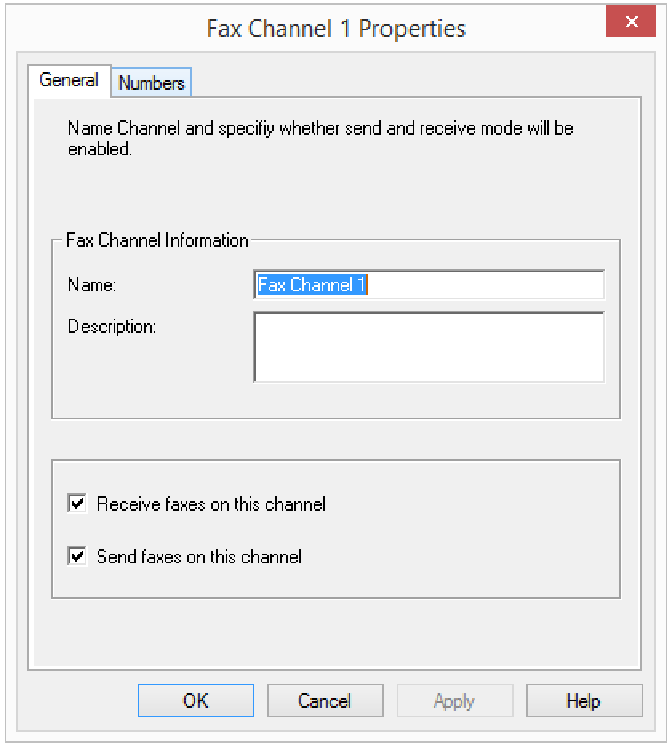
24.7.1 FAX CHANNEL PROPERTIES

This dialog helps you to configure the various parameters for the highlighted fax channel.

The values entered always refer to the highlighted fax channel. You can configure the fax channels individually.

The data, which you have entered when creating these fax channels, were applied as the default setting. You can still change these values here.

24.7.2 THE "GENERAL" TAB


Fax Channel 1 Properties

Name Channel and specifiy whether send and receive mode will be enabled.

Fax Channel Information

Name: Fax Channel 1

Description:

☑ Receive faxes on this channel

☑ Send faxes on this channel

This tab can be used to configure the general information of the fax channel.

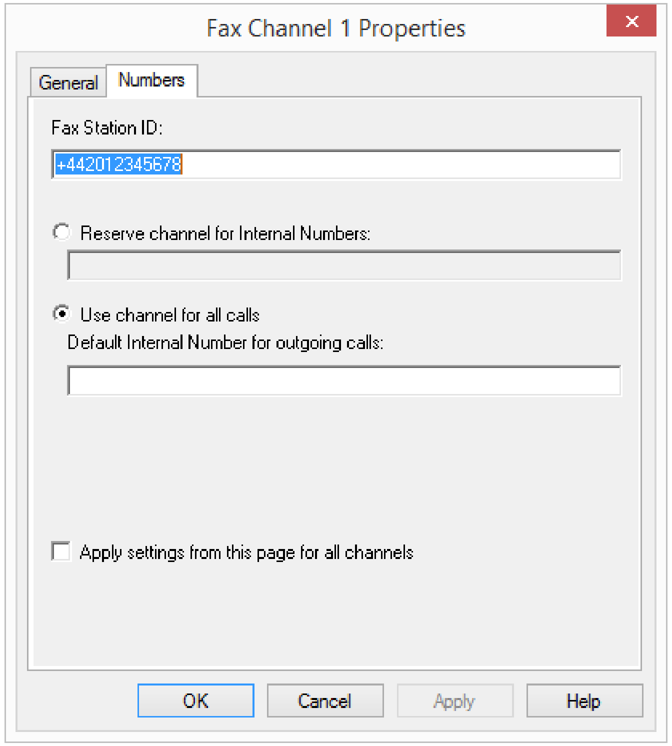
Fax Channel Information

The name of the fax channel can be changed. Make sure that the name is unique. As description, you can insert supplementary comments here.

Receive faxes on this channel / Send faxes on this channel

Here you can decide whether the selected fax channel should only be used to send and/or receive faxes. In order to achieve optimal availability, you can assign a number of channels for fax reception only, for example.

The "Numbers" Tab



Fax Station ID: +442012345678

○ Reserve channel for Internal Numbers:

● Use channel for all calls

Default Internal Number for outgoing calls:

□ Apply settings from this page for all channels

This dialog can be used to define the number to be signaled externally.

Fax Station ID

Enter here the number that the SwyxFax should transmit to the sending fax device when it receives a fax.

Reserve Channel for internal numbers

Here you can enter the fax extensions or ranges to which this fax channel should react, both when sending and receiving faxes. Please use only valid, i.e. already assigned fax numbers.

If this field remains empty, this channel will react to all fax extensions.

Several numbers separated by semicolons can be entered here.

Example:

If you enter "100-102;205", SwyxFax will react to the numbers 100, 101, 102 and 205.

Use Channel for All Calls

Enter the internal default number here. This number will be signaled to the telephone network when sending a fax. This default number is only used if the SwyxFax Client has configured "Use channel default". Please use only a valid, i.e. an already assigned fax number.

Clear

To restart an individual fax channel, highlight the relevant fax channel, and select "Channel | Reset" in the menu. If you want to reset all channels, restart the SwyxFax Server service.

24.8 FAX FORWARDING AS FAXMAIL OR PRINTED DOCUMENT

SwyxFax supports the delivery of fax documents via e-mail. SwyxFax uses the same mail server that SwyxServer uses to send voice messages. You only have to enter the email addresses for forwarding in the user administration.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

Fax forwarding refers to all fax documents that a user receives, regardless of whether this user has different fax numbers.

Format of the Faxmail

The Faxmail contains not only the sent document as an attachment, but also information about the document in the subject line and in the text of the email.

- Subject line
  Fax from Station <Sender's number> (<Sender's name>, if this can be resolved)
- Email text
  The email text contains detailed information on the fax procedure:
  Sender information

      Number, name, (if this can be resolved) and the transmitted Faxstation ID.

  Recipient information, e.g. the destination fax number
  Information about the transmission process

      Date (dd.mm.yyyy hh:mm), number of pages, duration of transmission process (mm:ss), the resolution (in dpi), the speed (baud rate, internal fax), the status (e.g. receive errors, successful transmission)

- Name of the attached file
  The attached file has a name which is composed from several parameters and is thus unique, so that the document can be stored directly under this unique name.

  faxdoc-
  <Date in format ddmmyy>-
  <Time in format hhmm>-
  <Sender's number>-
  <Sender's name>, if this can be resolved.
  <File format PDF or TIFF>

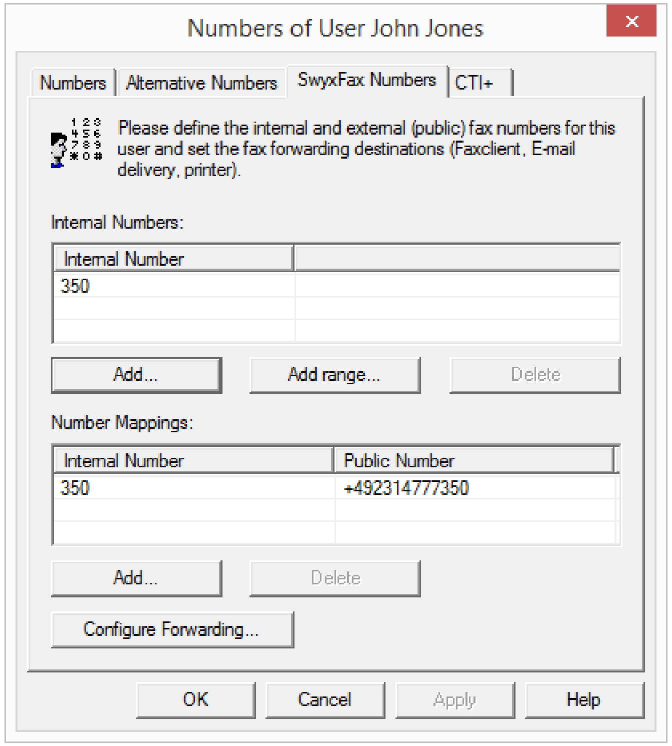
This is how you configure forwarding as Faxmail

1 Open the user list.

2 Open the user properties in the context menu.
The user's administrator properties open up.

3 Select the dialog "Numbers...".

4 Go to the "SwyxFax Numbers" tab.



Please define the internal and external (public) fax numbers for this user and set the fax forwarding destinations (Faxclient, E-mail delivery, printer).

Internal Numbers:

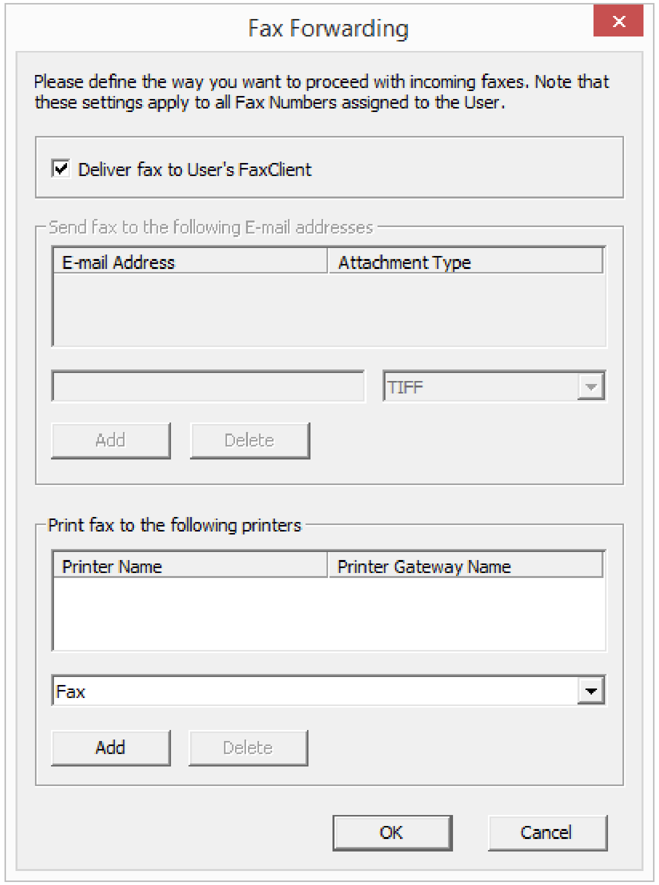
Internal Number	
350	

Number Mappings:

Internal Number	Public Number
350	+492314777350

5 Click on "Configure fax forwarding...".

6 The tab "Fax forwardings" appears.



Fax Forwarding

Please define the way you want to proceed with incoming faxes. Note that these settings apply to all Fax Numbers assigned to the User.

☑ Deliver fax to User's FaxClient

Send fax to the following E-mail addresses

E-mail Address	Attachment Type

TIFF

Print fax to the following printers

Printer Name	Printer Gateway Name

Fax

7 Choose the forwarding type. You can also select multiple options:

- SwyxFax Client
  In this case the fax document is stored on the SwyxFax Server, and can be retrieved by the SwyxWare user with the help of the SwyxFax Client.
- Email with fax attachment
  Enter the email address (e.g. "user@company.com") to which a Faxmail should be sent.
  Select the format of the email attachment. The fax document can be attached to the email in TIFF and/or in PDF format. If you select "TIFF and PDF", the email will include two attachments.
- Printing
  Activate this option if you want every fax to this fax extension to be output to the printer too. It is also possible to specify multiple printers here.

8 Confirm your input by clicking on "OK".

If you want to have your fax sent by email, you have to use the internet notation for email addresses, i.e. the address must contain the "@" symbol.

If you define forwarding only by email for a user, the fax will be deleted from the SwyxFax Server management after it is transferred to the email server.

Fax documents attached to an email can be TIFF or PDF files. These files are automatically opened by the programs (Windows Photo and Fax-viewer or Microsoft Office Document Imaging) which are included in the Windows 2000 and XP operating systems. To open PDF documents you will need Adobe Acrobat Reader. You will find it on your SwyxWare DVD.

The fax documents are saved as DCX files within SwyxFax. SwyxFax Client uses the SwyxFax Client viewer for displaying these documents.

24.9 FORM STORAGE

SwyxFax offers you the option of adding forms, such as letterhead, to the fax documents before they are sent. These are graphics files, which are stored in the database and which are added to the fax when it is sent.

You can choose different letterheads for the first page (after the cover page) and each additional page of the fax. In SwyxFax Client you can choose from the letterheads present in the database.

The forms must be stored as a PCX file in the database, in the category "Fax Letterhead". See *7.5.10 The "Files" Tab*, Page 97.

Format of the Letterhead Files

The PCX graphics must have a resolution of 1728x2338 and can have two colors. You can create such a PCX file using a graphics program (e.g. Irfan View). Alternatively, the following provides a description of how you can create such a file with the help of the SwyxFax Client.

This is how you create a letterhead

1. Design a new letterhead in an application (for example, Microsoft Word).
   Make certain that the letterhead has the DIN A4 format because otherwise you will have problems applying it to the documents to be sent.
2. Print the document you have created from this application and select the printer "SwyxFax".
   The SwyxFax Client Send dialog will be opened.
3. Deactivate the option "Send Cover Page" and enter your own fax extension in the "Fax" field and send the fax.
4. In a moment (refresh interval), the sent fax will appear in your fax inbox of your SwyxFax Client.
5. Highlight the fax in the fax inbox and open the context menu (right mouse button).
6. Select "Export...".
   The "Export Fax..." window will open.
7. Display the page you created as a letterhead and select "Export...".
8. Then select the format "PCX" and save the displayed page. The "Export" function always saves the currently displayed page only.
9. The PCX file created can be saved into the database (category "Fax letterhead") If you don't activate the option "Private", this template is available to all SwyxFax Client users as a form. See *7.5.10 The "Files" Tab*, Page 97.

24.10 TRACES

While SwyxFax Server is active, information regarding the operation will be written in files per default, ***E.5 Traces of the SwyxWare Services***, Page 428.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

- IpPbxFaxPrtGate-XXX (at error level per default)
  contains the messages of the SwyxFax Printer Gateway, and thus replaces the file 'printer log' from now on.
  You will find this file on the PC on which the 'SwyxFax Printer Gateway' service is started, in the directory "C:\ProgramData\Swyx\Traces".
- IpPbxFaxSrv-XXX (at error level per default)
  contains the messages of the SwyxFax Server.
  You will find this file on the PC on which the 'SwyxFax Server Printer Gateway' service is started, in the directory "C:\ProgramData\Swyx\Traces".
- activity.log
  This file contains information regarding all SwyxFax Server activities (Call Detail Records).
  You will find the settings for this Report file in the properties of SwyxFax Server (*24.5.7 Tab "Protocol"*, Page 368).
- MemoryDumps
  Here you will find DMP files as a reflection of the current memory. You will find this file on the PC on which the 'SwyxFax Server ' service is started, in the directory "C:\ProgramData\Swyx\MemoryDumps".

24.11 SWYXFAX PRINTER GATEWAY

You can specify one or more printers in the Fax forwarding table as recipients. Faxes that are assigned to a printer are processed by a separate Windows service "SwyxFax Printer Gateway".

This service is an independent component and is installed as default on the SwyxFax Server computer during installation, and automatically started in a restart. It regularly checks for print jobs from SwyxFax Server. These are executed and then removed from the fax job list. Therefore, print jobs are only visible for a short time in the SwyxFax Administration.

If for some reason the print job cannot be executed, for example because the SwyxFax Printer Gateway does not have access to the defined printer, the print job will be given the "Error" status and will remain in the fax job list.

User account of the SwyxFax Printer Gateways

SwyxFax Printer Gateway usually logs in using the user account in which the SwyxFax Server service is started. This user must therefore also have access rights for all of the printers required.

Alternatively, the configuration of the SwyxFax Printer Gateway can be changed so that it logs in under a different user account. To do this, start the configuration wizard and enter a different user account, which thus gains the necessary access rights.

24.12 PRINTING SERIAL LETTERS WITH SWYXFAX CLIENT

You can print serial letters from a Microsoft Office application (e. g. Word). To do this, create the letter as a Word document and enter defined serial print fields instead of an address. For more information on this, please refer to the documentation for the Microsoft application.

This function allows you to create and send serial faxes in SwyxFax Client.

Please refer to help.enreach.com/cpe/latest.version/FaxClient/Swyx/en-US/index.html#context/help/print_fax_$ for information on how to print serial faxes with SwyxFax Client.

25 SWYXCTI AND SWYXCTI+

With SwyxIt! in CTI mode (CTI SwyxIt!), you can control phones from your computer..

With SwyxCTI the following options are available:

- CTI SwyxIt! controls a SwyxPhone
- CTI SwyxIt! on a terminal server controls SwyxIt!

Additionally, the SwyxCTI+ option contains the following functions:

- CTI SwyxIt! controls a third-party telephone, such as a DECT telephone
- CTI SwyxIt! controls an external telephone via its call number

See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/phonecontrol_cti_$.

You need an appropriate license for the use of the SwyxCTI+ option.

If you use SwyxCTI+ in combination with SwyxWare for DataCenter, you have to activate "SwyxCTI" and "SwyxCTI+" in the standard feature profile.

In column "CTI+" of SwyxWare Administration user list, you can see if CTI+ is configured for a user. The number of users cannot be bigger than the number of available SwyxCTI+ licenses.

Using SwyxIt! in a terminal server environment is only useful, if SwyxIt! is operated in CTI mode. In order to achieve this, a registry key must be set. For further information please refer to the knwoledge database HOW TO: service.swyx.net/hc/en/articles/360000022140-How-to-force-use-of-CTI-in-SwyxIt-Client

25.1 AUTHORIZE SWYXCTI+ WITH A THID PARTY PHONE

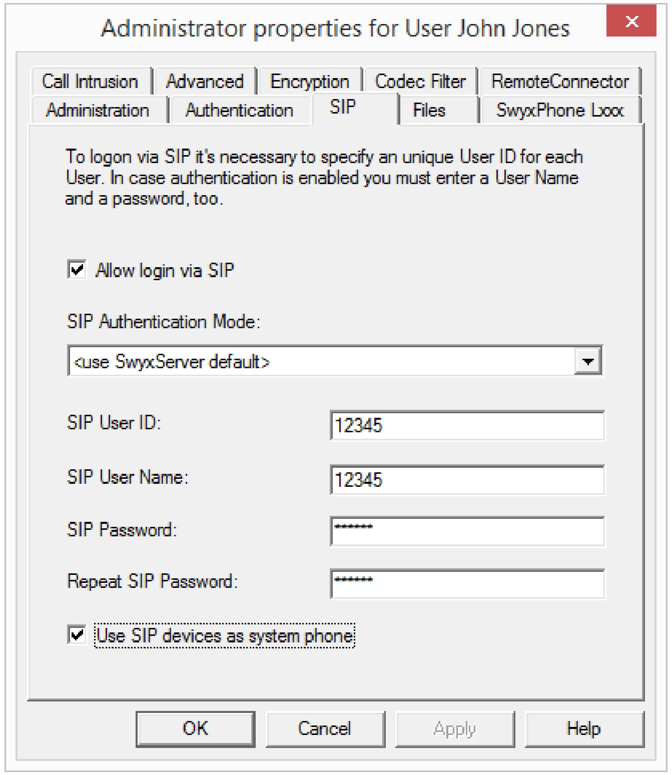
SwyxCTI+ with a third party device can be authorized within the user properties or the SIP registration. There, you can authenticate SIP devices for the user.

How to authorize SwyxCTI+ with a third party phone

1 Click an entry in the user list with the right mouse button.

2 Select "Properties" in the context menu and click on "Administration...".

3 Activate the "Allow logon via SIP" option in the "SIP" tab and enter SIP User-ID, SIP user name and SIP password into the respective fields.



Administrator properties for User John Jones

To logon via SIP it's necessary to specify an unique User ID for each User. In case authentication is enabled you must enter a User Name and a password, too.

☑ Allow login via SIP

SIP Authentication Mode: <use SwyxServer default>

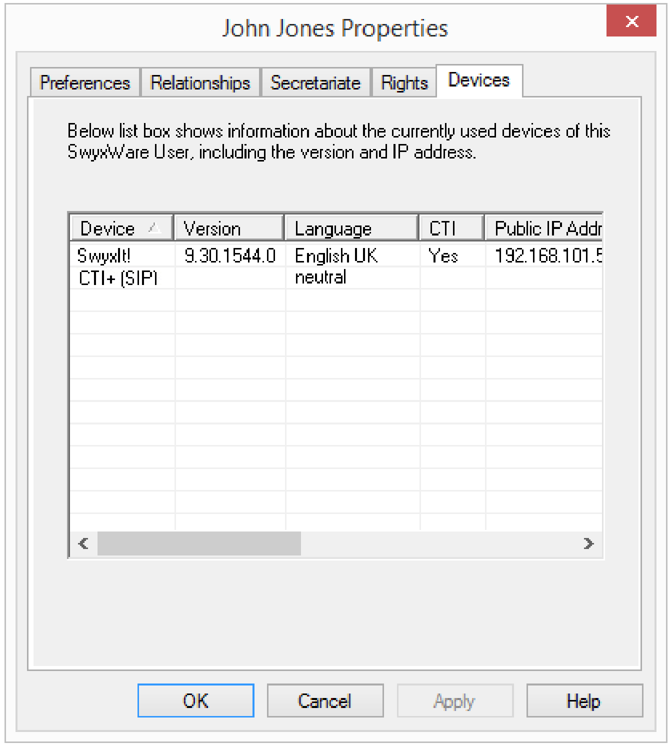
SIP User ID: 12345

SIP User Name: 12345

SIP Password: ******

Repeat SIP Password: ******

☑ Use SIP devices as system phone



John Jones Properties

Below list box shows information about the currently used devices of this SwyxWare User, including the version and IP address.

Device	Version	Language	CTI	Public IP Addr
SwyxIt!	9.30.1544.0	English UK	Yes	192.168.101.5
CTI+ (SIP)		neutral		

4 Activate "Use SIP devices as system phone" to authorize SwyxCTI+ with a third party device.

5 Click on "OK" and again on "OK".

Under the "Devices" tab in the user properties, the entry "CTI+ (SIP) is now listed among the used devices.

If the entry is not visible, the service has not been started or not enough SwyxCTI+ licenses are available. Check the entries in the Eventlog.

After activation of this option, SIP devices are no longer able to perform special functions, such as on hold, call swap, call transfer, and start or pick up second call. However, some of these functions can be set via function codes.

Please refer to *Feature Code (only possible as block dialing)*, Page 357 for further information on using DTMF strings with CTI+.

25.2 AUTHORIZE SWYXCTI+ WITH EXTERNAL PHONE VIA ITS NUMBER.

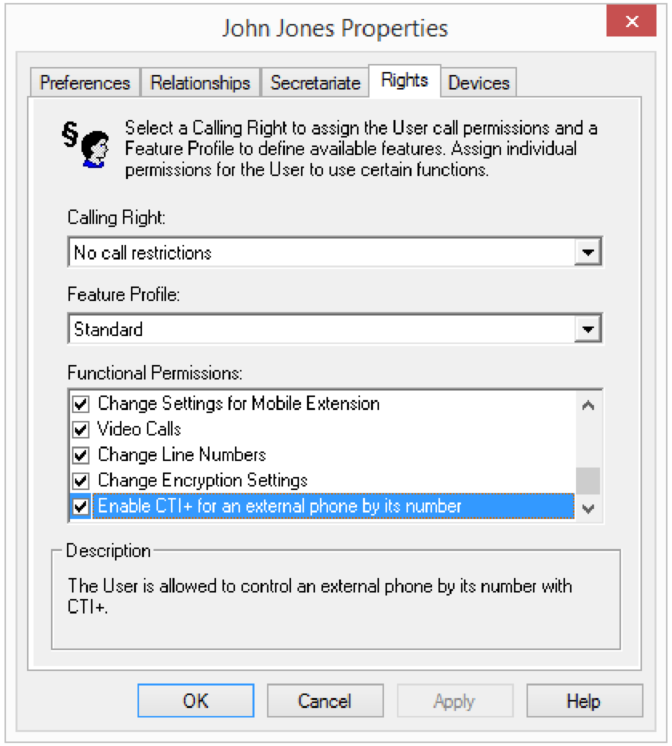
SwyxCTI+ with an external phone via its number can be configured in the user properties on the "Rights" tab.

This option is disabled by default, as an activation would significantly increase resource consumption (e.g. memory usage, start and stop behaviour.

How to authorize SwyxCTI+ with an external phone via its number.

1 Click an entry in the user list with the right mouse button.

2 In the context menu, select "Properties" and click on the "Rights" tab.



Select a Calling Right to assign the User call permissions and a Feature Profile to define available features. Assign individual permissions for the User to use certain functions.

Calling Right: No call restrictions

Feature Profile: Standard

Functional Permissions:

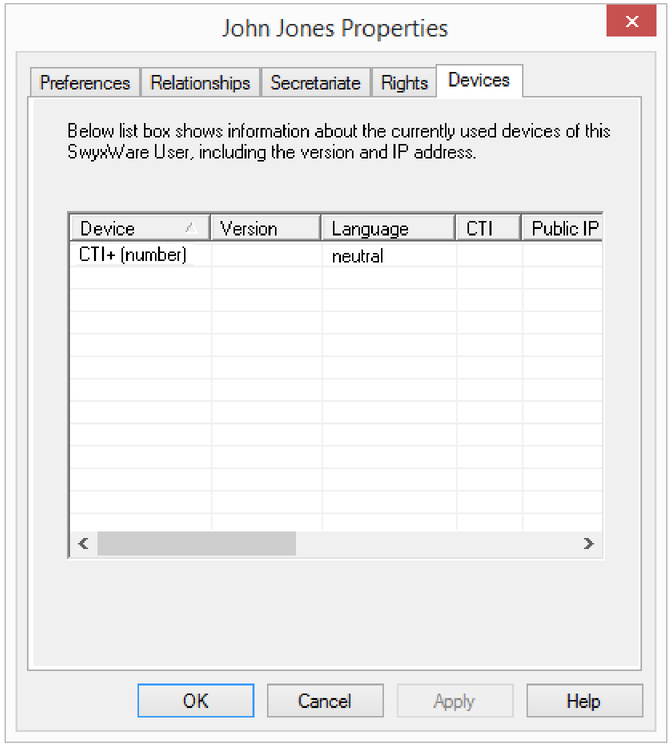
- ☑ Change Settings for Mobile Extension
- ☑ Video Calls
- ☑ Change Line Numbers
- ☑ Change Encryption Settings
- ☑ Enable CTI+ for an external phone by its number

Description

The User is allowed to control an external phone by its number with CTI+.

3 Under "Functional Permissions:", activate the option "Enable CTI+ for an external phone by its number".

4 Click on "OK".
Under the "Devices" tab in the user properties, the entry "CTI+ (number) is now listed among the used devices.
If the entry is not visible, the service has not been started or not enough SwyxCTI+ licenses are available. Check the entries in the Eventlog.



Below list box shows information about the currently used devices of this SwyxWare User, including the version and IP address.

Device	Version	Language	CTI	Public IP
CTI+ (number)		neutral		

Please refer to *Feature Code (only possible as block dialing)*, Page 357 for further information on using DTMF strings with CTI+.

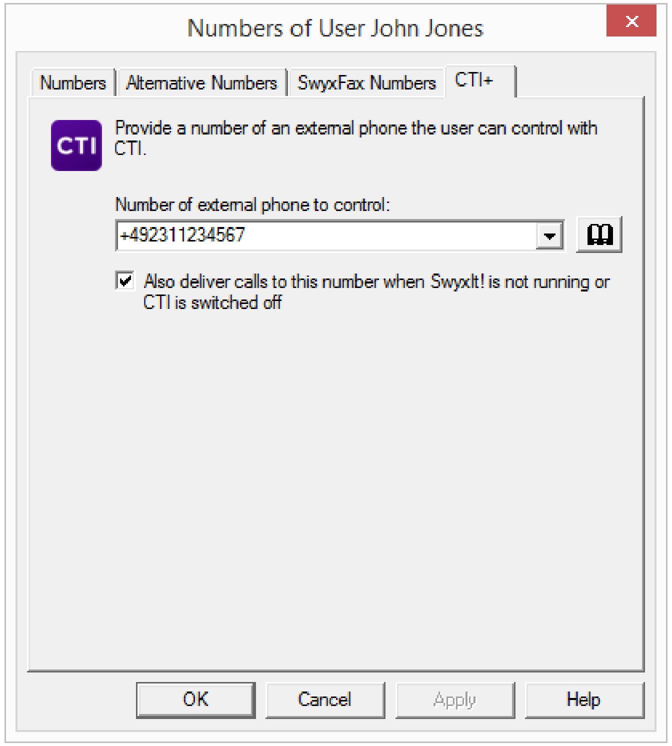
25.2.1 CONFIGURE A CTI PAIRING TO THE NUMBER OF AN EXTERNAL PHONE

The user can enter a phone number in SwyxIt!, with which he/she wants to control an external phone. It is also possible to enter this number in the SwyxWare Administration, so it is already available in the SwyxIt! CTI dialog, when the user sets up the CTI pairing. These two entry options are equal, i.e. deleting a number in the SwyxIt! CTI dialog will also delete the number in SwyxWare Administration.

> If a number of an external phone is assigned to the user, which has been previously assigned to another user as a CTI pairing, the first user immediately loses his/her CTI pairing with this phone.

How to create a CTI pairing with the number of an external phone.

1. Click an entry in the user list with the right mouse button.
2. Select "Properties" in the context menu and click on "Numbers".
3. Click on the "CTI+" tab and enter the number of the external phone into the entry field.



Provide a number of an external phone the user can control with CTI.

Number of external phone to control: +492311234567

☑ Also deliver calls to this number when SwyxIt! is not running or CTI is switched off

With the option "Also deliver calls to this number when SwyxIt! is not running or CTI is switched off" you ensure that incoming calls are forwarded to the external phone independently from SwyxIt!, even if the computer of the user is shut down or CTI is deactivated.

4. Click on "OK" and again on "OK".

> Please note that a CTI pairing with a number, which is assigned to the same user account is not possible.

How to change a CTI pairing with the number of an external phone.

1. Click an entry in the user list with the right mouse button.
2. Select "Properties" in the context menu and click on "Numbers".

3 Click on the "CTI+" tab and enter the number of the new external phone into the entry field.

4 Click on "OK" and again on "OK".

⚠ Please note that this change becomes immediately effective in SwyxIt!. The CTI pairing with the new phone will be created immediately and directly without any further confirmation.

How to delete a CTI pairing with the number of an external phone.

1 Click an entry in the user list with the right mouse button.

2 Select "Properties" in the context menu and click on "Numbers".

3 Click on the "CTI+" tab and delete the number of the external phone in the entry field.

4 Click on "OK" and again on "OK".

⚠ Please note that this change becomes immediately effective in SwyxIt!. The CTI pairing will be deleted directly.

26 CROSS-NETWORK CONNECTIONS

Configuration of SwyxWare for cross-network connections

- Internet connection via RemoteConnector

The RemoteConnecotor establishes a direct and secure connection between clients and SwyxServer via a TLS tunnel. The client does not need to be logged-on to the company network (LAN) or a virtual private network (VPN).

- WAN connections

Thanks to the "Trunks" concept, SwyxWare now supports an inter-location structure independent of the type of trunk used. The trunks/trunk groups simply represent instances of connections between locations/ conversation partners.

The route used to set up a connection is defined in detail via the Routing Table and Calling Right profiles.

For configuring forwarding or call permissions, see *14 Routing*, Page 239 or *9.1 Call Permissions*, Page 128.

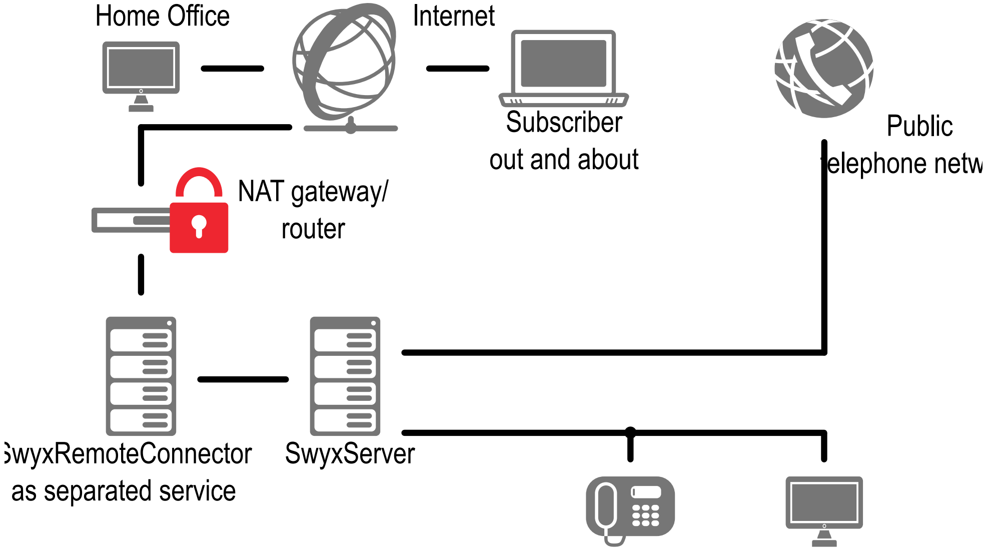
26.1 INTERNET CONNECTION VIA REMOTECONNECTOR

Remote Connector for SwyxIt! is a SwyxWare service that enables and manages the connection of SwyxWareclients to SwyxServer or Swyx-Standbyservers from the Internet. A direct TLS-encrypted connection is set up between the server and the client.

settings of the RemoteConnector for SwyxIt! have no influence on the RemoteConnector for Yealink.

Registrations via Internet with Windows user data are not possible. Make sure that you have configured authentication by user name and password for the user, see *Authentication with user name and password*, Page 166

A subscriber with SwyxIt! installed and configured can log-on to Swyx-Server and use SwyxWare telephony from his/her home office and via any type of Internet connection almost without any restrictions.



The user list of SwyxWare Administration shows whether the user is currently connected to one of his clients via RemoteConnector:
In this case, the column "via RemoteConnector" contains a "Yes".

When connecting via RemoteConnector DATEV, SwyxIt! Meeting, the SwyxIt! video function and SwyxIt! on a terminal server are not available in the current version.
When using a VPN connection, however, above functions can be used in their full scope.

see also *Authentication Service*.

26.1.1 AUTHENTICATION SERVICE

As of v12.20 SwyxIt! uses the authentication service for connections via RemoteConnector analogue to Swyx Mobile and Swyx Desktop for macOS.

This services establishes connections via RemoteConnector in a simple yet secure way. Within the client settings, users simply enter the public end point (as FQDN or IP Address) of the company network, to which the authentication service is connected.

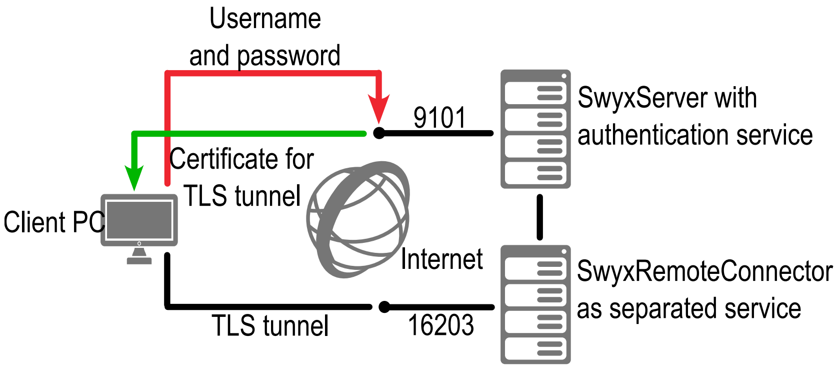


Fig. 26-1: Establishing connections via authentication service

When a connection is established, the client sends a request to the public endpoint and authenticates itself via HTTPS by using its SwyxWare user name and password. The required configuration data for the TLS tunnel (e. g. the client certificate and server address of the RemoteConnector) is transferred to the client computer (and/or smartphone), saved for further connections and subsequently updated as required.

26.1.2 CONFIGURATION

The Internet connection on the server is ensured by RemoteConnector server. This service can also be installed separately.

The RemoteConnector component comes standard activated for the SwyxServer and is also installed. The functionality of RemoteConnector has to be configured in the Swyx Connectivity Setup Tool, see *6 Swyx Connectivity Setup Tool*, Page 68.

The user's Internet connection is run through RemoteConnector Client. This service is integrated into clients and does not require any additional installation steps, see *26.1.3 Configuration of SwyxIt!*, Page 387.

Port forwarding via router

In order for the query from SwyxIt! out of the Internet to be forwarded to the RemoteConnector server on the company network, the forwarding needs to be configured on the company router (or NAT gateway) from the public "IP address:port" to the IP address of SwyxServer and TCP-Port 16203.

The following table illustrates an example configuration for a company network with only one public IP address:

Port forwarding to...	Public IP address:TCP port	Target IP address:TCP port
RemoteConnector on the SwyxServer	205.0.0.1:16203	192.168.0.2:16203
RemoteConnector as separated service	205.0.0.1:16203	192.168.0.16:16203

Port forwarding to the authentication service

In addition to the port forwarding to the RemoteConnector, the port forwarding to the authentication service must also be configured on the company router.

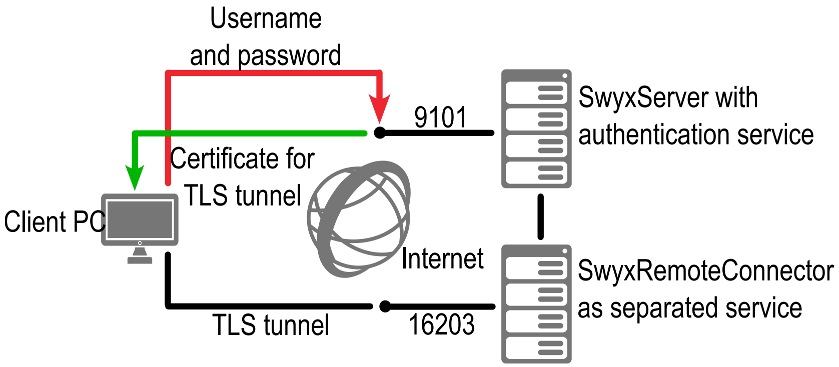


Fig. 26-2: Establishing connections via authentication service

The "public IP address(:port)" combinations must be entered into the Client connection settings. SwyxIt! automatically uses port 9101 if you don't specify a port. If there is also a valid resolvable DNS name on the Internet for the public IP address, then you can also use that in in stead of the public IP address.

See *26.1.3.1 Configure connection via RemoteConnector*, Page 387 (5), (6)).

The following table illustrates an example configuration:

Port forwarding to...	Public IP address:TCP port	Target IP address:TCP port
Authentication Service	server.net:9101	192.168.0.4:9101

26.1.3 CONFIGURATION OF SWYXIT!

The following describes the configuration measures facilitating the Internet connection to SwyxServer and guaranteeing seamless running:

Configure connection via RemoteConnector

Configuring voice compression

26.1.3.1CONFIGURE CONNECTION VIA REMOTECONNECTOR

To enable the connection of SwyxIt! to SwyxServerviaRemoteConnector, enter the following information in the "Public server address" field since v12.20 and later:
The public endpoint (as FQDN or IP address) of the company network with corresponding ports over which the Authentication Service must be entered in the connection settings of SwyxIt!. For example, connect.server.net:9101

How to configure the connection via RemoteConnector

1 Install SwyxIt! on the Windows computer.
See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/installing_swyxit_$.

2 Start SwyxIt!, click on "Settings| Local Settings", and open the "Local Settings" tab.

3 Click on the "More" button.
The "RemoteConnector" dialog window will appear.

4 Select on of the three connection modes.
See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/define_connection_settings_$.

5 Enter the public IP address of the company network and the port via which the authentication service can be reached in the "Public server address:" field.

6 Confirm your information by clicking on the "OK" button.
The connection to SwyxServer via RemoteConnector is configured.

In SwyxON, the password for the generation of the Client certificate is not required.

26.1.3.2CONFIGURING VOICE COMPRESSION

A minimum bandwidth of 84kbit/s is required for an Internet connection.

After installing SwyxIt! on the Windows computer, it might be necessary to adjust voice compression to the Internet connection's minimum bandwidth. The highest audio quality should always be used, if a sufficient data transmission rate is available for SwyxIt!. If the transmission rate is lower than 84 kbit/s (during upload or download), then voice compression will have to be used.

How to select a voice codec for the Internet connection

1. Start SwyxIt!, click on "Settings| Local Settings", and open the "Local Settings" tab.
2. Select a bandwidth in the "voice codec" field that corresponds to the bandwidth of the connection.

As telephony clients on both sides use the same voice codec during a call, please verify the list of authorized codecs in the codec filter for the server. See *7.5.20 The "Default Codec Filter" Tab*, Page 113.

Please also verify that the respective codecs are authorized for the individual users. See *11.2.1.10 The "Codec Filter" Tab*, Page 176.

> Starting SwyxIt! and then playing and listening to announcements can take some time because the files needed in this case must be loaded from SwyxServer via the Internet connection.

> Saving recordings may take longer and use additional bandwidth, if the directory for the recorded calls are not locally stored on the user PC.

26.2 WAN CONNECTIONS

SwyxWare can connect two locations via a WAN (Wide Area Network). In this case, you'll need to differentiate between two basic scenarios:

- Small Office - Connection
  A SwyxServer is installed at the London location (A) (e. g., at the headquarters) and there is no SwyxServer at the Liverpool location (B), but rather a network that already has an IP connection to the London location (A) (headquarters).
  See *26.2.1 Small Office - Connection*, Page 388.
  In this case, it would also be possible to connect the branch office via a SIP gateway trunk.
  See *19 SIP Gateway Links*, Page 321.
- SwyxLink (Server Server Link)
  Both London (A) and Liverpool (B) have a network with one SwyxServer installed at each location.

A requirement for the WAN connection is an IP connection between London (A) and Liverpool (B). Such an IP connection can be implemented in different ways:

- connection to a Remote Access Server (RAS), as well as a demand-dial connection (dial-in) or a permanent connection (leased line) or
- connection via the Internet.

For information about connecting a branch office to SwyxWare at the headquarters via a VPN connection using SwyxConnect , please refer to *19 SIP Gateway Links*, Page 321.

26.2.1 SMALL OFFICE - CONNECTION

This section describes how to create a connection between networks in which SwyxWare is installed.

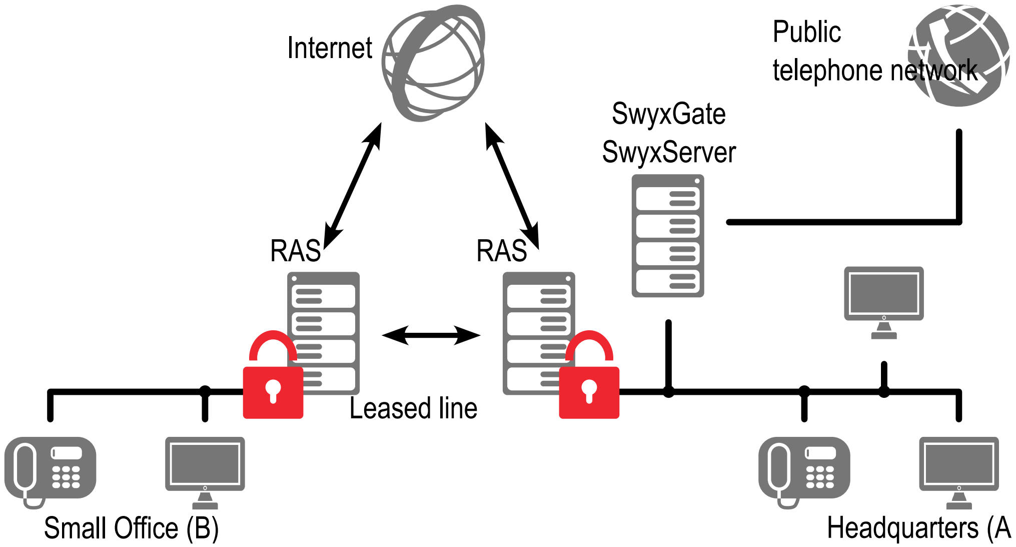


Fig. 26-3: Location Link for Small Office

You have a location at London (A) (headquarters) with a SwyxServer and an ISDN trunk (SwyxGate). A second location in Liverpool (B) (Small Office) is already connected to the Remote Access Server in London (A) using an IP connection, via either the Internet or a permanent line. In this case, the IP telephones or telephone clients connected at the Liverpool location (B) are managed at the London location (A) and external calls are made via the SwyxGate in London (A).

Configuration of SwyxIt!

SwyxIt! is configured for voice compression with low bandwidth according to the description found in 26Configuration of SwyxIt!, Page 387.

Configuration of SwyxPhone

The configuration for SwyxPhone is carried out in SwyxServer only.

How to configure SwyxPhone for a WAN connection

1 Open SwyxWare Administration and open the "Properties" dialog for the corresponding SwyxPhone user.

2 Go to "Settings|Administration..." and open the "SwyxPhone" tab.

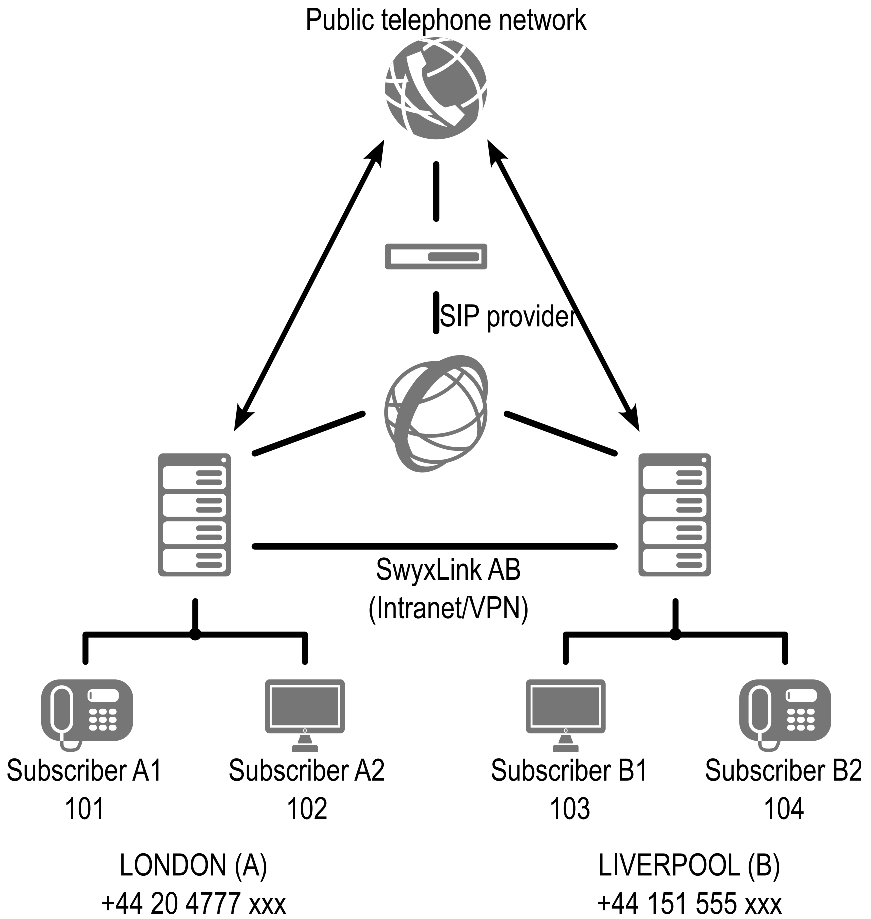
3 Then, in the "SwyxPhone" field, activate the option "Always compress voice data".

Data compression for SwyxPhone is a user property, which means if a different Small Office user logs in to SwyxPhone, then compression will also need to be configured for that user in SwyxServer.

Additional SIP devices within the Small Office also have to support compression.

26.3 LINKING OF TWO LOCATIONS (HEAD OFFICE AND BRANCH)

This scenario includes two locations, London (A) and Liverpool (B). An ISDN trunk to the local public network is installed at both locations. Furthermore, both locations have a SIP trunk to a SIP provider. The two locations are also connected directly via a SwyxLink trunk connection on a VPN.



When calls are made from London (A), the system should attempt to dial into the Liverpool location (B) and the local public network in Liverpool (C) first via the SwyxLink trunk connection. Thereafter, it should attempt to dial in via the SIP trunk and the public network (ISDN).

Internal calls should also be routed via the SwyxLink trunk connection.

Configuration at the London (A) Location

ISDN Trunk Settings

Parameter	
Name	ISDN London
Description	ISDN access in London
Public number	44151 4777 00 -99

SIP Trunk Settings

Parameter	
Name	SIP London
Description	SIP access in London
Public number	44151 888 00-99 (numbers assigned by provider)

SwyxLink Trunk AB settings

Parameter	
Name	SwyxLink AB
Description	Connects London with Liverpool
Managed	locally
Remote Server	SwyxServer B
Public number	44151 555 00 -99

Routing

- Calls from London to Liverpool (+44151*) should first be routed via the SwyxLink connection.
- If the SwyxLink connection is not available, then these calls should be routed via the SIP trunk (SIP London; priority 500).
- Only if these two routes fail should calls be routed via the public telephone network (ISDN London) to London.

Priority	Allowed	Phone number	Trunk Group
1000	Allowed	+44151*	SwyxLink AB
500	Allowed	+44151*	SIP London
100	Allowed	+44151*	ISDN London

Call Permissions

- It is permitted to route calls made via the SwyxLink trunk to London into the local public network in London (allowed; +[CC][AC]*). It is not permitted to make calls to other external numbers via this trunk (not allowed; +*). It is permitted to dial internal numbers in London (allowed; *).
- Users in London may make calls to any location in the United Kingdom (allowed; +44*).
- Calls made via the SIP trunk or ISDN trunk in London may be routed to any location (allowed; +*).

Profile	Allowed	Destination number	With public line access
SwyxLink-Trunk	Allowed	+[CC][AC]	All
SwyxLink-Trunk	Not allowed	+*	All
SwyxLink-Trunk	Allowed	*	All
User DO	Allowed	+44*	All
SIP-London	Allowed	+*	All
ISDN London	Allowed	+*	All

Configuration at the Liverpool (B) Location

ISDN Trunk Settings:

Parameter	
Name	ISDN Liverpool
Description	ISDN access in Liverpool
Public number	4430555 00-99

SIP Trunk Settings

Parameter	
Name	SIP Liverpool
Description	SIP access in Liverpool
Public number	44151 666 00-99 (numbers assigned by provider)

SwyxLink Trunk Connection Settings:

Parameter	
Name	SwyxLink AB
Description	Connects London with Liverpool
Managed	remotely
Remote Server	SwyxServer A
Public number	44204777000-999

Routing

- Calls from Liverpool to London (+4420*) should first be routed via the SwyxLink connection.
- If the SwyxLink connection is not available, then these calls should be routed via the SIP trunk (SIP Liverpool; priority 500).
- Only if these two routes fail should calls be routed via the public telephone network (ISDN Liverpool) to London.

Priority	Allowed	Phone number	Trunk Group
1000	Allowed	+4420*	SwyxLink AB
500	Allowed	+4420*	SIP Liverpool

Priority	Allowed	Phone number	Trunk Group
100	Allowed	+4420*	ISDN Liverpool

Call Permissions

- It is permitted to route calls made via the SwyxLink trunk to Liverpool into the local public network in Liverpool (allow; +44151*). It is not permitted to make calls to other external numbers via this trunk (not allowed; +*). It is permitted to dial internal numbers in Liverpool (allowed; *).
- Users in Liverpool may make calls to any location in the United Kingdom (allowed; +44*).
- Calls made via the SIP trunk or ISDN trunk in Liverpool may be routed to any location (allowed; +*).

Profile	Allowed	Destination number	With public line access
SwyxLink-Trunk	Allowed	+44151*	All
SwyxLink-Trunk	Not allowed	+*	All
SwyxLink-Trunk	Allowed	*	All
User B	Allowed	+44*	All
SIP Liverpool	Allowed	+4420*	All
ISDN Liverpool	Allowed	+4420*	All

26.4 INTERSITE PRESENCE

By setting up a SwyxLink it is possible to implement a connection between two or more SwyxServers. The configuration of this link allows status information (logged off, free, speaking) to be exchanged between users who are not logged on to the same SwyxServer. From version 2011 R2 onwards, the collaboration, video and instant messaging function (only SwyxIt! Messenger, not Swyx Messenger) is also possible across servers. Similarly, the users of one site will be displayed in the Global Phonebook of the other site, and vice versa.

A distinction is made between the following types of connection:

- Remote SwyxServer in the same organization
- Remote SwyxServer from another organization

See *17.4 Configuring a SwyxLink Trunk*, Page 296.

Below is a graphical representation of various scenarios for connecting multiple SwyxServers using different connection types.

26.4.1 CONNECTION OF THREE SWYXSERVERS WITHIN AN ORGANIZATION

In this example, three SwyxServers which are all within one organization (e.g. within a company) are each interconnected via a SwyxLink trunk. Within the configuration of the relevant trunk, the Intersite connection "Remote SwyxServer in the same organization" has been defined. In such a link-up there is typically a degree of mutual trust between the individual branches, allowing the status of colleagues to be exchanged among them. The administration in such a link-up is usually controlled centrally from one site for all connected systems.

This connection causes users of server A to be visible in the Global Phonebooks of server B and server C, and vice versa. If the administrator has created a unique number plan in advance for the organization, it can be defined that users are displayed in the Global Phonebook with only their internal numbers. If there is no unique number plan, it should be configured that a synchronization of the public numbers is carried out between the servers.

The visibility of the status information of the users or groups among each other, or the possibility of using functions such as Collaboration, Video and Instant Messaging (only SwyxIt! Messenger, not Swyx Messenger) across servers, can be configured from each server side via the relationships of the users and groups to each other. See *11.2.8 The "Properties..." Dialog: The "Relationships" Tab*, Page 202.

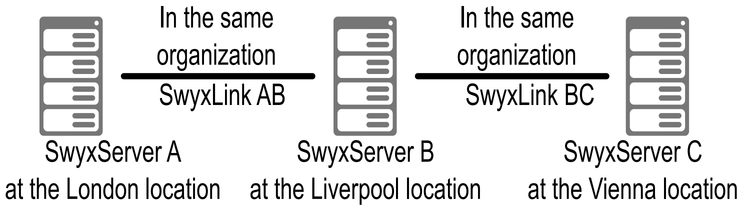

In the same organization
SwyxLink AB
In the same organization
SwyxLink BC
SwyxServer A at the London location
SwyxServer B at the Liverpool location
SwyxServer C at the Vienna location

Fig. 26-4: Intersite connection "Remote SwyxServer in the same organization"

Configuration at the London location (SwyxServer A)

SwyxLink Trunk AB settings

Parameter	
Name	SwyxLink AB
Description	Connects London with Liverpool
Managed	locally
Remote Server	SwyxServer B
Connection type	Remote SwyxServer in the same organization

Configuration at the Liverpool location (SwyxServer B)

SwyxLink Trunk AB settings

Parameter	
Name	SwyxLink AB
Description	connects Liverpool with London
Managed	remotely
Remote Server	SwyxServer A
Connection type	Remote SwyxServer in the same organization

SwyxLink Trunk BC settings

Parameter	
Name	SwyxLink BC
Description	connects Liverpool with Vienna
Managed	locally
Remote Server	SwyxServer C
Connection type	Remote SwyxServer in the same organization

Configuration at the Vienna location (SwyxServer C)

SwyxLink Trunk BC settings

Parameter	
Name	SwyxLink BC
Description	connects Vienna with Liverpool
Managed	remotely
Remote Server	SwyxServer B
Connection type	Remote SwyxServer in the same organization

26.4.2 CONNECTION BETWEEN TWO SWYXSERVERS OF DIFFERENT ORGANIZATIONS

In this scenario, the SwyxServer of Smith Ltd is connected to the SwyxServer of Jones Ltd by a SwyxLink trunk. As different companies are involved, the configuration of the SwyxLink trunk specifies the intersite connection "Remote SwyxServer from another organization". With this connection type, the administrator of a server can specify individual groups to be visible on the other server site. This is useful, e.g. if a group of employees in one company is collaborating with a group of employees in another company as a project team. With the help of the relationships within the group properties, the administrator can then specify precisely who should be signaled with the status information for the users in the group, and which users may use the collaboration, video and/or instant messaging functions.

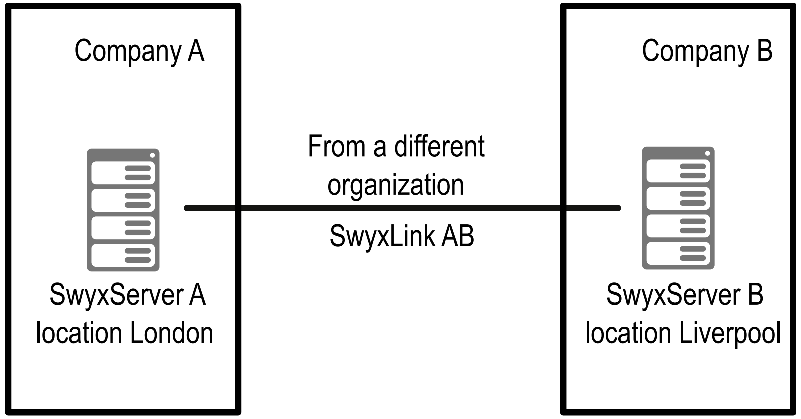


Fig. 26-5: Intersite connection "Remote SwyxServer from another organization"

Configuration at the London location (SwyxServer A)

SwyxLink Trunk AB settings

Parameter	
Name	SwyxLink AB
Description	Connects London with Liverpool
Managed	locally
Remote Server	SwyxServer B
Connection type	Remote SwyxServer from another organization
Select groups for publishing	Project team A

Configuration at the Liverpool location (SwyxServer B)

SwyxLink Trunk AB settings

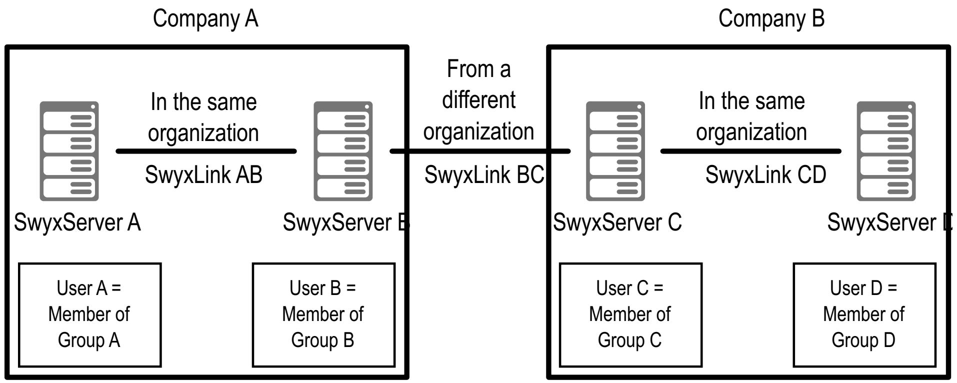
Parameter	
Name	SwyxLink AB
Description	connects Liverpool with London
Managed	remotely
Remote Server	SwyxServer A
Connection type	Remote SwyxServer from another organization
Select groups for publishing	Project team B

The type of connection within a SwyxLink trunk must always be identical on both servers (e.g. on server A and server B). I.e. if the configuration of the SwyxLink trunk AB on server A specifies the connection type "Remote SwyxServer in the same organization" , then on the remote server site, in this case server B, the SwyxLink trunk to server A must likewise be configured with the connection type "Remote SwyxServer in the same organization" .

26.5 DIFFERENT CONNECTION TYPES BETWEEN MULTIPLE SWYXSERVERS

In this scenario you see four SwyxServers, two in each case (servers A and B / servers C and D) being within one organization (here: Smith Ltd and Jones Ltd). Each pair is linked via a SwyxLink trunk with the connection type "In the same organization".

Between the organizations is a further SwyxLink trunk connection, in which the connection type is specified as "From another organization". For the example, a user is created on each server and assigned to a group.



As a result of this trunk configuration, the data of the following users is thus visible (or not visible) in the Global Phonebook of the other server sites:

On SwyxServer A,

- User A and User B are visible
- User C and User D are not visible

On SwyxServer B,

- User A, User B and User C are visible
- User D is not visible

On SwyxServer C,

- User B, User C and User D are visible
- User A is not visible

On SwyxServer D,

- User C and User D are visible
- User A and User B are not visible

Configuration on SwyxServer A

SwyxLink Trunk AB settings

Parameter	
Name	SwyxLink AB
Description	connects server A to server B
Managed	locally
Remote Server	Server B
Connection type	Remote SwyxServer in the same organization

Configuration on SwyxServer B

SwyxLink Trunk AB settings

Parameter	
Name	SwyxLink AB
Description	connects server B to server A
Managed	remotely
Remote Server	Server A
Connection type	Remote SwyxServer in the same organization

SwyxLink Trunk BC settings

Parameter	
Name	SwyxLink BC

Parameter	
Description	connects server B to server C
Managed	remotely
Remote Server	Server C
Connection type	Remote SwyxServer from another organization. Select Group B for publishing.
Relationship	Add the Group C from server C to the relationships of Group B on server B.

Configuration on SwyxServer C

SwyxLink Trunk BC settings

Parameter	
Name	SwyxLink BC
Description	connects server C to server B
Managed	locally
Remote Server	Server B
Connection type	Remote SwyxServer from another organization. Select Group C for publishing.
Relationship	Add the Group B from server B to the relationships of Group C on server C.

SwyxLink Trunk CD settings

Parameter	
Name	SwyxLink CD
Description	connects server C to server D
Managed	locally
Remote Server	Server D
Connection type	Remote SwyxServer in the same organization

Configuration on SwyxServer D

SwyxLink Trunk CD settings

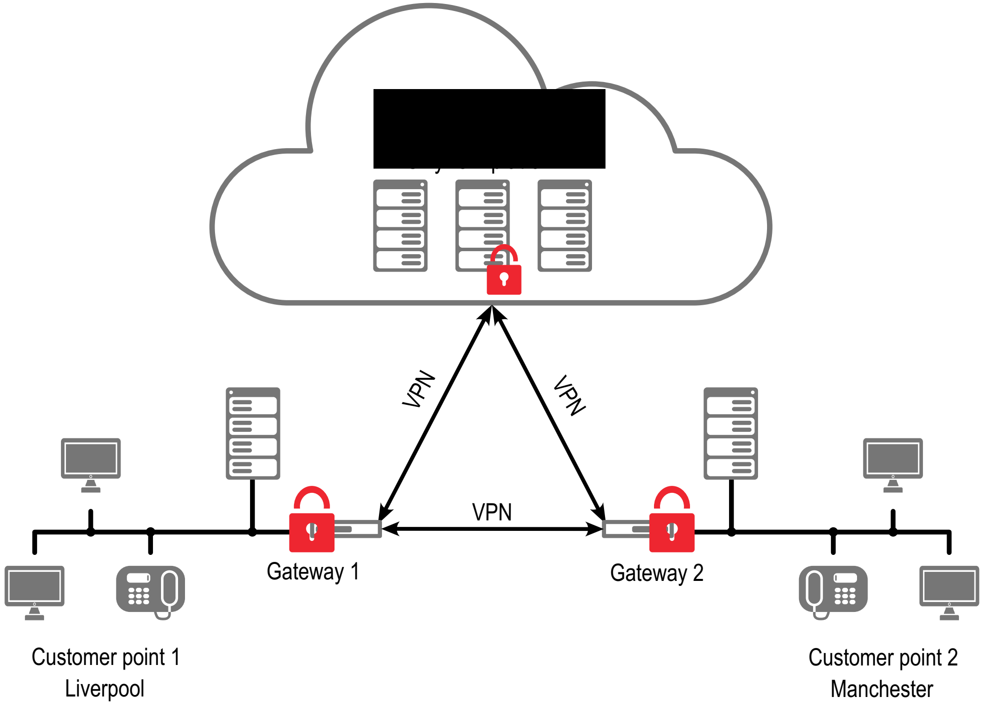
Parameter	
Name	SwyxLink CD
Description	connects server D to server C
Managed	remotely
Remote Server	Server C
Connection type	Remote SwyxServer in the same organization

26.6 CONNECTIONS BETWEEN LOCATIONS IN SWYXON

In SwyxON, SwyxServer is located in the computer center. All customer locations are connected to SwyxServer via VPN and carries out external telephone calls independent of other customer locations.

All locations are interconnected via VPN.

If telephone calls are made between the customer's locations, call signals and RTP data are exchanged directly between the locations.


[redacted]
VPN
VPN
VPN
Gateway 1
Gateway 2
Customer point 1
Liverpool
Customer point 2
Manchester

APP. A:CALL DETAIL RECORDS (CDR)

SwyxWare allows you to record information concerning connected calls, so-called "Call Detail Records", in a text file.

When saving and processing personal data, observe the respective applicable legal data protection regulations.

The following parameters can be configured:

- Activate / deactivate records (deactivated by default)
- Path and file name in which the record should be stored
- maximum file size.
- Display of external numbers

To define the parameters, go to the SwyxWare Administration and open "Properties" in the SwyxServer context menu. You can make all necessary settings on the "Call Detail Records" tab:

Here, you define the file and the directory where SwyxServer will save the Call Detail Records. If necessary, you can limit the file size (100 – 32000 Kbyte). If the maximum file size is exceeded, a new file with the same name plus a counter will be created and filled.

The CDR recorded in this way can be processed with a suitable billing software; in the simplest case Microsoft Excel, OpenOffice or StarOffice.

Write Call Detail Records in a database

Call Detail Records can also be written in a database instead of in a text file.

Single connection information cannot be deleted from the database. Please observe the respective applicable legal regulations. Please observe this in particular if you select the database as the memory location.

For further information see

Write Call Detail Records in a database service.swyx.net/hc/en-gb/articles/360000013819-Call-Detail-Records-in-eine-Datenbank-schreibe

(You may need to be logged in to view the content)

A.1 FILE FORMAT

The recorded ASCII text file contains a CDR for each line. Each CDR contains fields which are comma-separated and placed in quotation marks. +The first line is a header line containing comma-separated column names (in quotation marks).

Each line contains the following fields in the given order:

Attribute	Explanation
CallID	Identification for a call. Each call (each CDR) contains a unique number. This ID is communicated to SwyxIt!, which means that it can be used via the client SDK and it can also be queried in the call routing script. Format: String
Origination-Number	Caller's number In the case of internal calls, it is just the internal extension, for external calls it is the number that is signaled in the network. If the call goes through a trunk, the complete number will be entered in canonical format here (+44204777222). If no number is delivered from the network for an external call, this field will remain empty. Format: String
Origination-Name	Caller name Name of the Swyx client used to start the call, the user name or the name from the SwyxWare global phonebook. Format: String
CalledNumber	Called Number Number originally dialed by the caller. Format: String

Attribute	Explanation
CalledName	**Name of the person called** Name of the subscriber called, the user name or the name from the SwyxWare global phonebook. Format: String
DestinationNumber	**Destination Number** Number of the subscriber who picks up the call. This is the same as CalledNumber for calls which are not picked up. Format: String
DestinationName	**Destination Name** Name of the subscriber who picks up the call, the user name or the name from the SwyxWare global phonebook. CalledName will be used in the case of calls which are not picked up. Format: String
StartDate	**Start Date** Date on which SwyxServer receives the client's call. Format: dd.mm.yyyy
StartTime	**Start Time** Time at which SwyxServer receives the client's call. Format: hh:mm:ss
ScriptConnectDate	**Script start date** Date on which a script accepts the call. (Only for incoming calls.) Format: dd.mm.yyyy
ScriptConnectTime	**Script start time** Time at which a script takes the call. (For incoming calls only) Format: hh:mm:ss
DeliveredDate	**Delivery date** Date on which the call is delivered (e.g. by a ConnectTo in the script). (Only for incoming calls.) Format: dd.mm.yyyy
DeliveredTime	**Delivery time** Date on which the call is delivered (e.g. by a ConnectTo in the script). (For incoming calls only) Format: hh:mm:ss
ConnectDate	**Connection date** Date on which the call is picked up. Format: dd.mm.yyyy
ConnectTime	**Connection time** Time at which the call is picked up. Format: hh:mm:ss
EndDate	**End Date** Date on which the call is terminated. Format: dd.mm.yyyy
EndTime	**End Time** Time at which the call is terminated. Format: hh:mm:ss
Currency	**Currency of the charges** If AOC = '1'(Advice of charge) and if the public network supplies the charging units with currency, the currency is included here. If AOC = '1' and the public network only supplies the charging unit, the currency included here is the currency which was configured in the SwyxWare Administration. If AOC = '0', no charging information was delivered. Format: String See *A.3 The Charging Information*, Page 404.
Costs	**Cost of a call** If AOC = '1'(Advice of charge) and if the public network supplies the charging units with currency, the supplied value is included here. If AOC = '1' and the public network only supplies the charging units, the calculated value of the costs included here as configured in the SwyxWare Administration. If AOC = '0', no charging information was delivered. If no costs are incurred, this is shown as "0.00". Format: String
State	**State of the call** ● Initialized: Initial state when picking up the handset. ● Alerting: The call was ended while it was ringing at the destination number (DestinationNumber). ● Connected: The call was ended while it was connected to the destination number. ● ConnectedToScript: The call was ended while it was connected to a call routing script. ● OnHold: The call was ended while on hold. ● Transferred: The call was ended after it was transferred. Format: String

Attribute	Explanation
PublicAccessPrefix	**Public Line Access** For outgoing external calls: The public line access number dialed (optional). Format: String
LCRProvider	**LCR code** This field remains empty. Format: String
ProjectNumber	**Project Codes** The code for a project (optional). Format: String
AOC	**Charges information (Advice of Charge)** "1": The advice of charge information was taken from the network. '0'. The advice of charge information could not be taken from the network. Format: String
OriginationDevice	**Origin (Trunk)** This gives the origin of the call (Name of the trunk). Format: String
DestinationDevice	**Destination (trunk)** This gives the destination of the call (Name of the trunk). Format: String
TransferredByNumber	**Number of the transferor** Number of the subscriber who transferred the call. Format: String
TransferredByName	**Name of the transferor** Name of the subscriber who transferred the call. Format: String
TransferredCallID1	**ID of the first call** In the case of a call transfer, this is the CallID of the first CDR from which this CDR stems. Format: String
TransferredCallID2	**ID of the second call** In the case of a call transfer, this is the CallID of the second CDR from which this CDR stems. Format: String
TransferredToCallID	**ID of the transferred call** The CallID of the new CDR resulting from a call transfer. Format: String
TransferDate	**Date of transfer** Date on which the call is transferred. Format: dd.mm.yyyy
TransferTime	**Time of transfer** Time at which the call is transferred. Format: hh:mm:ss

Attribute	Explanation
Disconnect Reason	Reason for call termination ● Busy: Destination number is busy ● Reject: Destination rejects call ● NoAnswer: Destination does not pick up ● TooLate: A different device picked up the call ● UnknownNumber: The number called is unknown ● Unreachable: Destination cannot be reached ● DirectCallImpossible: A connection for a direct call is not possible (deactivated in the settings) ● DivertToCallerImpossible: A caller cannot divert a call to himself. ● NetworkCongestion: Network is overloaded ● BadFormatAddress: Format of the address is invalid ● ProceedWithDestinationScript: The call has been diverted to a call routing script of another subscriber ● CallRoutingFailed: Call routing failed (e.g. a call routing script could not be started) ● CallIgnored: The call has been ignored by the call routing script (e.g., when several ISDN devices are connected) ● PermissionDenied: Insufficient permission for this call ● CallDisconnected: Normal caller ● CallDeflected: The call was manually forwarded to another number or to the Voice Box without being answered ● IncompatibleDestination: Caller and destination are not compatible, e.g. different codecs. ● SecurityNegotiationFailed: Caller and destination have incompatible encryption settings, e.g. "Encryption mandatory" - "no encryption) ● NumberChanged: Destination number has been changed in PSTN ● NoChannelAvailable: No SwyxWare channel available ● OriginatorDisconnected: Caller ended the call ● CallTransferred: The call has been transferred. The call will be recorded further under the newly assigned TransferredToCallID. Format: String

A.2 EXAMPLES FOR CDR

The following examples are given to help you better understand CDRs. These are CDRs which are recorded after the call has been disconnected. To provide a better overview, only those CDR fields are listed, which help you to understand CDR recording.

For the calculation of the charges, see *A.3 The Charging Information*, Page 404.

A.2.1 CDR FOR A SIMPLE INTERNAL CALL

User A (number 123) calls user B (number 456). Before dialing the number, he dials *4711# to assign the call to a project. This results in the following CDR:

Attribute	Content
CallID	3
OriginationNumber	"+123"
OriginationName	"User A"
CalledNumber	"+456"
CalledName	"User B"
StartDate	"19.11.2012"
StartTime	"13.03:28"
DeliveredDate	"19.11.2012"
DeliveredTime	"13.03:24"
ConnectDate	"19.11.2012"
ConnectTime	"13.03:28"
EndDate	"19.11.2012"
EndTime	"13.03:48"
State	"Connected"
ProjectNumber	"+4711"
DisconnectReason	OriginatorDisconnected

A.2.2 CDR FOR AN EXTERNAL CALL

User A (number +44204777123) forwards an external call to John Jones (number +4420456789). SwyxServer uses the trunk "SwyxGate 1", to execute the call.

Attribute	Content
CallID	4
OriginationNumber	"+44204777123"
OriginationName	"User A"
CalledNumber	"+4420456789"
CalledName	"Jones, John"
StartDate	"19.11.2012"
StartTime	"13.03:28"
DeliveredDate	"19.11.2012"
DeliveredTime	"13.03:28"
ConnectDate	"19.11.2012"
ConnectTime	"13.03:28"
EndDate	"19.11.2012"
EndTime	"13.03:48"
State	"Connected"
PublicAccessPrefix	"+0"
DestinationDevice	"SwyxGate1"
DisconnectReason	CallDisconnected

The CalledName "Jones, Tom" comes from the global SwyxServer phonebook. The connection was terminated by the external subscriber (DisconnectReason = CallDisconnected).

A.2.3 CDR FOR A CALL WITH CALL ROUTING

User B has activated a call routing script. This script picks up a call, plays an announcement and transfers the call to an internal telephony client. If the call is not picked up there, the call will be transferred to the mobile telephone.

Attribute	Content
CallID	5
OriginationNumber	"+44204777123"
OriginationName	"User A"
CalledNumber	"+44204777456"
CalledName	"User B"
DestinationNumber	"+4416012345678"
DestinationName	""
StartDate	"19.11.2012"
StartTime	"13.03:28"
ScriptConnectDate	"19.11.2012"
ScriptConnectTime	"13.03:30"
DeliveredDate	"19.11.2012"
DeliveredTime	"13.03:55"
ConnectDate	"19.11.2012"
ConnectTime	"13.03:59"
EndDate	"19.11.2012"
EndTime	"13.05:09"
State	"Connected"
PublicAccessPrefix	"+0"
OriginationDevice	""
DestinationDevice	"SwyxGate1"

Attribute	Content
DisconnectReason	CallDisconnected

A.2.4 CDR FOR A TRANSFERRED CALL

User C (number +44204777101) calls user A (number +4416012345678) and puts this call on "Hold". User C then calls user B (+44521087654321) and speaks with him. User C then connects users A and B to one another. Due to the fact that user C initiated both calls, he will be charged for the costs for both calls. This results in three CDRs, which can all be used for cost calculation.

CDR 1 (Call from C to A)

Attribute	Content
CallID	3
OriginationNumber	"+44204777101"
OriginationName	"User C"
CalledNumber	"+4416012345678"
CalledName	"User A"
StartTime	"13.08:24"
ConnectTime	"13.08:45"
EndTime	"13.15:44"
Currency	"EUR"
Costs	"1.23"
State	"Transferred"
AOC	"1"
OriginationDevice	""
DestinationDevice	"SwyxGate1"
TransferredToCallID	8
TransferDate	"19.11.2012"
TransferTime	"13.10:06"
DisconnectReason	CallTransferred

CDR 2 (Call from C to B)

Attribute	Content
CallID	7
OriginationNumber	"+44204777101"
OriginationName	"User C"
CalledNumber	"+44521087654321"
CalledName	"User B"
StartTime	"13.09:34"
ConnectTime	"13.09:56"
EndTime	"13.03:48"
Currency	"EUR"
Costs	"4.33"
State	"Transferred"
AOC	"1"
OriginationDevice	""
DestinationDevice	"SwyxGate1"
TransferredToCallID	8
TransferDate	"19.11.2012"
TransferTime	"13:10:06"
DisconnectReason	CallTransferred

CDR 3 (Transferred Call; A Speaks to B)

Attribute	Content
CallID	8
OriginationNumber	"+4416012345678"
OriginationName	"User A"
CalledNumber	"+44521087654321"
CalledName	"User B"
StartTime	"13:10:06"
ConnectTime	"13:10:07"
EndTime	"13:15:44"
Currency	""
Costs	""
State	"Connected"
OriginationDevice	"SwyxGate1"
DestinationDevice	"SwyxGate1"
TransferredByNumber	"+101"
TransferredByName	"User C"
TransferredCallID1	3
TransferredCallID2	7

A.3 THE CHARGING INFORMATION

SwyxServer requires charging information in order to control the display of charges in the telephony client and in order to create the Call Detail Records. SwyxWare receives charging information from the public network via the ISDN channel from the "Advice of Charge" information element (IE). This section describes in detail how SwyxWare interprets charging information and how the charging information is transmitted to a sub-PBX or an ISDN device, which are switched after SwyxWare.

Furthermore, we will describe how charging information is transmitted via a SwyxLink trunk and how it is saved in the CDRs.

Charging Information via ISDN

Charging information can be transmitted by ISDN in various formats and at different times. SwyxWare uses this information, which occurs almost exclusively during practical application, during the connection (AOC-D) or at the end of the connection (AOC-E). There are different variations for both of the above variants: The transmission of charging units or the transmission of charges as currency units. The type of information that is transmitted depends on the provider and the existing line. For more detailed information on this, contact your ISDN provider.

"Advice of charge" in Charging Units

This type of charging information contains the number of charging units. The Deutsche Telekom generally uses this type of charge display. In order for the SwyxServer to be able to display the charges for a call in the telephony client or in the Call Detail Records, SwyxServer must know how expensive one charging unit is.

How to configure the value of the charging unit

1 Open the SwyxWare Administration.

2 Open the "SwyxServer | Properties" and switch to the "Charges" tab.

3 Set the value "Cost per charging unit".

Changes made to this value have no influence on the connections made in the past. The new value will be used when determining the charges for future connections.

Please note that the settings made in the administration are only valid for this type charging information. If the charges are transmitted in as currency units, these settings are ignored.

"Advice of charge" in Currency Units

This type of charging information contains the number of charging units, the value of a charging unit and the currency. Since this information is complete, SwyxServer ignores the configured charging unit value and the currency. Swiss Telecom generally sends this type of charging information.

Accuracy of the Charges

The accuracy of the charging information provided via ISDN depends on your provider.

Enreach cannot guarantee that the charges displayed match the costs charged by your provider. In addition, no provider will guarantee that the charging information provided via ISDN is 100% correct.

Charge information in sub-PBX or ISDN device on internal S_0/ S_{2m}-Bus

From SwyxWare version 4.0, fee information is also sent to the internal S_0/S_{2m}-Bus. This requires that the ISDN card be operated in NT mode (*D.1.2 SX2 in NT Mode*, Page 418). The SwyxServer then generally sends AOC-D information in currency units, regardless of how the charging information was signaled on the external ISDN line.

If a PBX or an ISDN device is in operation, which cannot interpret the AOCD information element, SwyxGate can be reconfigured so that it sends display information elements instead.

Charging Information via SwyxLink Trunk

SwyxServer also routes charging information to other locations via a SwyxLink trunk.

If user A1 at site A dials a number, which is transferred via a SwyxLink trunk to site B and an ISDN trunk_GB and from there into the PSTN, the charging information received by the ISDN trunk_GB will be sent via the SwyxLink trunk to user A1.

APP. B: AUDIOCODES TERMINAL ADAPTER

Connecting and operating "IP terminal adapters" for the operation of fax machines on the SwyxWare IP network.

We describe the configuration and updating of the AudioCodes terminal adapters MP-11x/FXS and MP-124/FXS with SIP firmware.

B.1 AUDIOCODES TERMINAL ADAPTER MP-11X OR MP-124 WITH SWYXWARE

The AudioCodes Terminal Adapter is a SIP terminal adapter (often referred to as a SIP FXS Gateway) for the connection of analog terminals (phone, fax machine). The AudioCodes company uses the term MP-11x to identify its FXS-type MP-112 (2 ports), MP-114 (4 ports) and MP-118 (8 ports) multiport adapters. The MP-124/FXS adapter has 24 ports. The functionality and configuration of this equipment is the same except for the different number of ports. MP-10x (MP-112, MP-114, MP-118) adapters use the same firmware but the MP-124 has its own firmware.

The configuration of the AudioCodes Terminal Adapter can take place via a web interface by entering the IP address as the web address.

This is how you determine the IP address of the AudioCodes Terminal Adapter

1. Connect the AudioCodes Terminal Adapter to the IP network.
   If DHCP is used (as delivered), the adapter has a new, associated IP address. You can find this e.g. in the log file of the DHCP server with the help of the MAC address, which is on the underside of the AudioCodes Terminal Adapter.
   If the AudioCodes Terminal Adapter is still in the state it was delivered in, i.e., it has not yet been used in an environment with DHCP and if you do not use DHCP, the adapter will have the IP address http://10.1.10.10.

How to change the DHCP setting

1. Open a web browser and enter the IP address of the AudioCodes Terminal Adapter as the web address.
   The Web configuration of the adapter and a window for entering a user name and password will appear.
2. Enter user name and password (default setting: Admin/Admin).
3. Open the page "Configuration | System | Application Settings | DHCP Settings".
4. In the field "Enable DHCP" you can change the DHCP setting (default: Enable).
5. Then save the changes by clicking "Submit" and "Burn", and restart the adapter. This should not be a soft reset via the web interface, but rather a cold start, e.g. by pressing the reset button on the back of the device.

When the equipment is delivered, the file "call_progress_germany.dat" is used for the country-specific ringtones. You can change this file for your own country-specific tones.

How to change ringtones

1. Open a Web browser and enter the IP address of the AudioCodes Terminal Adapter as the web address.
   The Web configuration of the adapter and a window for entering a user name and password will appear.
2. Enter the user name and password.
3. Select the page "Management | Software Update | Load Auxiliary Files".
4. Specify the ringtone file in the input field "Call Progress Tones file", or click on "Browse...".
5. Choose a *.dat file and click on "Load File".
   The file will be loaded on to the adapter.

6 Then save the change by clicking "Submit" and "Burn", and restart the adapter. This should not be a soft reset via the web interface, but rather a cold start, e.g. by pressing the reset button on the back of the device.

> The program DConvert.exe can be used to create another ringing tone file based on your settings. For more information please refer to the Audio-Codes Terminal Adapter home page (www.audiocodes.com)

B.2 UPDATE AUDIOCODES TERMINAL ADAPTER FOR SWYXWARE

If you are using an older version of the firmware (e.g. a version 4.80.38.002) or you have not purchased the AudioCodes Terminal Adapter from Enreach (or one of its partners), you need to use the firmware and configuration tested by Enreach.

You can obtain the files you will need from Support in a ZIP archive. When submitting your request, please indicate which AudioCodes Terminal Adapter you are using (MP-11x or MP-124). The ZIP archive contains the firmware (*.cmp), a preconfigured initialization file (*.ini) and a file for the German ringtones (call_progress_germany.dat).

The update and configuration procedures are described below.

The configuration uses an initialization file, which you should preferably customize to your circumstances before the firmware is updated.

> The initialization file is a text file split into two parts. The first part "1) User Parameters" contains the parameters that can be changed by the user. The second part "2) IpPbx Interoperability Parameters" contains the parameters that are required for interoperability with SwyxWare. These cannot be changed.

How to change the initialization file

1 Open the initialization file with an editor.

2 If you are not using a DHCP, change "DHCPEnable = 1" to "DHCPEnable = 0".

3 Change the IP address for "ProxyIp 0" by entering the SwyxServer's IP address.

4 You can change the numbers of the adapter's individual analog ports if you wish, in the parameters "TrunkGroup" (e.g. "TrunkGroup 0" has the number 201 for port 1). If your AudioCodes terminal adapter has more than 2 ports, remove the semi-colons at the beginning of the line.

5 You can change the authentication of the SIP registration for each port if you wish ("Authentication_0" parameter etc.).

6 Save the initialization file once you have made your changes.

How to update the firmware

1 Open a Web browser and enter the IP address of the AudioCodes Terminal Adapter as the web address.
The Web configuration of the adapter and a window for entering a user name and password will appear.

2 Enter the user name and password.

3 Start the Software Upgrade Wizard under "Device Actions" or "Maintenance | Software Update".

4 Click on "Start Software Upgrade". A separate window will open.

5 In "Load a CMP file from your computer to the device", click on "Browse...".

6 Select the *.cmp file.
The path to this file now appears in the assigned field.

7 Click on "Send file".
The file is loaded on to the adapter, and a display then shows whether the loading was successful.

8 Click on "Next", and load the previously customized initialization file (see *How to change the initialization file*, Page 407) on to the adapter.

9 In "Load an ini file from your computer to the device", click on "Browse...".

10 Select the *.ini initialization file. The path to this file now appears in the assigned field.

11 Click on "Send file". The file will be loadedon to the adapter. Then you can restart the adapter by clicking on "Reset".

Independently of updating the firmware, you can also load a changed initialization file on to the adapter as follows.

How to load the initialization file

1 Open a Web browser and enter the IP address of the AudioCodes Terminal Adapter as the web address.
The Web configuration of the adapter and a window for entering a user name and password will appear.

2 Enter the user name and password.

3 Select the page "Management | Software Update | Configuration File".

4 In "Send INI File to the device", click on "Browse...".

5 Select the *.ini initialization file.
The path to this file now appears in the assigned field.

6 Click on "Load INI File".
The file will be loadedon to the adapter.

7 Then save the changes by clicking "Submit" and "Burn", and restart the adapter.

APP. C:SWYXCONNECT 5000/8000

SwyxConnect 5000/8000 is structurally identical to the AudioCodes Mediant 500/800 and consists of a multifunctional media gateway to connect the PSTN with IP networks.

It has the following functions in conjunction with SwyxWare:

- SIP Gateway, so that calls can be set up from SwyxWare into the PSTN and vice versa
- Connection and integration of legacy PBX, or analog and ISDN devices with SwyxWare for migration scenarios
- Operation as independent SIP proxy in separated smaller locations with fallback function, in case the IP/VPN connection to the central location or SwyxServer fails

See the AudioCodes Mediant 500/800 manual for further technical details, user scenarios and functions.

C.1 SYSTEM REQUIREMENTS

- SwyxWare 2015 or newer
- AudioCodes Mediant Firmware v6.60A.245 or higher

C.2 OVERVIEW

The following chapter gives an overview on the technical concepts and components of SwyxConnect 5000/8000.

C.2.1 VARIANTS

Enreach offers SwyxConnect 5000/8000 in different configuration levels:

- Up to two ISDN PRI connections
- Up to 8 ISDN BRI connections
- Up to four FXS connections
- SAS support (License for operation as SIP proxy)

C.2.2 KEY CONCEPTS

This chapter summarizes the most important terms required for the configuration of SwyxConnect 5000/8000.

C.2.2.1 PROXY SET

The proxy set consists of up to five proxies, which are grouped in order to achieve higher availability. They can be used for load distribution or as backups for one another in case of breakdowns.

C.2.2.2 IP GROUP

An IP group is an entity which is formed in order to be assigned further definitions. It serves for logical structuring. You can, for example, assign proxy set IDs to IP groups, i.e. define, which proxies shall be used for which group. The IP group will then register with these proxies via SIP.

With IP groups, you can furthermore define, where calls shall be forwarded to (call routing rules). Calls can e.g. be defined as destinations of PSTN calls. Rules may also be defined, which use the IP group of the call to decide the destination.

C.2.2.3 TRUNK GROUP

A trunk group is a logical group of physical trunks and channels to the PSTN and/or to connected devices. It consists of one or more BRI, PRI or FXS connections. The physical trunk (BRI, PRI, FXS) must be assigned the numbers which are valid for it. The channels must also be assigned to the trunk.

A BRI trunk typically consists of two channels, a PRI trunk of 30 channels.

C.2.2.4 ACCOUNT TABLE

The account table is used to configure SIP accounts. If you want to use SwyxConnect 5000/8000 with SwyxWare, please create a SIP account for each PSTN trunk, i.e. every SIP gateway trunk configured in SwyxWare needs a SIP account onSwyxConnect with the same configuration data (username, password). This creates a one-to-one relationship between the PSTN trunks of SwyxConnect, the SIP accounts of SwyxConnect and any SIP gateway trunks of SwyxWare.

You can also use SwyxConnect for the connection of ISDN or analog telephones, which are each assigned to a SwyxWare user. In this case you configure a SIP account in the account table for each telephone, applying the same SIP login data of the SwyxWare user to which you want to assign the telephone.

C.2.2.5 CALL DIRECTIONS: IP-TO-TEL, TEL-TO-IP AND IP-TO-IP

IP-to-Tel calls are SIP calls which are forwarded from the IP network into the public telephony network. SIP calls which are forwarded to ISDN or analog phones locally connected to SwyxConnect 5000/8000, are also IP-to-Tel calls.
Calls which are forwarded from the PSTN (public switched telephone network) into the IP network via SIP are Tel-to-IP calls. The same applies to calls to the SIP-IP network from ISDN or analog phones connected to SwyxConnect 5000/8000.

IP-to-IP calls are calls that take place within the SIP network and do not proceed to the ISDN or analog network, e.g. a call from a SIP client to a proxy (and finally to another SIP client).

C.2.3 FUNCTIONAL UNITS OF SWYXCONNECT 5000/8000

SwyxConnect basically consists of two functional units (applications):

The first application is the gateway. The gateway provides the functionality to make ISDN and analog calls, and serves, at the same time, as a bridge into the SIP network. Thus, calls can be forwarded per SIP from the IP network to the ISDN or analog network, and the other way around. This function is comparable to the SwyxGate. The gateway application is always active.

The second application is the SAS application (Stand Alone Survivability). It can optionally be activated and must be separately licensed. The SAS application is comparable to a SIP proxy. Provided SwyxConnect is connected via IP to SwyxWare, the SAS application will act as a pure proxy, which transparently forwards all SIP messages between the SIP endpoints. This means that all additional functions used by SIP end devices with SwyxWare are retained (e.g. SIP subscribe for name key statuses, MWI for voice box display, etc.). If the IP route (e.g. the VPN route) fails between SwyxWare and SwyxConnect, the SAS Application takes over the transmission between the SIP terminals automatically, i.e.SwyxConnect it provides the complete PBX functionality and transmits calls between the PSTN gateway, the SIP terminals and the ISDN or analog phones, which are connected via SIP.

As SwyxConnect is separated into two functional units, two TCP/UDP ports have to be used (one port per application).

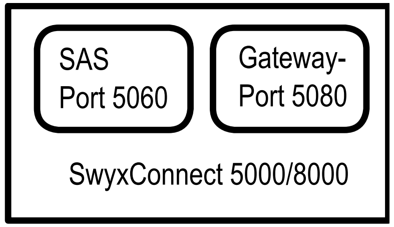


Fig. C-1: Structure of SwyxConnect 5000/8000:

C.2.4 MANIPULATIONS

SwyxConnect 5000/8000 can be used to manipulate CallControl messages in two ways:

Firstly, rules based on call direction can be defined using the web configuration, for processing numbers. However, this only applies to simple number manipulation, e.g. removing the "0" for public line access from the destination number of IP-to-Tel calls, as here the public line access number should not be forwarded into the PSTN.

The second possibility, using INI files or a Telnet or SSH access, is more extensive and allows parts of the (SIP) CallControl messages to be changed, removed or added. For SwyxConnect, this means that SIP message manipulations can be separately defined for the gateway for incoming or outgoing SIP calls. The rules themselves are grouped in Manipulation Sets. These Manipulation Sets in turn can be assigned to incoming calls only, or outgoing only.

Due to its complexity, Enreach recommends not using this option. However, it is still mentioned at this point, because the INI file templates with the basic configurations include such rules, and these are essential for successful operation of SwyxConnect on SwyxWare.

C.2.5 ROUTING

Routing offers the possibility of forwarding calls with the help of configurable criteria via specific destinations (e.g. IP groups or trunk groups). An example is the definition of a routing rule, which will forward a call into the PSTN via a particular ISDN trunk according to a particular sender (sender number or SIP gateway trunk).

C.2.6 COMBINATION OF MANIPULATION AND ROUTING

Manipulation and routing rules can be combined with one another. You can basically specify whether first the routing and then the manipulation rules are executed, or the converse. Furthermore, the order of the rules within these units can be defined by arranging the rules in the table accordingly (from top to bottom).

The manipulations configured with an INI file, which manipulate the (SIP) CallControl messages themselves, are an exception. These always take precedence over the routing rules.

While SwyxConnect is subdivided into its functional units (gateway and SAS application), the units are also listed according to the call flow of the CallControl messages (*Fig. C-2: Functionality of manipulation rules*, Page 411). This is a scenario, in which SAS is active, i.e. the IP route to SwyxWare is interrupted. An incoming call from the PSTN is transferred via the gateway application to the SAS application and from there in turn via the gateway application to an ISDN telephone, which is connected to a trunk of SwyxConnect.

The call directions are shown in the upper area of the illustration. The part of the call from the gateway application to the SAS application is a Tel-to-IP call. The SIP message received from the IP network to the SAS application belongs to the IP-to-IP category. The part of the call from the SAS application to the gateway application is an IP-to-Tel call.

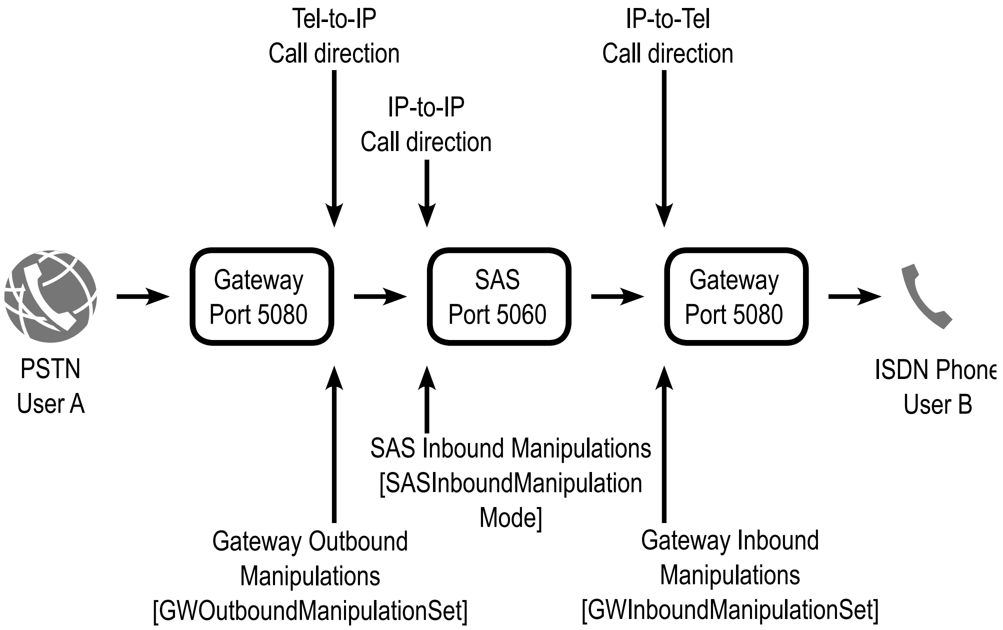


Fig. C-2: Functionality of manipulation rules

The lower area shows the points where the manipulation rules take effect. The gateway outbound manipulations are applied as a SIP message leaves the gateway in the direction IP. The gateway inbound manipulations are applied to the SIP messages that are sent to the gateway from the IP side. On the same principle, the SAS inbound manipulation rules are applied to the SIP messages that are transferred from the IP side to the SAS application.

C.2.7 DIGIT MAPPING

Digit Map pattern rules can be applied for Tel-to-IP calls, which use Overlap Dialing. In the scenarios described here, the aim is to delay the application of routing rules with the help of the digit map pattern, until the destination number has reached a length which ensures that the desired routing rule is applied. Up to 52 digit map pattern rules can be defined, separated from one another with a concatenation character ("|"). The string must not exceed 152 characters.

The following special characters may be used in the character string:

- [n-m] range of digits (letters are not allowed)
- . Any number of digits until the next notation
- x Any single digit
- T Wait for timeout when dialing

In the example "DigitMapping = 00[1-7]xxx|x.T", the section "00[1-7]xxx" collects numbers that start with 0 and then contain a digit between 1 and 7, followed by any three further digits. Always conclude a digit map with "x.T", in order to ensure that numbers which do not correspond to any formulated digit map pattern rule are still dialed. If the digit map is not concluded with "x.T", only numbers corresponding to a digit map pattern rule are accepted by SwyxConnect.

For further information, please see the AudioCodes Mediant 500/800 manual.

C.2.8 APPLICATION SCENARIOS

SwyxConnect 5000/8000 is used in conjunction with SwyxWare in two basic scenarios.
The first scenario uses SwyxConnect solely as a SIP gateway. In the second scenario, SwyxConnect is used in a separate location, so that it is used as a SIP gateway and also as a SIP proxy.

C.2.8.1 SWYXCONNECT 5000/8000 AS SIP GATEWAY

If SwyxConnect is used as a SIP gateway, all SwyxWare components and also SwyxConnect are usually in the same LAN of a company's central location (*Fig. C-3: SwyxConnect 5000/8000 as SIP Gateway*, Page 412).

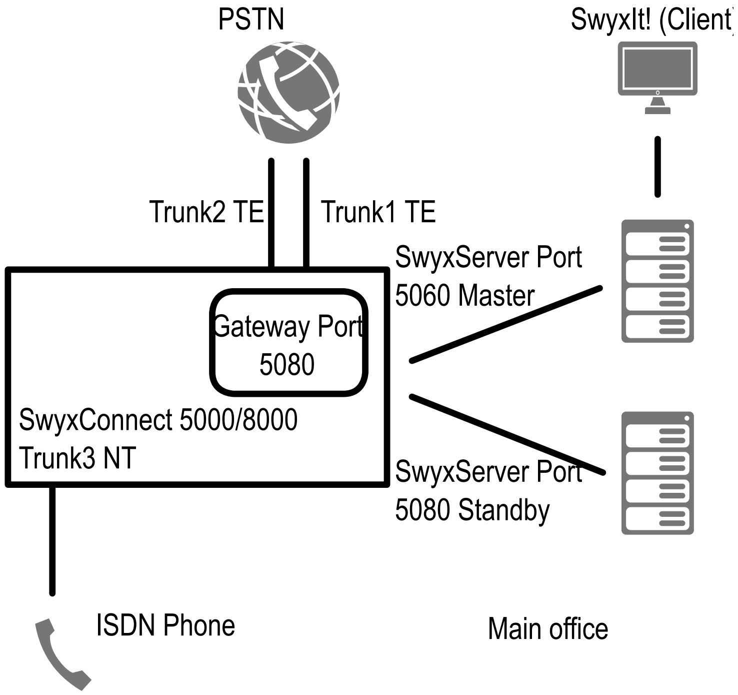


Fig. C-3: SwyxConnect 5000/8000 as SIP Gateway

In this example, SwyxConnect logs on to the currently active Swyx-Server of the master/ standby pair via SIP REGISTER. SwyxConnect automatically uses SIP OPTIONS to check, which SwyxServer is active. Only the active SwyxServer will reply to the SIP OPTIONS with 200 OK. After the active SwyxServer is detected, SwyxConnect logs in via SIP REGISTER to the SwyxServer. The master and the standby SwyxServer are configured within SwyxConnect in a proxy set.

SwyxConnect can be configured for various trunks. In the example, two trunks are connected to the PSTN in TE mode. These two trunks are configured in SwyxWare as two SIP gateway trunks.

The example further shows the login of an ISDN telephone via Trunk3. In SwyxWare, the ISDN phone is logged in as a SIP user. Thus, the SIP log-in data is stored in the SwyxConnect's Account Table for Trunk3, which is configured in NT mode. SwyxConnect will use this SIP log-in data to log in as a SIP SwyxWare user.

Please note that only the Gateway application is active on SwyxConnect. The SAS application is deactivated by default.

C.2.8.2 SWYXCONNECT 5000/8000 AS SIP GATEWAY WITH SAS

The operation of SwyxConnect with all configuration levels to SwyxWare, including master/ standby support and SAS, is described in the following example (see *Fig. C-4: SwyxConnect 5000/8000 as SIP Gateway with SAS*, Page 413).

SwyxWare is at the company's central location and is linked via IP (VPN) to a secondary location of the company. SwyxConnect Is located at this secondary location.

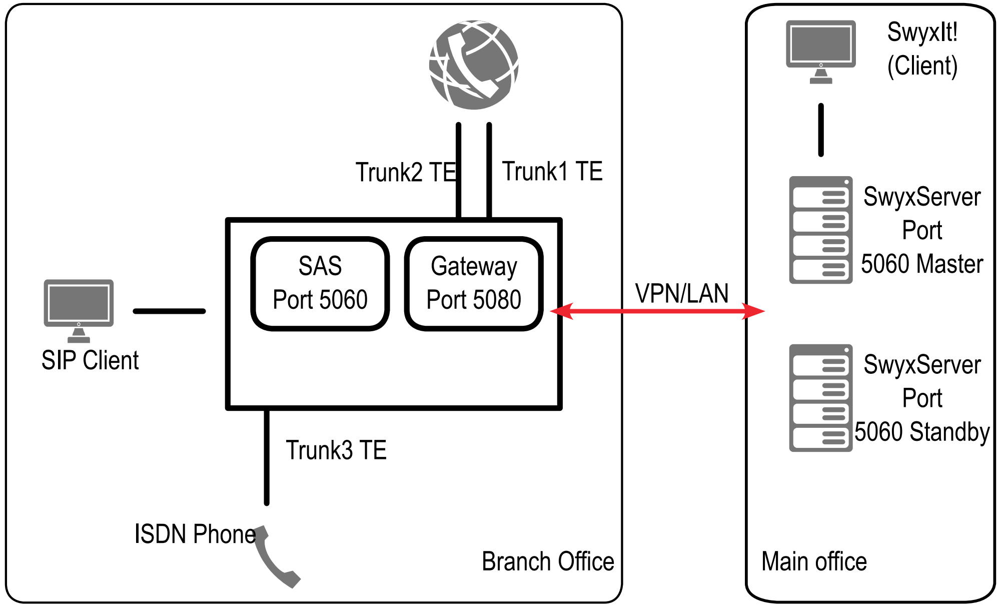


Fig. C-4: SwyxConnect 5000/8000 as SIP Gateway with SAS

Unlike the previous example, the SwyxConnect's SAS application is active here. The remaining configuration of SwyxConnect, concerning the trunks to the PSTN and the trunk for the connection of the ISDN phone, is unchanged.

Please note that in this example, the gateway application of SwyxConnect does not log in directly to SwyxWare with the trunks: all SIP messages are sent and received via the activated SAS application (proxy). Similarly, SIP clients must be configured such that they log in directly to SwyxConnect (SAS application (proxy)). In this configuration, the SAS application can process any transmissions independently, if the IP route between main and secondary location is interrupted. Thus, all SIP clients, which are logged on via SwyxConnect, can call each other directly, as well as any subscribers that are connected via an ISDN/ analog trunk. Calls can likewise be set up to the PSTN, and incoming calls picked up from the PSTN.

C.3 CONFIGURING SWYXCONNECT 5000/ 8000 FOR USE WITH SWYXWARE

Not all the necessary settings for using SwyxConnect with SwyxWare can be selected in the web configuration. Enreach provides some INI files as templates, which are necessary to make specific settings for SwyxConnect.

The following steps are required for startup:

- Preparing SwyxWare, i.e. creating SIP gateway trunks and SwyxWare users; setting up SwyxWare locations, if necessary
- Connection of SwyxConnect to the LAN and the PSTN
- Configuration and installation of the customized INI files on SwyxConnect

C.3.1 PREPARATION OF SWYXWARE

1 In the SwyxWare Administration, configure the SIP gateway trunks that you want to use.

2 When selecting the profile for the trunk group, choose the SwyxConnect profile matching your connection.

If you want to connect ISDN or analog telephones to SwyxConnect, configure for each of these a SwyxWare user with the option of logging in through SIP.

> Important: For the SIP user name and the SIP user ID, choose the extension that this user should be given. This is essential to ensure that when the SAS is used in the separated location, the user will still be able to call with the extension in emergency mode.

C.3.2 STARTUP OF SWYXCONNECT 5000/8000

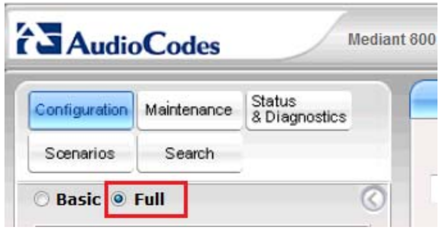
1 Connect SwyxConnect to the LAN. Ethernet connections are redundant and can be found on the front panel.

2 Connect SwyxConnect to the power supply. It will start, and after a little while it can be reached on the preset address IP 192.168.0.2 (subnet mask 255.255.225.0, gateway 192.168.0.1).

3 Start a web browser, deactivate the proxy settings and then enter "http://192.168.0.2.", to establish a link to SwyxConnect.

4 For the user name and password, enter "Admin" (factory setting). Entries are case-sensitive.

5 After log-on, set the view of the tree structure to "Full" so that all entries become visible (recommended after every login).
You can also find an entry in the tree structure using Search. Click on "Search", and enter all or part of the entry name.



6 Upload the new firmware and the file for the CallProgress tones to be used.

7 Start the update of the firmware by calling up the parent menu "Device Actions | Software Upgrade Wizard".
The wizard takes you through the individual steps to update the firmware.
Confirm the following dialogs and wait for SwyxConnect to restart.

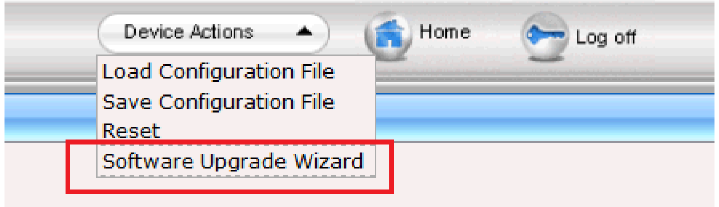


Fig. C-5: Device Actions

8 Finally the connection to the PSTN and/or to any ISDN or analog telephones has to be set up. Connect SwyxConnect to your NTBA and the terminal devices. The figures below show the pin configuration of the PRI and BRI modules of SwyxConnect.

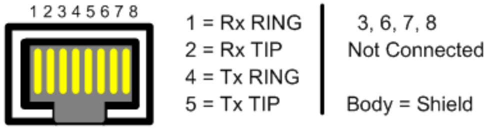


Fig. C-6: RJ-48c Pin configuration of an E1/T1 PRI plug-in module

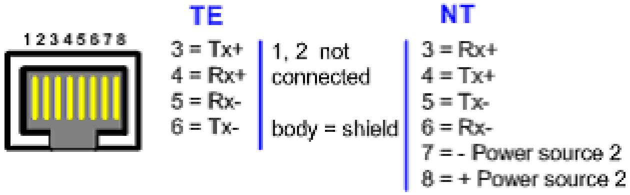


Fig. C-7: RJ-45 Pin configuration of a BRI plug-in module

C.3.3 CONFIGURATION AND INSTALLATION OF THE INI FILES

The INI files are divided into three sections. In the first part, you configure the parameters which are specific to the environment. These include e.g. the configuration of the ISDN trunks you use, and of the SIP accounts. In the second section, basic settings are selected SwyxConnect, which are necessary for the operation with SwyxWare. As a rule, no changes have to be made here. The optional SAS functionality is configured in the third part. In order to use this option, additional licenses are required.

C.3.3.1 CONFIGURATION OF THE INI FILE

Open the necessary INI file for your application case. Enreach recommends a text editor, which supports automatic syntax highlighting, e.g. Notepad++;

notepad-plus-plus.org

How to configure the gateway:

1 Under "[SYSTEM Params]" enter your NTP server and adjust the parameters for the automatic time change, if applicable.
As a rule, further settings are not necessary.

2 In the "[InterfaceTable]" table configure the SwyxConnect IP address as well as the subnet mask, gateway- and DNS server addresses.

3 In the "[ProxyIp]" section, configure the IP address of your IpPbxServer.
The following paragraphs describe the physical connection of SwyxConnect.

4 Activate the options appropriate for your usage.
If you configure an external line under "[TrunkGroup]", replace "NUMBER" with your subscriber number, e.g. 4777, for +44 20 4777 000 999.
If you operate a device on a port, replace "NUMBER" with the extension of the relevant subscriber, e.g.100, for +44 20 4777 100.
Under "[TrunkGroupSettings]", activate the lines according to the ports to be used.

5 Under "[Account]", specify the login data of your SIP gateway trunks and devices according to your SwyxWare configuration.

6 Under "[PSTN Params]", configure the protocol properties of the connections to be used.

7 With DIGITMAPPING numbers are configured which need special handling when dialing with Overlap Dialing, such as emergency numbers, exchange number or extensions of devices connected directly to SwyxConnect.

8 The section "[PstnPrefix]" determines the routing of SwyxConnect. If you operate SwyxConnect with external lines only, just put an asterisk for each port used and replace USERNAME corresponding to the account table above. If you also run devices, configure the extension to be routed on the corresponding trunk group.

> The routing starts as soon as a corresponding number is found in the table. Since the asterisk acts like a wildcard, this applies to every dialed number. This line should therefore always have the highest index in this table.
> If you want to use the SAS function with SwyxConnect, the routing should be configured in the corresponding section of the INI file.

9 If your ISDN connections support the "Clip No Screening" feature, activate the corresponding number of lines and configure USERNAME corresponding to the account table under "[SourceNumberMapIp2Tel]".

For the SAS configuration, you then execute the following steps:

10 In the section "[ProxyIP]", enter the IP address of SwyxConnect.

11 Activate the configuration for "[ProxyIp]", "[ProxySet]" and "[IpGroup]".

12 Under "[TrunkGroupSettings]" activate the parameters according to the ports configured under point 4.

13 Under "[Account]" activate the parameters according to the number of user accounts configured under point 5.

14 In the following sections numbers are configured. Replace the relevant wildcards here in order to adapt SwyxConnect to your environment.

15 The section "[PstnPrefix]" describes, as in point 7, the routing of SwyxConnect in gateway and SAS mode. Configure here the Routing Records for your external lines and connected devices, both for the local host IP address for SwyxConnect in SAS mode and for the operation of regular gateway.

16 Under "[SIP Params]", activate all parameters and configure the IP address of SwyxConnect once again.

17 The parameters described in the following sections must only be activated and generally need no further change. This is also valid for all parameters under "[SIP Params]", except SASDEFAULTGATEWAYIP. Configure the IP address of the SwyxConnect here.

C.3.3.2 INSTALLATION OF THE INI FILE

After you have customized the INI file, upload it to SwyxConnect. To do this, click on "Device Actions | Load Configuration File" (see *Fig. C-5: Device Actions*, Page 414).

After the installation of the INI file the web configuration of SwyxConnect is available via the configured IP address via HTTPS.

Passwords for account-specific data are not saved when an INI file is exported. So if you want to import a saved INI file on a device, you have to reconfigure the passwords in it first, or reset them afterwards in the web configuration.

APP. D:INTERNAL CONNECTIONS (BRI/PRI)

Configuration settings of SwyxWare in scenarios with other telecommunication systems

In an installation scenario with another telecommunication system, the following possibilities can be imagined:

- SwyxWare as master system
  In this case, an existing telecommunication system is operated as a sub-telecommunication system on SwyxWare, for example. SwyxWare manages the access to the public telephone network as well as to other networks. The sub-PBX is connected via ISDN to SwyxWare. The ISDN cards provided for this must be operated in NT mode in this case.
  See *D.1 SwyxWare as the main telecommunication system*, Page 417.
- SwyxWare as sub-telecommunication system
  In this case an existing telecommunication system is operated as master telecommunication system, for example. SwyxWare is connected to this as a sub-PBX. A prerequisite for this is the subsystem capability of the existing telecommunication system. The access to the public network is managed by the existing telecommunication system
  See *D.2 Connection of SwyxWare as Sub-telecommunication System on a Main Telecommunication System*, Page 420.
- SwyxWare in addition to an existing telecommunications system
  In this case SwyxWare is operated in addition to an existing telecommunications system. Both systems have access to the public telephone network and/or other networks.
  See *D.3 SwyxWare alongside another system with additional access to the public network*, Page 422.

D.1 SWYXWARE AS THE MAIN TELECOMMUNICATION SYSTEM

In this case, an existing telecommunication system is operated as a sub-telecommunication system on SwyxWare, for example. SwyxWare manages the access to the public telephone network as well as to other networks. The sub-PBX is connected via ISDN to SwyxWare. The ISDN cards provided for this must be operated in NT mode in this case.

D.1.1 OPERATING THE SX2 CARDS IN NT MODE

This chapter describes how to use the SX2 card in NT mode to connect ISDN devices and telecommunication systems to SwyxWare. These descriptions include the hardware requirements, any restrictions of the supported devices and the required configuration options of the SX2 cards and SwyxWare.

Supported devices on the Basic Rate Interface (BRI)

The SX2 QuadBRI can be used in NT mode. Multiple-subscriber lines and direct-dialing-in lines will be supported. Telecommunication systems with Basic Rate Interface, terminal adapters for transferring the ISDN interface to an analog line or ISDN phones can be connected to the cards. When using the SX2 QuadBRI a connection to up to 4 Basic Rate Interfaces of a telecommunication system is supported at the same time.

> Only ISDN phones with a separate power supply such as cordless phones can be connected to the ISDN cards. Simple ISDN phones which can be connected to the power supply only via the ISDN interface can not be connected.

It is also possible with the help of "BRI-BUS Power-Adapter to feed power to the BRI-bus (EXSG10001)" to apply a current to the BRI bus and thus to supply terminal devices. The computers power supply (mains) is used for this.

Supported devices on the Primary Rate Interface (PRI)

The use of the SX2 SinglePRI or SX2 DualPRI in NT mode is supported by the driver software of the card. A direct dialing-in telecommunication system with Primary Rate Interface can be connected to the ISDN card.

D.1.2 SX2 IN NT MODE

To use the NT mode, you must have a SwyxWare installation and a SwyxWare Administration. SwyxServer and SwyxGate must be ready for operation.

In order to operate the SX2 card in NT mode, the card must be appropriately prepared before it is installed in the computer. See *15.2.1 Preparation of the SX2 QuadBRI before insertion*, Page 247 or *15.2.3 Preparation of the SX2 SinglePRI*, Page 256

You do not need a special connection cable to operate SX2 cards in NT mode.

Configuring the SX2 cards for NT mode

The NT mode of the SX2 card is set in the driver according to the descriptions under *This is how you modify the ISDN card driver configuration*, Page 265. Here you have to select the NT mode on the "Connection" tab in step **(4)**. If necessary, repeat this setting for all lines of the SX2 card which can be used by the telecommunication system.

If the line is configured as a SX2 QuadBRI, the LED, which is associated with this line, will blink. This simplifies the identification when operating several SX2 QuadBRI cards.

D.1.3 OPERATION OF SEVERAL SX2 CARDS IN ONE COMPUTER

It is possible to operate several ISDN cards in one computer. On performance grounds, we recommend operating a maximum of 76 ISDN channels from one computer. Combinations of different SX2 cards are also possible; a maximum of four logical cards, for example:

- four SX2 QuadBRI
- two SX2 DualPRI (one SX2 DualPRI is equivalent to two "logical" cards)
- two SX2 SinglePRI and two SX2 QuadBRI
- one SX2 DualPRI and two SX2 QuadBRI

Synchronizing the SX2 cards

If there are several SX2 cards in one computer, three cases can be differentiated:

- All cards are directly connected to the public line (TE mode)
  In this case all cards receive the same pulse from the public line. There is no need to synchronize the cards.
- All cards operate internal lines (NT mode)
  If all cards are operated in NT mode, synchronization is recommended if a call is made via two different ISDN cards.
- Mixed operation of cards in TE mode and in NT mode
  If a call which is e.g. coming via an ISDN card from the public ISDN, is forwarded via a second card in NT mode e.g to a sub-PBX, the two cards should be synchronized. That is, the card in NT mode gets its pulse from the card that is connected to the public line.

For synchronizing two SX2 cards, you need a special cable: "Synchronisation Cable EXSG 10002".

This is how you synchronize two SX2 cards

1. The two cards must be connected to each other with the Synchronisation Cable EXSG 10002.

   The SX2 cards are in front of you with the PCI plug strip facing down and the ISDN connections to the left. Regardless of the type of ISDN card, you will then find two PCM plug strips in the upper right corner. The upper plug strip is labeled "OUT", the lower one "IN".

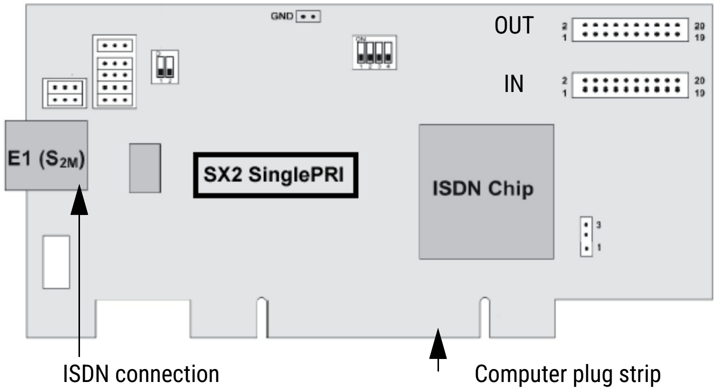


Fig. D-1: Schematic representation of SX2 SinglePRI

2. Now connect the "OUT" plug strip of the card that will be operated in TE mode (master), to the "IN" plug strip of the card that is to be operated in NT mode.
3. Insert these connected cards into the computer (*15.2.5 Insertion of the ISDN Card*, Page 263).
4. If no driver has been installed for the SX2 cards, it can be installed after this insertion (*15.2.5 Insertion of the ISDN Card*, Page 263).
5. Next, start the configuration of the driver in computer management (*15.2.7 Configuration of the ISDN Card*, Page 265).

   Enter the appropriate settings under "Properties".
6. Select "ISDN Parameters" on the "Advanced" tab.
7. In the tree structure, highlight the ISDN controller of the card that will be operated in NT mode.

   For details of how to identify the ISDN controller, please refer to *The "ISDN Ports" Tab*, Page 274.

   In the information field "Connected to:", it should now be indicated that a PCM cable has been connected to the card.

   In the field "Clock source for lines in NT mode", activate the option "Obtain clocking from other board connected via PCM bus".
8. In the tree structure, highlight the ISDN controller of the card that will be operated in TE mode (master).

   Here, the option "Derive clock from line in TE-mode or use on-board clock generation" must be activated in the field "Clock source for lines in NT mode".

> If you want to operate multiple cards in NT mode and synchronize them with a card that is connected to the public line in TE mode, you can feed through the pulse from the public line with further synchronization cables. To do this, connect the "OUT" plug strip of a previously synchronized card (NT mode) to the "IN" plug strip of a further card in NT mode, and so on.

D.1.4 CONNECTING A SUB-TELECOMMUNICATION SYSTEM (SUB-PBX) TO SWYXWARE

In order to continue to use analog equipment, such as existing fax devices or DECT telephones, these devices can be operated together with SwyxWare in a sub-PBX (sub-telecommunication system) environment.

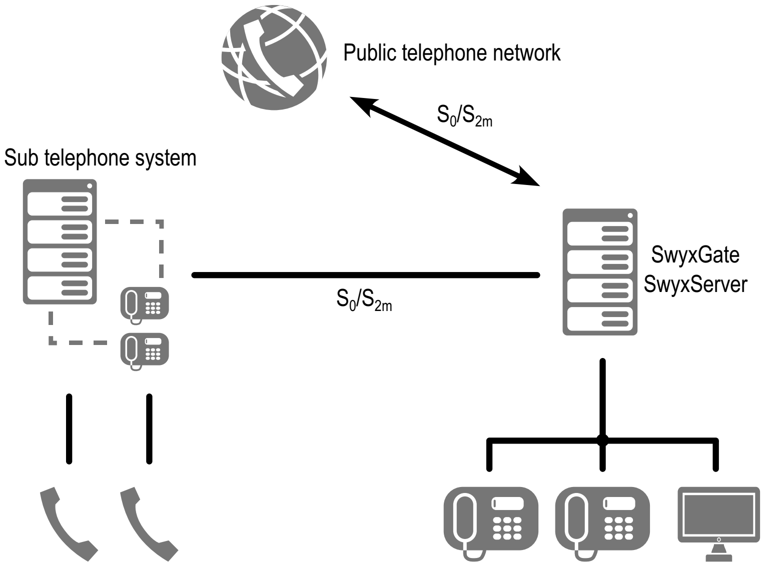


Fig. D-2: Connection of a Sub-PBX to the Internal PRI

In this case, an additional SwyxGate is installed or an existing one is used and the sub-PBX (sub-telecommunication system) is connected to this SwyxGate via a BRI/PRI connection.

Requirements

One or more lines must be available in the SX2 card for the connection of the sub-PBX.

The line which is available in the SX2 card for the internal connection must be configured in NT mode (*D.1.1 Operating the SX2 cards in NT Mode*, Page 417).

D.1.5 CONFIGURATION OF THE ISDN TRUNK GROUP AND ISDN TRUNKS (SWYXGATE LINES)

To connect a sub-PBX to SwyxServer, a corresponding ISDN trunk group (SwyxGate lines) must be configured.

How to configure the ISDN trunk group and trunks to the sub-PBX

1. Create an ISDN trunk group (*This is how you create an ISDN trunk group*, Page 265).
2. In the context menu, select "Properties".
3. On the "Profile" tab, select the profile "Internal Lines".
   The number format is set according to the default setting.
4. Leave the public line access blank. In this case SwyxWare is the superior telecommunication system.
5. If other number ranges are used in the range of the sub-PBX, configure the number replacement accordingly.
   See *10 Numbers and Number Mappings*, Page 146.
6. On the "Routes" tab, specify which calls from SwyxWare will be forwarded to the sub-PBX.
7. On the "Rights" tab, define the rights of the calls that are made from this sub-PBX into SwyxWare, e.g. whether these may be forwarded to the public telephone network.
8. Select the location of the sub-PBX on the "Location" tab.
9. End the configuration of the ISDN trunk group with "OK".
10. Next, set up one or more ISDN trunks belonging to this trunk group. You can allow only incoming or only outgoings calls for these, for example.

If you configure a spontaneous public line access for the sub-PBX (sub-telecommunication system), the lines within the sub-PBX will behave as if they were directly operated on SwyxWare.

D.2 CONNECTION OF SWYXWARE AS SUB-TELECOMMUNICATION SYSTEM ON A MAIN TELECOMMUNICATION SYSTEM

SwyxWare can also be implemented as a sub-telecommunication system. An existing sub-telecommunication system is expanded but remains the main telecommunication system.

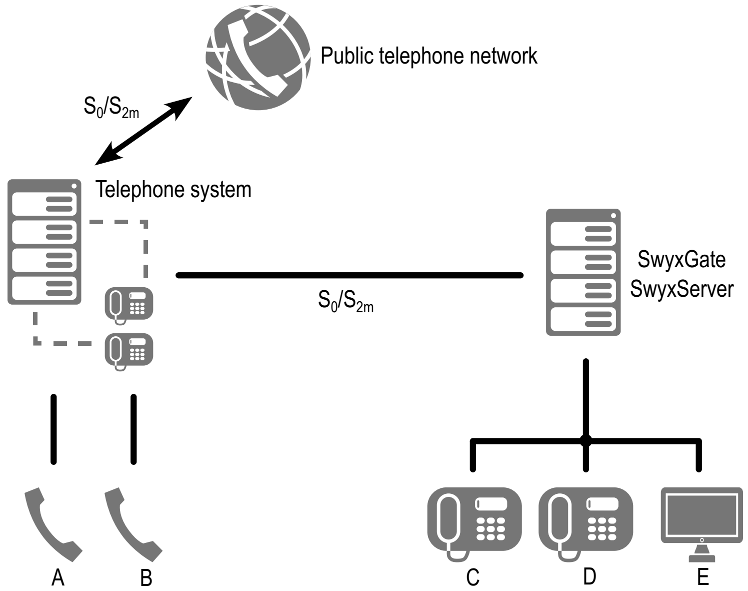


Fig. D-3: SwyxWare as sub-telecommunication system

In this case, the SX2 card is connected with the BRI/PRI connection of the main telecommunication system instead of with the PSTN.

Requirements

In the main telecommunication system, there must be an available BRI/PRI for the SwyxWare connection. In the SX2 card, the appropriate BRI/PRI must be available for the connection to the main telecommunication system.

The SX2 card that is used for the connection to the main telecommunication system must be configured in TE mode, i.e. as for the connection to the PSTN.

D.2.1 CONFIGURATION OF THE ISDN TRUNK GROUP AND TRUNKS

In SwyxServer the ISDN trunk group and the trunks must be appropriately configured for the access to the superior system.

How to configure the ISDN trunk group and trunks to the superior system

1. Create an ISDN trunk group (*This is how you create an ISDN trunk group*, Page 265).
2. In the context menu, select "Properties".
3. On the "Profile" tab, select the profile "Internal Lines".
   The number format is set according to the default setting.
4. The public line access of the PBX is the digit or sequence of digits that must be dialed within the main telecommunication system to gain access to an external line. Ask the main telecommunication system administrator about this.
5. If other number ranges are used in the range of the sub-PBX, configure the number replacement accordingly.
   See *10 Numbers and Number Mappings*, Page 146.
6. On the "Routing Records" tab, specify which calls from SwyxWare will be forwarded to the superior system.
7. On the "Rights" tab, define the rights of the calls that are made from this system into SwyxWare.
8. Select the location of the sub-PBX on the "Location" tab.
9. End the configuration of the ISDN trunk group with "OK".
10. Next, set up one or more ISDN trunks belonging to this trunk group. You can allow only incoming or only outgoings calls for these, for example.

Please make certain that the numbers assigned to users are within the range that you have configured in the main telecommunication system for SwyxWare. This should especially be checked when new numbers are allocated by the administrator.

D.3 SWYXWARE ALONGSIDE ANOTHER SYSTEM WITH ADDITIONAL ACCESS TO THE PUBLIC NETWORK

For a SwyxWare installed as a sub-telecommunication system, you can also provide a separate direct access to the public network or to other networks such as a SIP link or a SwyxLink.

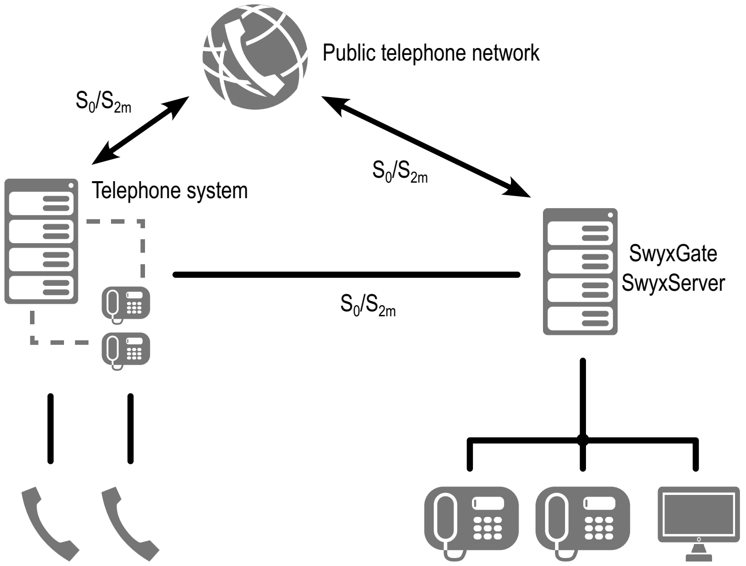


Fig. D-4: SwyxWare as a Sub-Telecommunication System with its own Access to PSTN

The lines necessary for this, e.g. from an additional SX2 card, must then be connected to the public telephone network and configured appropriately for the direct connection to the PSTN (*15.2.6 Installation of the software for the ISDN card*, Page 264).

In this scenario, various ISDN trunk groups are set up:

- ISDN trunk group(s) for access to the other telecommunication system
- ISDN trunk group(s) for access to the public network
- further trunk groups (e.g. SIP or SwyxLink) for access to other networks

The forwarding table determines how calls are forwarded in such a scenario (*14 Routing*, Page 239).

Please ensure that the permissions with which calls are forwarded are carefully configured.

D.4 INSTALLATION OF A GATEWAY WITH SX2 DUALPRI V2

In an environment with another PBX (e.g. a fallback SwyxServer), it is possible to forward the exchange connection directly to a PBX if necessary. The SX2 DualPRI V2 has an additional relay, enabling the calls to be forwarded directly even if there is a breakdown.

So long as the relay is activated, i.e. the software (SwyxGate, SwyxServer) is active, the connected PBX is treated as a sub-telecommunication system. If the relay is released, e.g. because

- there is a power failure,
- the service SwyxGate is stopped, e.g. directly by the administrator.

then the connected PBX is linked directly to the external line.

> *Example:*
>
> *The SX2 DualPRI V2 is configured so that one part (a controller, equivalent to a PRI) is directly connected in TE mode to the external line and the other part forwards the calls in NT mode to a sub-PBX (e.g. a fallback SwyxServer). If the computer now breaks down, the opening of the relay causes the external line to be connected through directly to the PBX.*

Preparation of the SX2 DualPRI V2 before insertion

Before the card is inserted, a jumper is set to establish whether the relay should be used on this card, see , Page 253.

This is how you check the relay status in the card driver

1. Start the configuration of the driver in computer management (*15.2.7 Configuration of the ISDN Card*, Page 265).
2. The relay function must be allowed for one of the two ISDN Controllers.
   On the "Advanced" tab, select the entry "ISDN Parameter".
   The status of the relay function is indicated in the information field "Standby Information:".
   "Standby relay status: enabled / disabled".

If the status is "disabled" for both ISDN controllers, the relay function is deactivated. There will be no through-connection of the external line to the sub-PBX if SwyxWare is disabled.

Clocking in the Standby Configuration

In a Standby configuration, one of the ISDN Controllers of SX2 DualPRI V2 is configured in TE mode, the other one in NT mode. The ISDN controller in NT mode must be configured in a way that in the card driver configuration on the "ISDN Parameters" tab the option "Obtain clocking from other board connected via PCM bus" is activated (can be activated in NT mode only!). This ensures that the ISDN controller is synchronous to the ISDN controller in TE mode.

APP. E:TOOLS & TRACES

Tools to support the analysis of installation problems

For current information regarding this topic, please consult the articles in our Knowledgebase:

service.swyx.net/hc/en-gb

When saving and processing personal data, observe the respective applicable legal data protection regulations.

E.1 POWERSHELL SUPPORT

With the help of SwyxWare PowerShell mode, administrative processes can be run in an automated manner via command lines or with PowerShell scripts.

Over 100 Cmdlets help to run both simple administrative processes as well as complex administration tasks.

It is recommended to have general knowledge of the use of Windows PowerShell before using SwyxWare PowerShell.

By running PowerShell commands with administrator rights, you obtain full control over SwyxWare, which can have grave effects on SwyxWare configuration.
Test your commands and scripts and use the parameter "-whatif" in order to check the potential consequences of a command.

When all or many users, groups or trunks are processed in an operation, then the system load on the SwyxServer may reach levels that are too high. Run the corresponding commands or scripts only within a period of low server demand.

The PowerShell module for SwyxWare supports Windows PowerShell for V3.0 and higher, and can only be used with SwyxWare V2013R3 and higher.

Installation

The PowerShell module comes default with SwyxWare installed.

See *5.5 Installation of the SwyxWare Administration*, Page 64.

Starting

You can run the PowerShell module via the corresponding symbol in the start menu entry. In this case, Windows PowerShell is launched with the SwyxWare module loaded.

Alternatively, you can open Windows PowerShell directly and reload with the command "Import-Module IpPbx".

Help on module and list of Cmdlets

You can access further information on working with the module using the command "Get-Help about_IpPbx_Module".

You can open a list of all Cmdlets available with the command: "Get-Command -Module IpPbx".

Here, you can run individual Cmdlets with the parameter "?", which every Cmdlet supports.

You can obtain detailed help on the individual Cmdlets with "Get-Help -full <CmdletName>".

E.2 ACTIVE DIRECTORY EXTENSION

This function is not available for SwyxON.

SwyxWare users can be managed in the Windows user administration. There you can

- when creating a new Windows domain user (Active Directory user and computer), directly create an associated SwyxWare user and assign him basic SwyxWare parameters such as name and number
- assign corresponding SwyxWare users to Windows users that already exist
- change basic SwyxWare parameters in the Windows user administration
- when deleting a Windows user account, remove the associated SwyxWare user directly

You will find details on the use of the Active Directory extension in *11.6 Configure users in the Windows user administration*, Page 209.

Installation of the Active Directory extension

The Active Directory extension must be registered in the Windows user administration. To do this, start the SwyxWare-Configuration Wizards (*5.4.2 Configuring SwyxWare*, Page 54) or use the program IpPbxAdExtConfig.exe in the SwyxWare program directory to perform the registration in the Active Directory. Next, for display of the relevant SwyxWare interface in the Active Directory, install the 'AD Integration' of the SwyxWare Administration on the computer from which you call the Active Directory user administration.

Removal of the Active Directory extension

When SwyxWare is uninstalled, the registration of the Active Directory extension is not removed from the Active Directory. Using IpPbxAdExtConfig.exe, which you will find on the SwyxWare DVD under "Tools\AD Extension", it is possible to remove the extensions. To do this, start a command line with domain administrator rights and enter

```
IpPbxAdExtConfig /u
```

Parameter /v is used to display the current status of registration, and /r to register the extension again.

E.3 USER IMPORT ASSISTANT

User data can be imported from an Excel table or a directory service into the SwyxWare database. All directory services which grant LDAP access are supported. Tests were done with Microsoft Active Directory and SunOne Directory Server.

You can find the program 'IPPbxUserImport' on the SwyxWare DVD in the directory 'tools\SwyxUserImportAssistant'.

Copy the directory 'tools\SwyxUserImportAssistant' from the SwyxWare DVD locally on to the computer on which the SwyxWare Administration is installed.

You can use the following functions:

- Import of users (name and phone number)
- Detection of location from the phone number
- Email notification to new SwyxWare users

The program IPPbxUserImport can only create users if it is started by a user who has at least user administrator rights. If you want to import from an LDAP directory, the current Windows user account must be a member of this domain.

How to import user data

1. Copy the directory 'tools\SwyxUserImportAssistant' from the SwyxWare DVD locally on to the computer on which the SwyxWare Administration is installed.
2. Start IPPbxUserImport.

3 Authenticate the access to the SwyxServer either under the current Windows user account or with user name and password. The user account must have at least SwyxWare user administrator rights.

4 Specify the source from which the user data is imported:
Directory service

- Connection to LDAP directory
  Specify the path to the LDAP Directory Server whose user data you want to import (e.g. LDAP://DC=company,DC=net). If the current Windows user account is not sufficient for the LDAP access, activate the checkbox and enter here a name (e.g. "CN=Jones\, Tom,OU=Development,OU=Users,OU=London,DC=company,DC=net") and the corresponding password.
  If the computer is a member of an Active Directory domain and the current Windows user account is a member of this domain, a link to this own Active Directory is automatically suggested.
  You can select or delete existing profiles of previous imports from the selection list.
  You can check with 'Test' whether the entered authentication parameters are sufficient.
  Click on "Next>".
- Selection of the organizational unit
  Select in the tree structure the organizational units (OU) whose users you want to import.
  You can choose here how the SwyxWare user name is generated:
  - from the Windows user account,
  - from the full name,
  - from the last name or
  - last name, first name.
  If you want to import only users who already have a phone number in the LDAP directory, activate the corresponding option.

Excel file

- Excel Import
  Specify the XLS file, and the sheet with the user data to be imported. Assign the column names in the Excel table to the corresponding SwyxWare data (user name, external number and email address, optionally Windows user account and description).

Click on "Next>".

5 Specify the location and the group membership of the new users. You can also make the location automatically identifiable from the phone number.
Click on "Next>".

6 You can define a user here to serve as a template for the new users. The procedure for this is similar to the function 'Create new user account and apply the properties of an existing user' in the SwyxWare Administration when creating a new user. However, files such as skins, ring tones, and Call Routing scripts are not included. You also specify the call permissions and the feature profile of the new users.
Decide whether public phone numbers should be copied with the import.
If you want to assign internal numbers, activate the checkbox and specify how many final digits of the phone numbers should be used.
Activate the checkbox if the new users should receive an email with their SwyxWare user data after their creation. You can specify the email server and the text of the email here, using 'Configure email'.
Click on "Next>".

7 A list of the users to be imported is displayed with all individual parameters. You can still edit this now.
Users who are already present are neither displayed nor imported; the selection criterion for this is the user name.
Click on "Next>".

8 The users are imported.
If the import of a user fails, a red error message appears in the list, otherwise there is a green success message. The numbers of successful and failed imports are also shown after a run.
You may be able to change user parameters here in the list of failed imports, and start a new import.
Click on "Next>".

9 An overview of all imported users is then displayed.

10 Close the program with 'End'.

All imported users now appear as activated SwyxWare users with the configured properties in the SwyxWare Administration.

E.4 TEST PROGRAMS FOR THE ISDN CARDS

To check the functionality of the ISDN cards, you can find a corresponding utility program for the different ISDN cards under the following link:

Swyx ISDN SX2 driver (32bit & 64bit)

https://www.enreach.de/produkte/support/support-downloads.html#cat_6

E.4.1 TEST PROGRAMS FOR THE SX2 CARD FAMILY

To check the correct operation of the ISDN card, please install the test programs:

E.4.1.1 CONNECTION TESTER CONTEST

If the card is already connected to the ISDN network at this time, you can use the "contest" connection test program to check whether the card works properly.

Please enter the number of the line you would like to test in the field "Subscriber Number" and click on "Start".

A connection to your own line will be created and some test data will be transmitted. If this test was successful you can immediately resume installation of SwyxWare.

If it was not possible to create a self-connection, consult the detailed information on troubleshooting included in the enclosed Help information.

E.4.1.2 D CHANNEL MONITOR

You will find the installation version of the D channel monitor on the SwyxWare DVD in the directory \Tools\D-Channelmonitor. This program will help you to record the information exchanged between the ISDN card and the telecommunications system or the switching. This recording can provide further indications for troubleshooting.

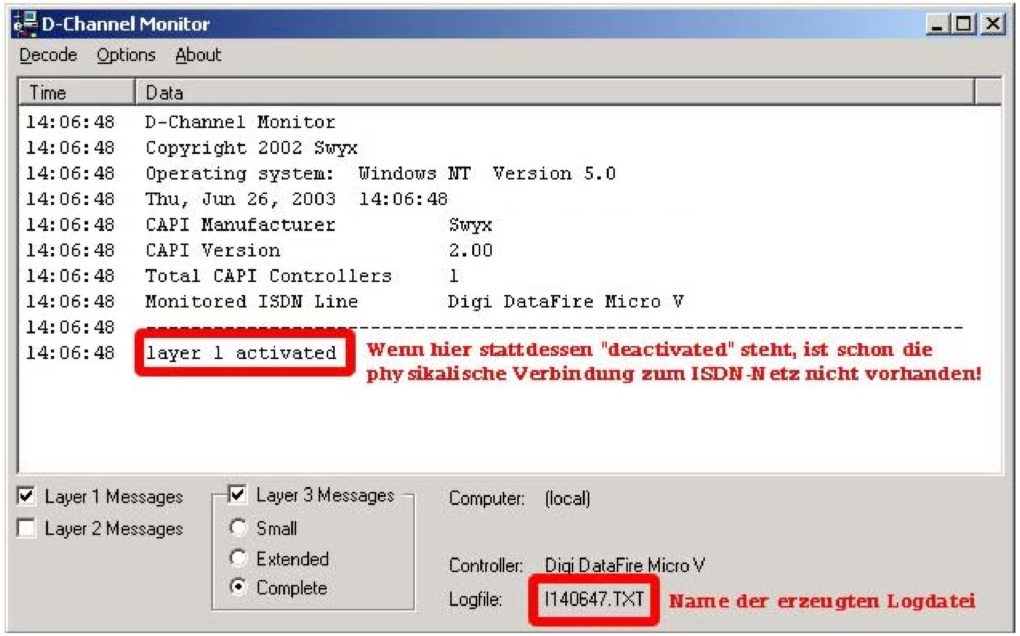
The D channel monitor can be called as follows:

```
dcm [-c x] [-l1x] [-l2x] [-l3x]
```

You can use the following parameters:

Parameter	Standard	Explanation
-c	c 1	A CAPI Controller will be selected.
-l1	l1+ (on)	Level1 messages are switched on or off using -l1+ or -l1- respectively.
-l2	l2- (off)	Level2 messages are switched on or off using -l2+ or -l2- respectively.
-l3	l3s	Level3 messages l3- is switched off l3s is used to display the names of the information elements. -l3l is used for a full display. In addition, some information elements are displayed completely. -l3x is used to display the names of the information elements in detail.

The D Channel Monitor appears:



```
14:06:48  D-Channel Monitor
14:06:48  Copyright 2002 Swyx
14:06:48  Operating system:  Windows NT  Version 5.0
14:06:48  Thu, Jun 26, 2003  14:06:48
14:06:48  CAPI Manufacturer          Swyx
14:06:48  CAPI Version               2.00
14:06:48  Total CAPI Controllers     1
14:06:48  Monitored ISDN Line        Digi DataFire Micro V
14:06:48  ---------------------------------------------------------------
14:06:48  layer 1 activated
```

Wenn hier stattdessen "deactivated" steht, ist schon die physikalische Verbindung zum ISDN-Netz nicht vorhanden!

☑ Layer 1 Messages
□ Layer 2 Messages
☑ Layer 3 Messages
○ Small
○ Extended
● Complete

Computer: (local)
Controller: Digi DataFire Micro V
Logfile: I140647.TXT

Name der erzeugten Logdatei

The trace file will be saved in the directory "C:\ProgramData\Swyx\Traces" and is given the name that is indicated in the D Channel Monitor.

If you have several cards installed or if you work with a SX2 QuadBRI, start one D channel monitor per line. When the program is started in this case you will be prompted to select the controller you want.

Trace files for all of the lines, which have something to do with the occurring problem, are required. For example, if you operate a line with three ISDN line, activate one D Channel Monitor for each of these three controllers.

An exact description of your ISDN configuration is always helpful.

If there is a problem on the ISDN side, we recommend a trace of the SwyxGate and the SwyxServer (ETraces of the SwyxWare Services, Page 428).

E.5 TRACES OF THE SWYXWARE SERVICES

All SwyxWare services can create and save run protocols, so-called traces (Log) in a corresponding file. These trace files help to identify errors.

History logs are preset for deletion after 7 days. Please observe the respective applicable legal regulations. Please observe this in particular if you change the settings for memory restriction.

The Swyx Trace Tool simplifies the settings of tracing for the individual services. It is installed along with the SwyxServer. The trace range of the SwyxWare services is set to default values after the installation. The SwyxWare services will be continually generating log files.

Events that occur during the configuration of SwyxWare are recorded in the Windows Installer tracing. See ETracing during installation, Page 432.

E.5.1 SWYX TRACE TOOL

Swyx Trace Tool is an instrument for administrators to set the extent of traces (Logs). It can also help to upload log files directly to your support service.

Swyx Trace Tool offers the following specific functions:

- Even the default setting generates many useful traces.
- Traces can be archived and deleted in set time intervals.
- For exact error analysis it is often necessary to trace the individual actions of the service in more detail. The so-called Trace Level is specified globally for all SwyxWare services running on a computer. In the Trace Tool you can open trace profiles (.ttf) with ready trace settings. Enreach Support can create other customer-specific trace profiles, for subsequent use by the customer.
- So-called "Process Memory Dumps" can be generated by SwyxWare and uploaded.
- The link to a ticket ID will ensure that transferred traces can be assigned to the correct support case.

- To obtain a complete picture for support, information can be added and uploaded about the installed SwyxWare versions, the operating system used, the event log for the time, and Swyx-related registry entries and the configuration files (*.config).

File name for the Trace files

The trace files are all named in the following format:

<Name of the service>-yyyymmdd-hhmmss.log

A second file with the same name, e.g. for clocks changing , is given an additional index (-n).

E.5.1.1 INSTALLATION OF THE SWYX TRACE TOOL

The Swyx Trace Tool is automatically installed along with the installation of the SwyxServer. The default settings are activated at this time.

Memory requirement

To avoid taking up too much memory space, the Swyx Trace Tool automatically deletes old files (ZIP files) according to the following criteria:

- Every SwyxWare service automatically terminates the protocol - as before - if the memory space available on the hard disk falls below 100 MB.
- When more memory space is again available, logging is automatically resumed - as before.
- The Cleanup function is started automatically every 15 minutes by the Microsoft Scheduler, and compresses all 'old' files into a ZIP file. These are then deleted in accordance with the specified retention period (*This is how you set the retention period for trace files*, Page 431).

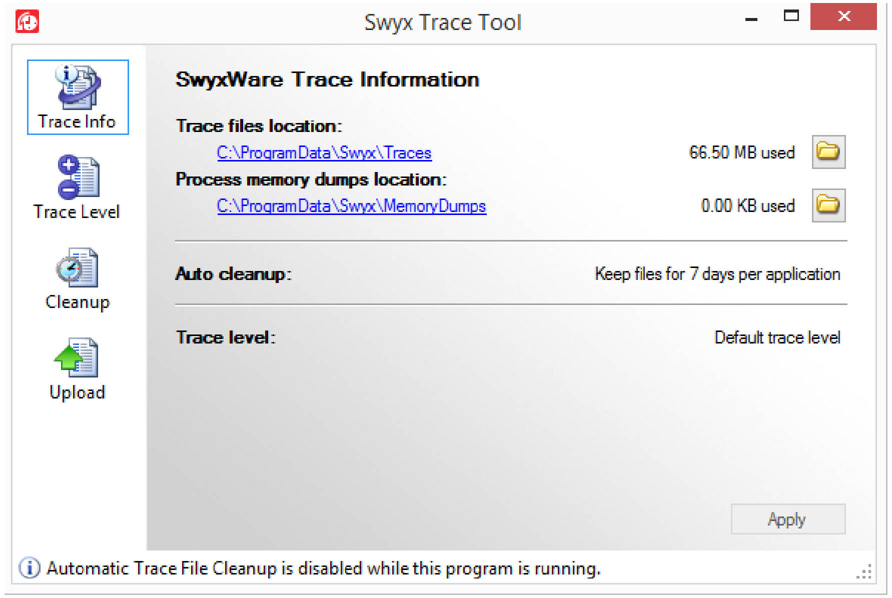
File transfer

The log files (traces) can be stored either on the web server provided by Enreach, or on a partner's web server. In the latter case, the relevant Internet address (URL) for this web server must be given beforehand. Alternatively, e.g. if the server has no direct Internet access, you can store the files as a ZIP archive (on the desktop) and send them to support by another means.

> Please note that you have to obtain a ticket ID from Support before the transfer (upload) to the Enreach web server. You then enter this ticket ID before the transfer.

How to transfer trace files

1 Start the Swyx Trace Tool under "Start | Programs | SwyxWare | Swyx Trace Tool".
The Swyx Trace Tool homepage opens up.



SwyxWare Trace Information

Trace files location:
C:\ProgramData\Swyx\Traces 66.50 MB used

Process memory dumps location:
C:\ProgramData\Swyx\MemoryDumps 0.00 KB used

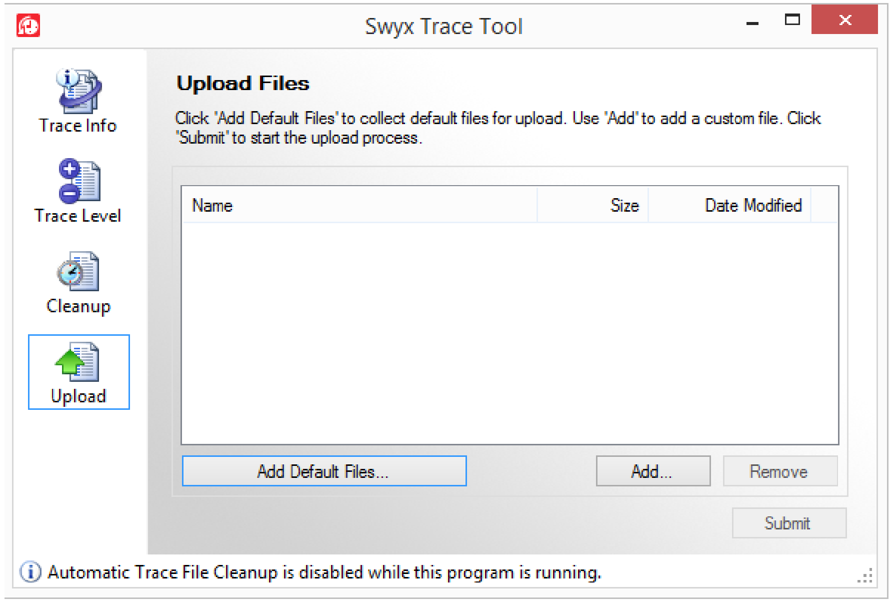
Auto cleanup: Keep files for 7 days per application

Trace level: Default trace level

Automatic Trace File Cleanup is disabled while this program is running.

You will find information here about where the trace files and the memory dumps are stored.
Here you can change the memory location for the Trace files and the memory dumps, by clicking on the directory icon.
You can also see the time interval after which old files are deleted, and the current trace settings.

2 Select "Upload" in the left bar.



Upload Files

Click 'Add Default Files' to collect default files for upload. Use 'Add' to add a custom file. Click 'Submit' to start the upload process.

Automatic Trace File Cleanup is disabled while this program is running.

3 Enter the files to be transferred.
You can select any files you want with "Add...".

4 Select "Add Default Files..." to select files of the event logs. The wizard will guide you through the collection of the file packet:

- Problem Description
  Enter a description for the problem that has occurred.
- Trace files and process memory dumps
  Choose whether only the event logs of the SwyxWare services (trace files) should be added, or also memory dumps from non-reacting SwyxWare services.
  You can restrict the files to a useful period.
- System Information
  Add further information here about the complete system:
  - For the SwyxWare information, the installed product versions and a dump of the Swyx-relevant registration keys are recorded.
  - The Microsoft System Information file (collected with the help of MSinfo.exe) contains all relevant data about hardware, software and configuration of the computer being used.
  - The Microsoft Event Log contains all information on events that were not directly caused by SwyxWare, but occurred in the same period.
- Database backup
  You can save the entire SwyxWare database here, and add it too.

5 The complete file list is created. This may take a few minutes. The progress will be displayed.

6 Click on "Finish..." to assemble the packet. You will see an overview of all the included files.

7 Click "Submit" to start the Upload Wizard, which will assist you with the transfer.
You can transfer files to Enreach or to another URL. Alternatively, you can also archive the files as ZIP files, which you will find on your desktop after being packed.
The ticket ID is used to generate the standard name for such a transfer file.

The support ticket ID is absolutely essential for the transfer to the Enreach upload server.

E.5.2 AUTOMATIC FILE DELETION (CLEANUP)

You can have 'old' files deleted automatically, i.e. the ZIP files that are no longer within the retention period. In the default settings, this is done every 15 minutes with the Microsoft Scheduler. You have several different options:

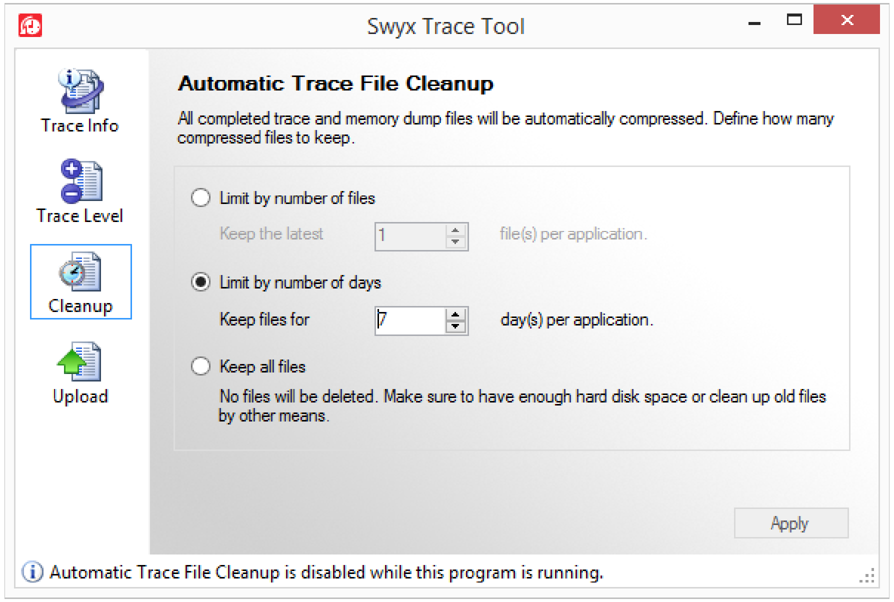
- You can limit the number of log files. Since each service logs a different amount, the traces go back differing lengths of time.
- You can specify a period for which traces should be saved. You say how many complete calendar days they should be kept (default: 7).
  Example: If you specify "1" here, the complete last calendar day (yesterday) is kept until the present day is ended.
- You can keep all files. In this case, make sure you have sufficient memory space!

Please observe the respective applicable legal regulations. Please observe this in particular if you change the settings for memory restriction.

This is how you set the retention period for trace files

1 Start the Swyx Trace Tool under "Start | Programs | SwyxWare | Swyx Trace Tool".
The Swyx Trace Tool homepage opens up.

2 Select "Cleanup" in the left bar.
The current settings are displayed.



Automatic Trace File Cleanup

All completed trace and memory dump files will be automatically compressed. Define how many compressed files to keep.

○ Limit by number of files
Keep the latest 1 file(s) per application.

● Limit by number of days
Keep files for 7 day(s) per application.

○ Keep all files
No files will be deleted. Make sure to have enough hard disk space or clean up old files by other means.

Automatic Trace File Cleanup is disabled while this program is running.

3 You can specify here which files should be kept, and for how long:

- Set number of files
  The number of log files to be kept is specified here. The periods of time can differ in length according to the logged component.
- Specify retention period
  You specify here how many complete calendar days they should be kept (default: 7 days). Example: If you specify "1" here, the complete last calendar day (yesterday) is kept until the present day is ended.
- Keep all files
  In this case, make sure there is sufficient available memory space.

When you click on "Apply", your chosen settings are immediately adopted by the Swyx Trace Tool.

E.5.3 TRACE PROFILE - SCOPE OF TRACES

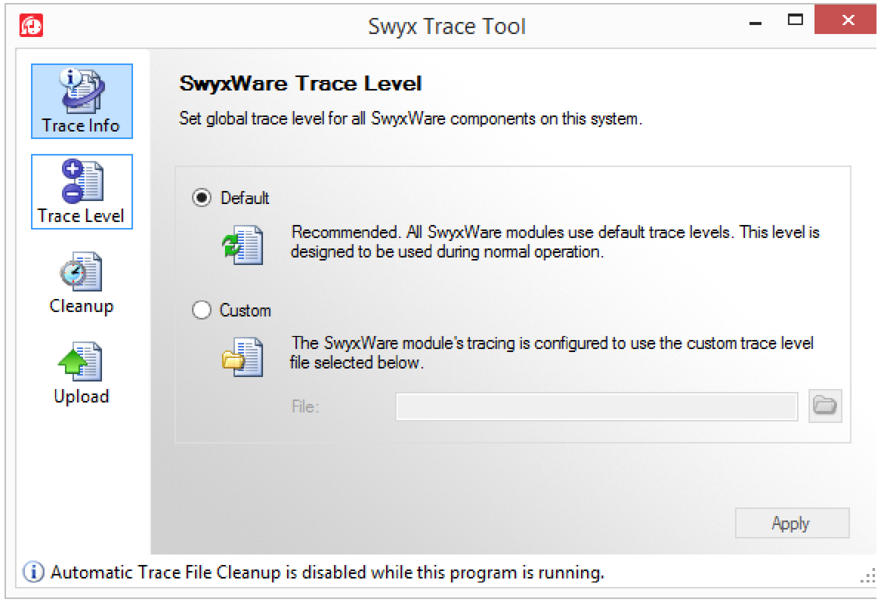
A defined trace level is already generated as default. If a different setting is required in exceptional cases, Support will send you a file containing the necessary trace settings for your specific case. This file is read in. After the support case is resolved, please restore the default settings.

A few trace profiles for special cases are already supplied (.tfl files in SwyxWare folder.

How to set the scope for trace files

1 Start the Swyx Trace Tool under "Start | Programs | SwyxWare | Swyx Trace Tool".
The Swyx Trace Tool homepage opens up.

2 Select "Trace Level" in the left bar.



SwyxWare Trace Level

Set global trace level for all SwyxWare components on this system.

● Default

Recommended. All SwyxWare modules use default trace levels. This level is designed to be used during normal operation.

○ Custom

The SwyxWare module's tracing is configured to use the custom trace level file selected below.

File:

Automatic Trace File Cleanup is disabled while this program is running.

- Standard
  Restore the default settings.
- User-defined
  In this case you read in a special .tfl configuration file, which has been sent by Support for example. Enter the path to this file, or choose one of the supplied profiles.

When you click on "Apply", your chosen settings are immediately adopted by the Swyx Trace Tool.

E.5.3.1 SWYX TRACE TOOL FROM THE COMMAND LINE

You can also start the Swyx Trace Tool from the command line. To do this, move to the Swyx Trace Tool program directory, and enter

```
TraceTool /<Parameter>
```

You can use the following parameters:

Parameter	Explanation
?	Displays an overview of all parameters.
default	Activates Standard Tracing and deletes existing user settings.
init	Sets the default settings without overwriting existing user settings.
all	Saves all user settings.
save <File Name>	Saves the current trace settings. Only the differences to the standard tracing are stored in this file.
name <Brief Description>	Short description of the trace settings. This name is later displayed in the Swyx Trace Tool for the trace selection.
load <File Name>	Copies the trace settings from the specified file.
silent	Suppresses all further outputs from the Swyx Trace Tool
cleanup	Deletes all ZIP files that no longer meet the retention criteria.
user <User Name Authentication>	The cleanup is executed under the given user account. Specify the password with pass <password>.
pass <password>	Gives the password of the user account given with user
compress	Compresses all trace files that are no longer being written.
infoBox	Displays all files that were deleted in the automatic cleanup.
infoLog	Logs the automatic deletion of the files in the Windows event display.
installTask	Installs the task planner, which executes the automatic cleanup.
uninstallTask	Removes the task planner for the automatic cleanup.

E.5.4 TRACING DURING INSTALLATION

The events during the installation are recorded in the Windows Installer trace. For this, start the installation from the command line with

```
setup.msi \l*vx Log_File
```

Log_file stands for the directory and the name of the log file, e.g. c:\Install.log.

E.5.5 TRACING FROM SWYXIT!

The trace files generated by SwyxIt! may contain personal data.

Please observe the respective applicable legal regulations. Please pay attention to this, especially when saving processing personal data for tracing, see *Deactivate tracing*, Page 433.

SwyxIt! offers the possibility of logging the activities of the software. By default tracing is deactivated.

For exact error analysis it is often necessary to trace the individual actions in more detail. The SwyxIt! program directory contains files (TraceOn.reg, TraceOn-x64.reg). Activate the tracing by double clicking on the respective file.

The so-called trace depth is determined using a number of registration entries.

Use these REG files only if you are asked to do so by a Enreach Support employee.

SwyxIt! Traces cannot be deleted automatically. In order to meet the valid data protection regulations, it may be necessary to delete the corresponding entries manually.

Where can the trace files be found?

You'll find the trace files in the temp directory of the user who executes SwyxIt!. You can find the temp directory quickly by entering the address %temp% in Windows Explorer. The Explorer then navigates automatically to the temp directory valid for the user.

If you want to collect the trace files for a longer period in special cases, you can adjust the target directory for the trace files. Open the registry editor and adjust the value "Logfile" under the key ""HKEY_LOCAL_MACHINE\SOFTWARE\Swyx\Client Line Manager\CurrentVersion\Tracing". If only a file name is specified there, the trace files are written to the temp directory. If a full path is given there (e.g.: c:\trace\SwyxIt!.log), the trace files are written to the corresponding directory.

Deactivate tracing

Please observe the respective applicable legal data protection regulations and change the trace level back again following troubleshooting.

After troubleshooting, you should deactivate the history logs again. You will find the files necessary for this (TraceOff.reg, TraceOff-x64.reg) in the program directory of SwyxIt!. Deactivate the tracing by double clicking on the respective file.

APP. F:IBM NOTES INTEGRATION

SwyxWare integration in a IBM Notes environment

In this chapter, you will find out how you can use SwyxWare and IBM Notes together. All elements relevant for the administrator are explained in detail. Further descriptions of SwyxIt! user-relevant features are contained in the SwyxIt! manual.

> To integrate SwyxIt! into an environment with IBM Notes you need the Option Pack or Additional function Swyx Connector for Notes.

F.1 OVERVIEW

The IBM Notes integration for SwyxIt! includes the following features:

- Name resolution from SwyxIt! out of IBM Notes for incoming calls and for list search
- Displaying an IBM Notes contact for an incoming call
- Sending an email from SwyxIt!
- IBM Notes functions on the Speed Dial, such as calendar information
- Direct dialing from IBM Notes. See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/#context/help/dial_from_notes_$.

Requirements

To use Swyx Connector for Notes you need at least IBM Notes V9.

Voice messages

SwyxServer uses the SMTP protocol for sending voice messages.

Sending voice messages to a Domino server, and the remote inquiry feature are thus already supported by older SwyxWare versions.

Calendar Query

With the calendar query you can define Call Routing Manager rules, based on calendar entries made in IBM Notes.

Name Resolution for SwyxIt!

Notes Integration resolves unknown phone numbers using the personal and global Lotus/IBM/HCL Domino database. You can also configure and share additional databases, see *F.3 Configuration of the database display and selection*, Page 435.

Displaying an IBM Notes contact for an incoming call

When receiving a call, the corresponding contact can be opened automatically in the IBM Notes client. You can decide for each database, whether the contacts shall be opened automatically.

Sending an email from SwyxIt!

Send an email directly from SwyxIt! to a IBM Notes contact. The email feature can be started from different lists (e.g. the Call Journal), the SwyxIt! Messenger or the context menu of a speed dial button.

IBM Notes features on the Speed Dial

Certain IBM Notes features can be started directly with the SwyxIt! Speed Dial buttons.

- Display of calendar information

  In the context menu of a Speed Dial, you can call up the IBM Notes calendar of the person stored on the Speed Dial. The availability information from the calendar is also displayed.
- Meeting planning

  You can create a meeting request via the context menu of the speed dial button. The person assigned to the speed dial button will be added as participant.

- Delegate Task

  You can create a new task via the context menu of the speed dial button. The person assigned to the speed dial button will be added as recipient.
- Resolution of IBM Notes users via the Speed Dial button

  The context menu of a Speed Dial button displays whether the contact can be assigned to a IBM Notes user, one of your IBM Notes contacts, or if no assignment is possible. The menu item changes according to the assignment.

F.2 INSTALLATION AND DISTRIBUTION

The following installation and configuration steps are required to make Swyx Connector for Notes available to users:

- Configuration of the database display and selection *F.3 Configuration of the database display and selection*, Page 435

F.3 CONFIGURATION OF THE DATABASE DISPLAY AND SELECTION

The following section describes the configuration of the database display. Here you can select, which databases shall be made available to the users for IBM Notes integration purposes. You can also configure which database fields shall contain important information for the name resolution, e.g. name, phone numbers etc.

Your database selections are saved in the SwyxWare database as a global XML file, and will be used by all clients logged on to corresponding SwyxServer.

F.3.1 CONFIGURATION REQUIREMENTS

The configuration requires SwyxIt! including the IBM Notes Plugin logged on to your SwyxServer. See also https ://help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/installing_notes_$.

The configuration tool of the Plugin can either be started in user mode, or in various administrator modes.

F.3.2 DATABASE SETTINGS

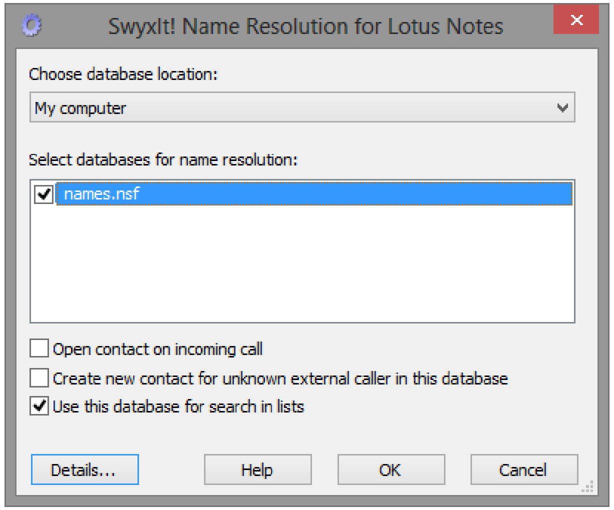
The following paragraphs describe the definition of databases and database fields.

To configure the IBM Notesintegration

1 Start the Notes Plugin configuration tool in administrator mode. Select "NotesAddInSettings.exe" in the SwyxIt! program directory with one of the following parameters:

Parameter	Function
-a	Starts the AddIn in administrator mode, meaning that the "Details" button and all databases are available. The standard settings are loaded by default. Any changes are saved as XML file. To make these changes available to the users, the file has to be uploaded into the database.
-a -f	Starts the Add-In in administrator mode. After startup, a window opens in which a configuration file (XML) can be selected for further editing. To make these changes available to the users, the file has to be uploaded into the database.
-a -d	Starts the Add-In in administrator mode. The current configuration file from the SwyxWare database is uploaded, and can be edited. After editing, the file has to be uploaded into the database again.

The window containing the database configuration for the name resolution, is opened in administrator mode. Contrary to the user mode, the administrator mode contains all IBM Notes databases as well as the "Details" button. Depending on the selected parameters for the call, the system either uploads the default settings, the settings from the SwyxWare database, or the settings from a selected XML file.


SwyxIt! Name Resolution for Lotus Notes

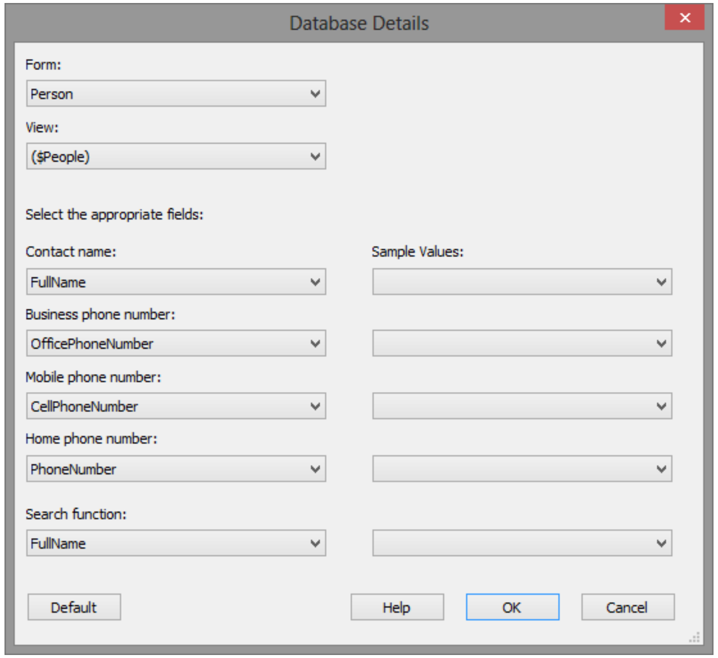
Choose database location:
My computer

Select databases for name resolution:
☑ names.nsf

□ Open contact on incoming call
□ Create new contact for unknown external caller in this database
☑ Use this database for search in lists

2 In the field "Choose database location", either select the Domino server or your own computer. Any available databases are displayed. Enable all databases that shall be made available to the users for selection. The access to enabled databases may be further restricted in the user mode.

3 Now, configure the database fields to be used for the name resolution. Select the respective database in the dialog box "SwyxIt! Name Resolution for IBM Notes", and click on the "Details" button. The dialog box "Database Details" including the default settings is displayed.


Database Details

Form: Person
View: ($People)

Select the appropriate fields:

Contact name:	Sample Values:
FullName	
Business phone number:	
OfficePhoneNumber	
Mobile phone number:	
CellPhoneNumber	
Home phone number:	
PhoneNumber	
Search function:	
FullName	

4 Select the form, the view, and the fields containing the individual values, such as name or phone number. Sample values for your selection are displayed in the right-hand column. Please verify that your field selection is correct.

5 In the last field "Fulltext Search", select the database field for fulltext search. This value is used for:

- the search function in the phonebook. Any IBM Notes contacts are also taken into account.
- the name resolution in the SwyxIt! input field.

For this setting to take effect, the users must enable "Use this database for fulltext search" checkbox during configuration (default setting: enabled).

6 Click "OK" to save the changes for this database.

7 If required, select another database for configuration in the "SwyxIt! Name Resolution for IBM Notes" dialog, or click on "OK" to save the changes.

8 In the following dialog box, select a storage location for the XML file containing the configuration settings. The name "NotesDbDefaults.xml" is set by default.

9 After configuring the database options, the settings have to be distributed to the users. See *F.3.3 Saving and distributing the database configuration*, Page 437.

F.3.3 SAVING AND DISTRIBUTING THE DATABASE CONFIGURATION

After configuring the database options, any settings saved in the "NotesDbDefaults.xml" file must be uploaded into the SwyxWare database as a global file in the "Other" category. These settings are then used by any user logged on to the SwyxServer.

Even if parameter -d has been used to download the file from the database during startup of the administrator mode, the file must be uploaded manually into the database.

How you save and distribute the database configuration

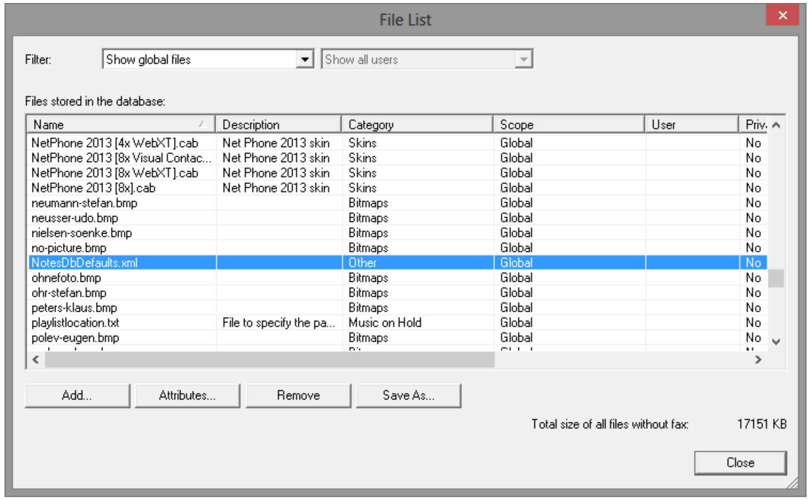
1 Start the SwyxWare Administration and log in to the SwyxServer.

2 Click the SwyxServer entry with the right mouse button to open the context menu.

3 Select "Properties".

4 Select the "Files" tab.

5 Click on the "Edit" button. The dialog box with the available files is displayed.



File List

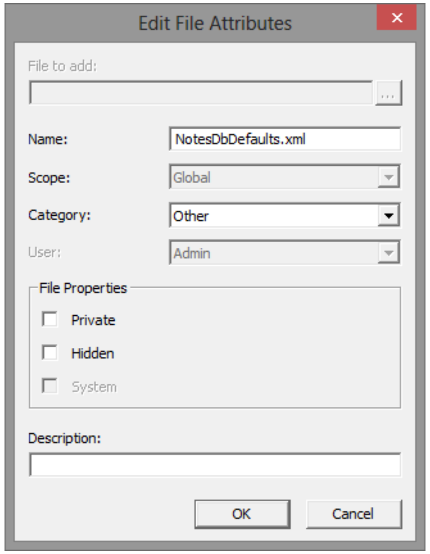
Filter: Show global files | Show all users

Files stored in the database:

Name	Description	Category	Scope	User	Priv.
NetPhone 2013 [4x WebXT].cab	Net Phone 2013 skin	Skins	Global		No
NetPhone 2013 [8x Visual Contac...	Net Phone 2013 skin	Skins	Global		No
NetPhone 2013 [8x WebXT].cab	Net Phone 2013 skin	Skins	Global		No
NetPhone 2013 [8x].cab	Net Phone 2013 skin	Skins	Global		No
neumann-stefan.bmp		Bitmaps	Global		No
neusser-udo.bmp		Bitmaps	Global		No
nielsen-soenke.bmp		Bitmaps	Global		No
no-picture.bmp		Bitmaps	Global		No
NotesDbDefaults.xml		Other	Global		No
ohnefoto.bmp		Bitmaps	Global		No
ohr-stefan.bmp		Bitmaps	Global		No
peters-klaus.bmp		Bitmaps	Global		No
playlistlocation.txt	File to specify the pa...	Music on Hold	Global		No
polev-eugen.bmp		Bitmaps	Global		No

Total size of all files without fax: 17151 KB

6 Click on "Add". The dialog box for the file upload is displayed.



Edit File Attributes

File to add:

Name: NotesDbDefaults.xml

Scope: Global

Category: Other

User: Admin

File Properties

□ Private

□ Hidden

□ System

Description:

7 Click ... next to the "File" field and select the ‘NotesDbDefaults.xml’ file you saved.

8 Select the scope "Global" and the category "Other", and enter a description if required.

9 Confirm your changes with "OK". The file is uploaded into the database. Any existing configuration files will be overwritten.

Your configuration settings are now available to all users logged on to this SwyxServer.

See also *7.5.10 The "Files" Tab*, Page 97.

APP. G: ESTOS, DATEV, C4B INTEGRATION

With various additional interfaces it is possible to integrate applications of third party manufacturers into SwyxWare:

ESTOS MetaDirectory

ESTOS MetaDirectory 4 is a server application, which merges different databases to form a single consistent LDAP directory. Contact data from various databases are thus provided to the SwyxIt! users and updated automatically.

C4B XPhone Connect Directory

Alternatively, you can also use C4B XPhone Connect Directory V6.0.81 SR 1 as an interface between external data sources and SwyxIt! C4B XPhone Connect Directory accesses the corresponding data directly, no replication takes place.

In order to access the ESTOS MetaDirectory or C4B XPhone Connect Directory, SwyxIt! has to be installed with the "Swyx VisualContacts" component.

For more information on custom SwyxIt!installation, see help.enreach.com/cpe/latest.version/Client/Swyx/en-EN/index.html#context/help/custom_setup_$.

"Swyx Connector for DATEV" option

The linking of ESTOS MetaDirectory or C4B XPhone Connect Directory also enables the integration of DATEV pro into SwyxWare. Thereby, the DATEV contact data and the telephony function are merged with SwyxIt!, the computer telephony client.

In order to access the ESTOS MetaDirectory and to integrate DATEV, DATEV Basis pro V 2.0 or higher has to be installed on the user PC. SwyxIt! has to be installed with the Swyx Connector for DATEV component.

For more information on custom SwyxIt!installation, see https :// help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/custom_setup_$.

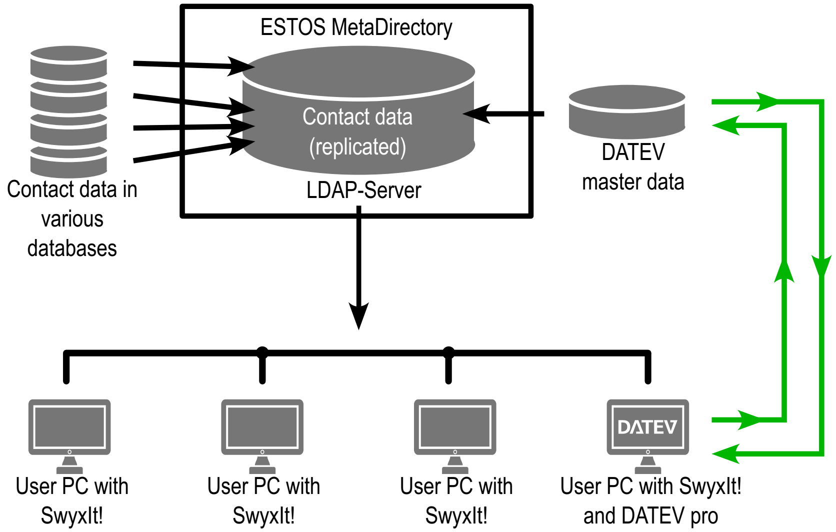


Fig. G-1: ESTOS MetaDirectory in SwyxWare environment

G.1 SYSTEM REQUIREMENTS FOR ESTOS METADIRECTORY 4 PROFESSIONAL AND C4B XPHONE CONNECT DIRECTORY V6.0.81 SR 1

For further information on system requirements for ESTOS MetaDirectory 4 Professional see estos.com/service/downloads

For further information on system requirements for C4B Xphone Connect Directory V6.0.81 SR 1 see

c4b.com/en/xphone-connect/system-requirements/

G.2 ESTOS METADIRECTORY OR C4B XPHONE CONNECT DIRECTORY USES PORT 712 BY DEFAULT.

ESTOS Metadirectory Professional 4 or XPhone Connect Server with C4B XPhone Connect Directory v6.0.81 SR 1 must be installed on a server in the company network.

You will find the installation file for ESTOS MetaDirectory 4 Professional on the ESTOS Home page.

When installing C4B XPhone Connect Directory v6.0.81 SR 1, you must select the mode for exclusive use of third-party applications and devices as well as the custom installation mode.

You need an appropriate license for the use of ESTOS MetaDirectory or Xphone Connect Directory.

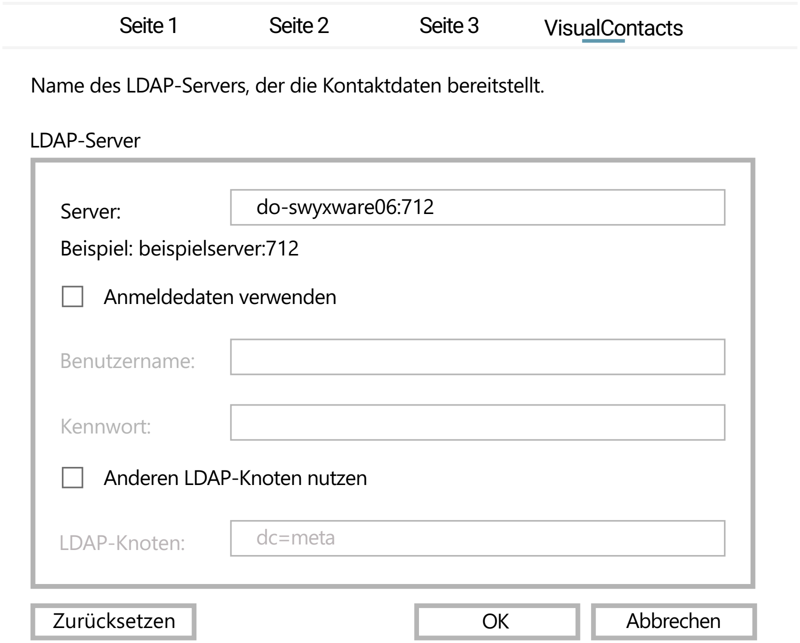
For detailed information on ESTOS MetaDirectory and XPhone Connect Directory, please refer to the corresponding manufacturer documentation.

G.2.1 SPECIFY LDAP SERVER PARAMETERS

ESTOS MetaDirectory and C4B XPhone Connect Directory are based on an LDAP (Lightweight Directory Access Protocol) server. The LDAP server provides a directory service for the contact details.

To enable access to ESTOS MetaDirectory or C4B Xphone Connect Directory via SwyxIt!, the access parameters of the LDAP server must be specified within SwyxIt! on the "VisualContacts" tab.

You can call up the LDAP server parameters by clicking on the Settings button in the "VisualContacts" tab.



Name des LDAP-Servers, der die Kontaktdaten bereitstellt.

LDAP-Server

Server: do-swyxware06:712

Beispiel: beispielserver:712

□ Anmeldedaten verwenden

Benutzername:

Kennwort:

□ Anderen LDAP-Knoten nutzen

LDAP-Knoten: dc=meta

- The IP address, or the name of the server on which ESTOS MetaDirectory or C4B XPhone Connect Directory is installed, must be entered in "Server".
  The port must also be specified if necessary. ESTOS MetaDirectory and C4B XPhone Connect Directory use port 712 by default.
- If an authorization is required for access to the server, the option "Use login" must be activated, and the user name and password must be entered.
- For access to a particular LDAP node in the MetaDirectory, the option "Use different LDAP node" must be activated, and the required node specified.

LDAP server parameters for automatic distribution of SwyxIt!

For an automatic SwyxIt! distribution, the LDAP server parameters can be preset by the administrator by means of the following command line parameters:

LDAP_HOST

LDAP_PORT

e. g.: LDAP_HOST="exampleserver.net"LDAP_PORT=712

See *20.3.2 Automatic distribution of SwyxIt! in a network*, Page 338.

For more information on VisualContacts and DATEV, see help.enreach.com/cpe/latest.version/Client/Swyx/en-US/#context/help/visualcontacts_datev_$.

G.3 SWYX VISUALGROUPS

The current documentation for SwyxVisualGroups can be found at:

help.enreach.com/docs/manuals/english/VisualGroups.pdf

APP. H:SWYX PUSH NOTIFICATION SERVICE

Via Push Notification Service server services can send notifications to client applications to notify them of certain events. This technology makes the communication between server and client more efficient and thus saves battery since the client's constant change queries become obsolete.

For the Swyx Mobile for iOS Client push notifications are required to make use of features that are available with iOS 10, e.g. CallKit integration. In addition, for Swyx Mobile for iOS and Android push notifications result in lower battery consumption on mobile devices. Push notification and consequently the aforementioned benefits are available in the Swyx Mobile clients from version 2.0.0 onwards.

Swyx Mobile clients version 1.x which do not support push notifications can still be used with SwyxServer version 11. These clients, however, do not have the CallKit integration and cannot be developed further. Users of these versions will be referred to the new version, provided they are connected to an active Push Notification Service, and can automatically transfer the existing configuration to the current version.

A Swyx Mobile Version 3.00 or higher requires a SwyxWare Version 12.10 with the latest Push Notification Service Version.

H.1 INSTALLATION OF THE SWYX PUSH NOTIFICATION SERVICE

Supported operating systems:

- Windows Server 2025
- Windows Server 2019
- Windows Server 2016

Requirements for a firewall:

To guarantee the data transfer between the Push Notification Service and the corresponding Apple/Google server, make sure, that the required ports on the Internet firewall are open:

- iOS devices
  Outbound TCP connections to port 443 on api.push.apple.com
- Android devices
  Outbound TCP connections to port 443 on fcm.googleapis.com

How to install the Push Notification Service

You will find this file on the SwyxWare DVD in the "PushNotificationService" directory.

1. Start the installation file ‚PushNotification.msi‘.
   The installation wizard will open.
2. Click on "Next ".
3. Select the target folder and click on "Next".
4. Click on "Install" to start the installation.
   The service is being installed.
5. Complete the installation by clicking on "Finish".

APP. I: APPLICATION EXAMPLES

SwyxWare as Conference Server integrated into an existing PBX

I.1 SWYXSERVER AS A CONFERENCE SERVER

SwyxWare is ideally suited to function as a Conference server for an existing telecommunications system in the company. In this way, an existing, classical telecommunication system can be expanded to include a modern conference server functionality and later be completely replaced with a VoIP telecommunication system, without compromising any of the investments that have already been made. The existing SwyxWare now has to be extended with the corresponding number of users and channel licenses, if necessary.

Requirements

If you would like to equip the conference room with extended functions such as authentication of the conference participants via PIN, you will need the SwyxWare option pack 'Extended call routing'.As your Enreach distribution partner from whom you have purchased your SwyxWare or send your questions per email to presales@swyx.com.

SwyxWare is operated on several internal BRI or PRI connections of the existing telecommunication system to be extended, depending on the capacity required. The classical telecommunication system must support the Euro-ISDN signaling protocol on these ports (or Q.Sig on an internal BRI).

Please note that you will need one B channel per conference participant, which means that to hold two three-person conferences at the same time, you will need six channels or three BRIs, for example.

Installation

Install SwyxWare as a sub-telecommunication system (*D.2 Connection of SwyxWare as Sub-telecommunication System on a Main Telecommunication System*, Page 420).

Make certain that conference participant is set up correctly and assign him an additional number if necessary (*11.9 Conference*, Page 213).

Configuration

The necessary configurations can be differentiated in the configuration of the telecommunication system, which takes precedence over the SwyxWare, and in the configuration of the SwyxWare.

This is how you configure your telecommunication system for a Conference server

1 The numbers of the conference rooms have to be entered into the routing table of the telecommunication system, so they can be signaled to SwyxWare at the internal S_0 or S_{2m}. You may have to ask the manufacturer of your old telecommunication system about this.

This is how you configure SwyxWare for a Conference server

1 Configure SwyxServer and SwyxGate for operation as a sub-telecommunication system.
See *D.2 Connection of SwyxWare as Sub-telecommunication System on a Main Telecommunication System*, Page 420.

2 Based on your needs, enter additional numbers to the conference participants configured in SwyxWare Administration (*7.5.4 The "Internal Numbers" Tab*, Page 91).

3 Configuration of the Conference Participant:
Create rules here, if necessary with the help of the Call Routing Manager, which allow authentication via a PIN, number identification or similar parameters.

External subscribers can reach the conference room per direct dial or by transferring the call from telephone in the telecommunication system.

If the number of conference participants equals the number of available SwyxGate channels, additional subscribers who would like to dial into the conference will receive a busy signal.

I.2 SWYXIT! AND SWYXPHONE IN A TERMINAL SERVER ENVIRONMENT

The possibility of using SwyxWare, SwyxIt! and SwyxPhone in a Microsoft or Citrix terminal server environment is described below.

In a Citrix Terminal Server environment, the functionality of audio devices on the client computer (remote audio) is not supported.

Terminal server basics

A terminalserver configuration is made up of the following components: terminal server service, the protocol (Remote Desktop Protocol or Independent Computing Architecture Protocol) and the terminal clients.

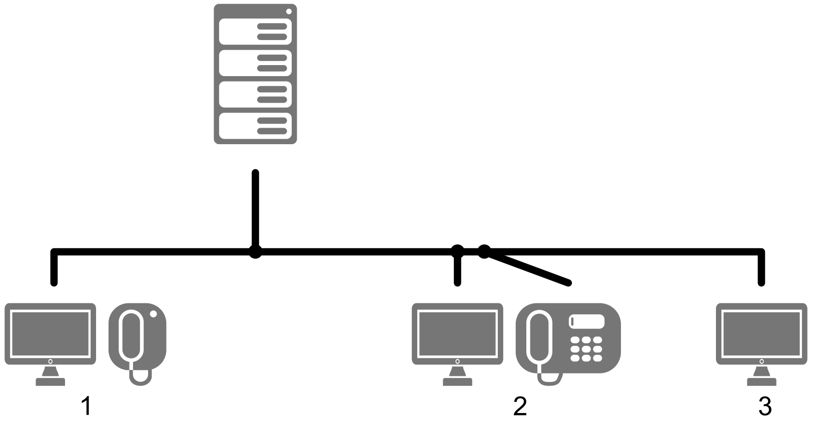
The terminal server service runs on one or a series of Microsoft Windows servers. Applications such as MS Word, Excel, Outlook, CRM applications or even SAP are installed on these servers.

The terminal servers now make the installed applications available to the terminal clients by using a specific protocol. In the case of Microsoft, this is RDP (Remote Desktop Protocol) and ICA (Independent Computing Architecture protocol) for Citrix. The applications in this system are always run on the terminal server and the protocols serve to transport the desktop contents to the terminal client that then displays this content. The keyboard entries and mouse movements are sent from the terminal client to the terminal server.

Each user only sees his individual session, which is transparently managed by the server operating system. The user is independent of the work session of other clients.

There are a number of advantages of this technique, which actually isn't so new (text-based terminals were the first interactive entry devices for the classical mainframe computers):

- Central storage of data and applications. This allows central backup and updates.
- Effective use of computer capacity
- The display device, i.e. the Terminal Client, can be "simple". Starting with a Windows computer, Linux clients, thin clients without hard disk, fan, etc.
- The low bandwidth also allows access via slow lines or when travelling.
- A connection interruption or a work station system crash is not a problem. The session can be restored and you can start where you left off.



- User 1 Outlook and SwyxIt!
  Terminal Client: A normal Windows computer or a Thin Client
  local SwyxIt!
  Screen displays Session 1

- User 2: Word and SwyxIt!
  Terminal Client: Linux or
  no locale SwyxIt!, but SwyxPhone
  Screen displays Session 2
- User 3: Word and Excel
  Terminal Client:
  no local SwyxIt!
  Screen displays Session 3

I.2.1 CONFIGURATIONOF

SwyxIt! can be installed on a terminal server, so that all terminal clients may use this SwyxIt!. If Outlook is also installed on the terminal server, you can dial your contacts directly from the contacts.

You can visit SwyxIt! or SwyxPhone

- in CTI mode on the local computer, see *I.2.1.2 CTI SwyxIt! on terminal server*, Page 446,
  or
- Configure your audio devices for a remote desktop environment and use SwyxIt! directly on the terminal server, see *I.2.1.1 Configure audio devices for remote desktop environment*, Page 445

I.2.1.1 CONFIGURE AUDIO DEVICES FOR REMOTE DESKTOP ENVIRONMENT

The corresponding configuration is required both on the terminal server and on the client computer.

> The configuration of audio devices for Remote Desktop is only partially supported as of SwyxWare version 13.10. Only use this function for test purposes.

To configure the audio devices on the terminal server

1 Enter "Services" in the search field on the taskbar and confirm with the Enter key.

2 Set the start mode of the "Windows Audio" service to "Automatic" and start the service.

3 Check whether a recording device and a playback device are activated in the operating system.

4 Open the Windows command line via Start | Run.

5 Enter "gpedit.msc" in the command line to open the Group Policy Editor.

6 Configure the following policies via the "Edit policy setting" hyperlink:

Entry path	Required Setting

`Computer Configuration\`
`Administrative templates\`
`Windows Components\`
`RemoteDesktopServices\`
`RemoteDesktopService-Host\`
`DeviceAndResourceRedirection\`
`Allow audio and video playback redirection`
	Enabled

`Computer Configuration\`
`Administrative templates\`
`Windows Components\`
`RemoteDesktopServices\`
`RemoteDesktopService-Host\`
`DeviceAndResourceRedirection\`
`Allow audio recording redirection`
	Enabled

`Computer Configuration\`
`Administrative templates\`
`Windows Components\`
`App Privacy\`
`Let Windows apps access the microphone`
	Enabled, Default for all apps: Force Allow

7 Install SwyxIt!

8 Open the Windows command line via Start | Run.

9 Enter "regedit" in the command line to open the registry editor.

10 Configure the following registry value under:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Swyx\Client Line
Manager\CurrentVersion\Options\EnableRemoteAudio
REG_DWORD      value=0x01
```

To configure the audio devices on the client computer

The audio devices that you want to use with SwyxIt! are connected to the client computer.

1 Enter "Remote Desktop Connection" in the search field on the taskbar and confirm with the Enter key.
2 Select "Show options" or "Show options".
3 Select the "Local Ressourses" tab.
4 In the "Remote audio" area, click on "Settings".
5 Activate the options "Play on this computer" and "Record from this computer".
6 Open the RDP connection to the terminal server.
7 Start SwyxIt! and log on to SwyxServer.
8 In SwyxIt!, click on "Settings | Local configuration..." in the menu bar.
✓ The "Properties of..." page appears.
9 Select the "Audio mode" tab.
10 Make sure that the desired audio devices are marked as "Remote audio" in the list.
✓ The configuration is complete, you can use your audio devices with SwyxIt! on the terminal server.

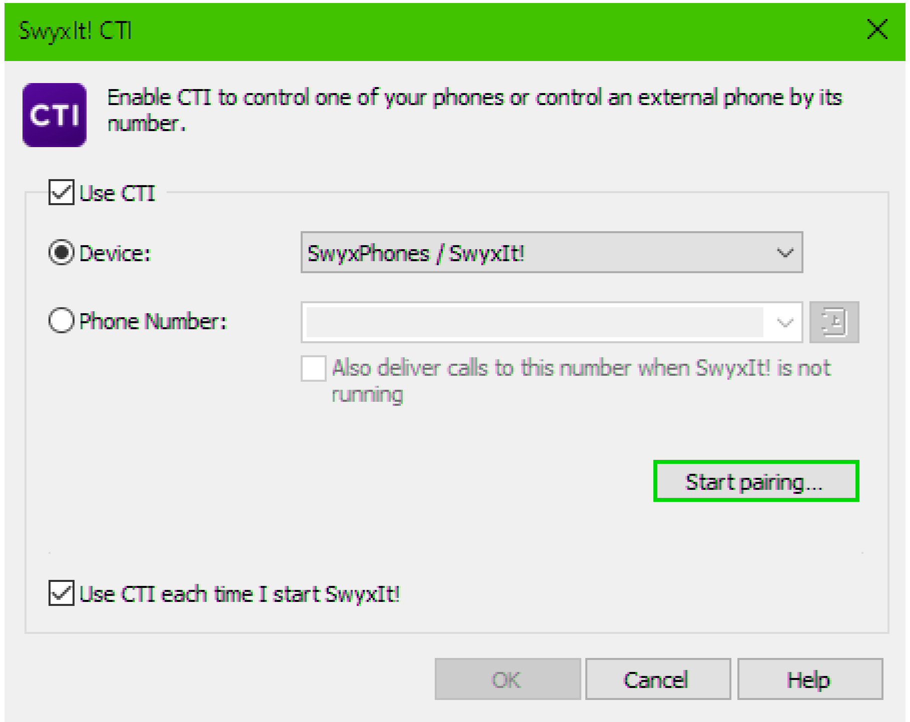
I.2.1.2 CTI SWYXIT! ON TERMINAL SERVER

CTI SwyxIt! or on a terminal server controls a local SwyxIt! or SwyxPhone

CTI SwyxIt! runs on a terminal server and controls a SwyxPhone or a SwyxIt! on the user's computer. The local SwyxIt! is used in particular for voice output and recording via a handset or headset.

To activate CTI mode on the terminal server to control the local SwyxIt! or SwyxPhone

1 Click on "Settings | CTI..." in the menu bar.
Mark the checkbox "Use CTI to control a device".



SwyxIt! CTI

Enable CTI to control one of your phones or control an external phone by its number.

☑ Use CTI

● Device: SwyxPhones / SwyxIt!

○ Phone Number:

□ Also deliver calls to this number when SwyxIt! is not running

☑ Use CTI each time I start SwyxIt!

2 Select the "Device" option.
3 Then, click on "Start pairing".
4 CTI SwyxIt! now searches for a SwyxPhone or SwyxIt! that is logged on to SwyxServer under the same user.
5 Confirm the request in the local SwyxIt! or SwyxPhone by clicking "Accept".
6 Within CTI SwyxIt!, click "OK" in the terminal server environment to start the pairing.

When installed on a terminal server, CTI SwyxIt! shows a special behavior:

- Recording wizard does not start
- No warning if there are too many colors

When installing the TAPI service provider, create one TAPI line for each SwyxIt! user that will use CTI SwyxIt! on the terminal server.

Automatic activation of CTI SwyxIt! in terminal server environments for users

In order to activate the CTI mode automatically for users, a registry key has to be set at the client computer.

After the key has been set, the option "Enable CTI" in the CTI dialogue is automatically activated for the user. Furthermore the option is greyed out, so the user cannot disable this mode.

APP. J:PROVISION OF STATISTICS AND TRAPS VIA SNMP

Administrators can use statistical values to quantify the availability of SwyxWare via SNMP (Simple Network Management Protocol).

The availability of SwyxWare can be monitored. In addition to the entries in the Windows event log, SwyxWare now features an option to generate what are known as SNMP traps or query performance values via SNMP Read.

In order to be able to use these functions, Windows SNMP Support must be installed as a Windows component. Windows SNMP Support is a Windows Server component.

J.1 WINDOWS SNMP SERVICE

All entries in the event log can be converted into SNMP traps using standard Windows programs. This means that an entry in the event log can be sent to a destination as a message. The following Windows programs are used to do this:

- evntwin
  You can use this Windows program to specify which event traps are generated.
- evntcmd, eventtriggers
  As an alternative to the evntwin program, you can use evntcmd to configure which event traps should be generated and export this configuration. You can use eventtriggers to import this configuration on another Computer.
  Data can even be exported/imported from a remote location.

How to activate the generation of traps

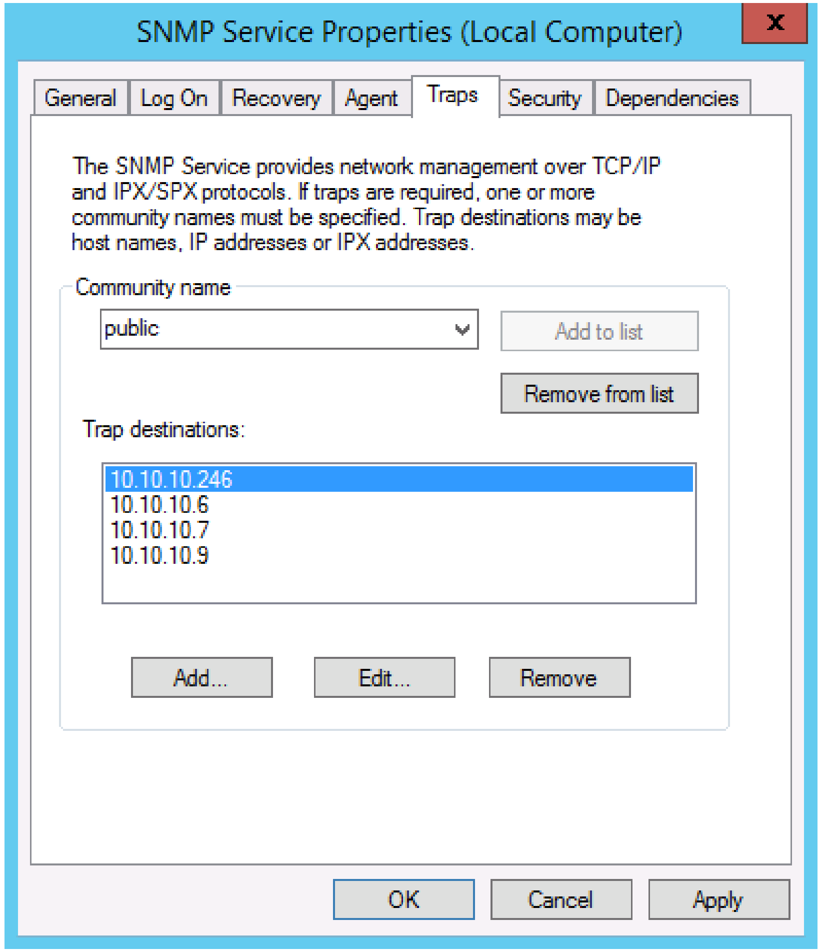
1 Under "Start | Settings | Control Panel | Software | Add/Remove Windows Components", open the Windows components installation.

2 Select "Management and Monitoring Tools".
Click on "Next>".

3 Select "WMI SNMP Provider" in the "Management and Monitoring Tools" window.

4 Confirm the installation with "OK".
Once the installation is complete, two new services (SNMP Trap Service and SNMP Service) will appear.

5 You can define the destination for the SNMP traps on the "Traps" tab in the SNMP Service Properties dialog box.



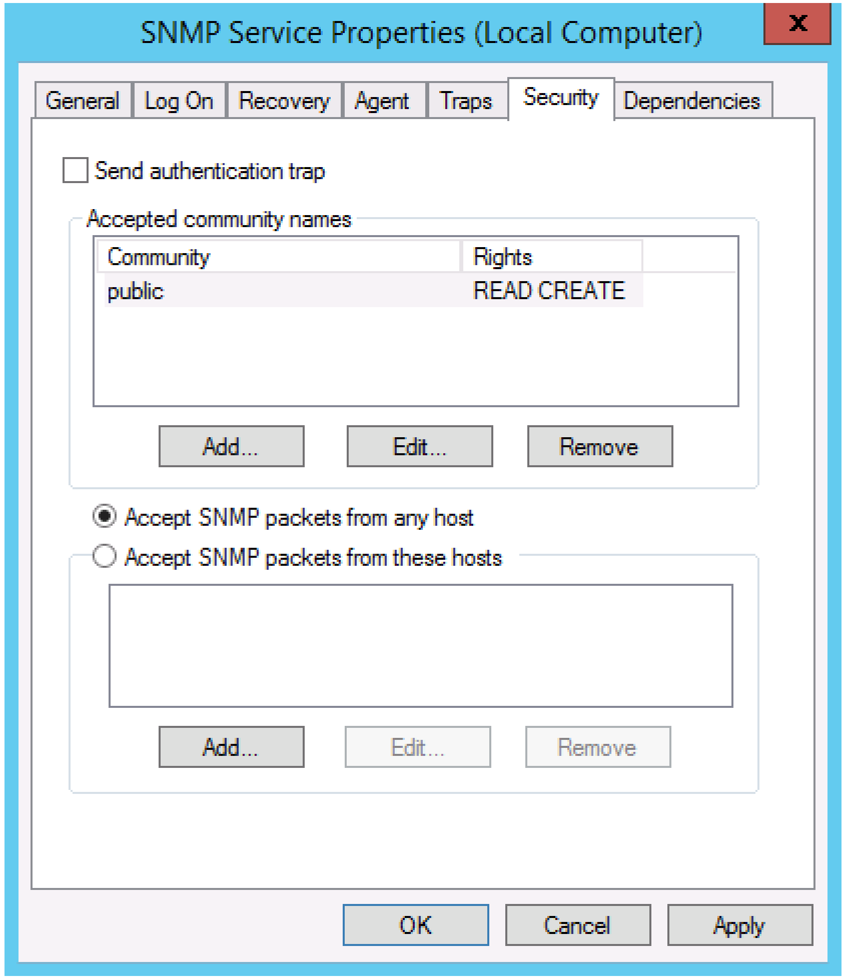
SNMP Service Properties (Local Computer)

The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.

Community name: public

Trap destinations:
10.10.10.246
10.10.10.6
10.10.10.7
10.10.10.9

6 Add "public" to the list under "Accepted community traps" on the "Security" tab.



□ Send authentication trap

Accepted community names

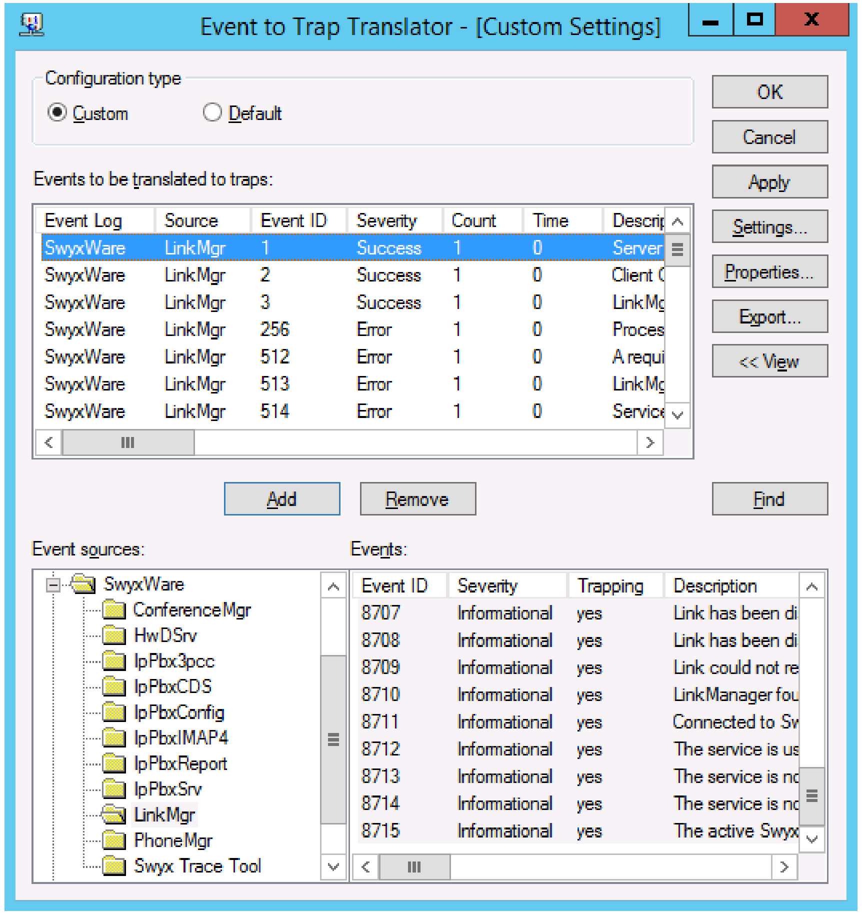
Community	Rights
public	READ CREATE

● Accept SNMP packets from any host

○ Accept SNMP packets from these hosts

7 Then restart the Microsoft SNMP service.

8 You can then use 'evntwin' to select the entries to be generated in the Traps event log. In the example below, in addition to the entries in the event log, traps from SwyxLinkManager are generated every time.



Configuration type

● Custom ○ Default

Events to be translated to traps:

Event Log	Source	Event ID	Severity	Count	Time	Descrip
SwyxWare	LinkMgr	1	Success	1	0	Server
SwyxWare	LinkMgr	2	Success	1	0	Client (
SwyxWare	LinkMgr	3	Success	1	0	LinkMg
SwyxWare	LinkMgr	256	Error	1	0	Proces
SwyxWare	LinkMgr	512	Error	1	0	A requi
SwyxWare	LinkMgr	513	Error	1	0	LinkMg
SwyxWare	LinkMgr	514	Error	1	0	Service

Event sources:

- SwyxWare
  - ConferenceMgr
  - HwDSrv
  - IpPbx3pcc
  - IpPbxCDS
  - IpPbxConfig
  - IpPbxIMAP4
  - IpPbxReport
  - IpPbxSrv
  - LinkMgr
  - PhoneMgr
  - Swyx Trace Tool

Events:

Event ID	Severity	Trapping	Description
8707	Informational	yes	Link has been di
8708	Informational	yes	Link has been di
8709	Informational	yes	Link could not re
8710	Informational	yes	LinkManager fou
8711	Informational	yes	Connected to Sv
8712	Informational	yes	The service is us
8713	Informational	yes	The service is nc
8714	Informational	yes	The service is nc
8715	Informational	yes	The active Swyx

SNMP READ

In your SNMP monitoring program, please use the MIB (Management Information Base) file provided (ippbx.mib) on the DVD under tools\SNMP to query the performance values of the SwyxWare via SNMP.

J.2 PERFORMANCE STATISTICS VIA THE WMI INTERFACE

SwyxWare provides what are known as performance counters via the Windows WMI interface. Currently, the following counters are available:

SwyxServer

- "Active Calls"
- "Active External Calls"
- "Active Internal Calls"
- "Calls"
- "Logged-in users"
- "SwyxIt!"
- "Conference Devices"
- "SwyxPhones"
- "H323 devices"
- "SIP devices"
- "Running Scripts"
- "Executed Scripts"
- "Scrip load time"
- "% script file cache hits"
- "% script file cache misses"
- "Script file cache size"
- "Gateway trunks"
- "Link trunks"
- "Trunks"
- "Client devices"
- "Workitem queue length"
- "Number of subscriptions"
- "Rejected registrations"
- "Rejected subscribtions"
- "Rejected calls"
- "Licenced users"
- "Licenced channels"
- "PBX config objects"
- "PBX config user objects"
- "PBX config status objects"
- "Script devices"
- "PBX script objects"
- "PBX script user objects"
- "PBX script call objects"

SwyxWare Trunk

- "Active Trunk Calls"
- "Trunk Calls"
- "% Channels used"
- "Trunk registered at server"
- "Active Trunk Calls Inbound"
- "Active Trunk Calls Outbound"

SwyxWare Location

- "Inter Location Call Limit"
- "Inter Location Calls"

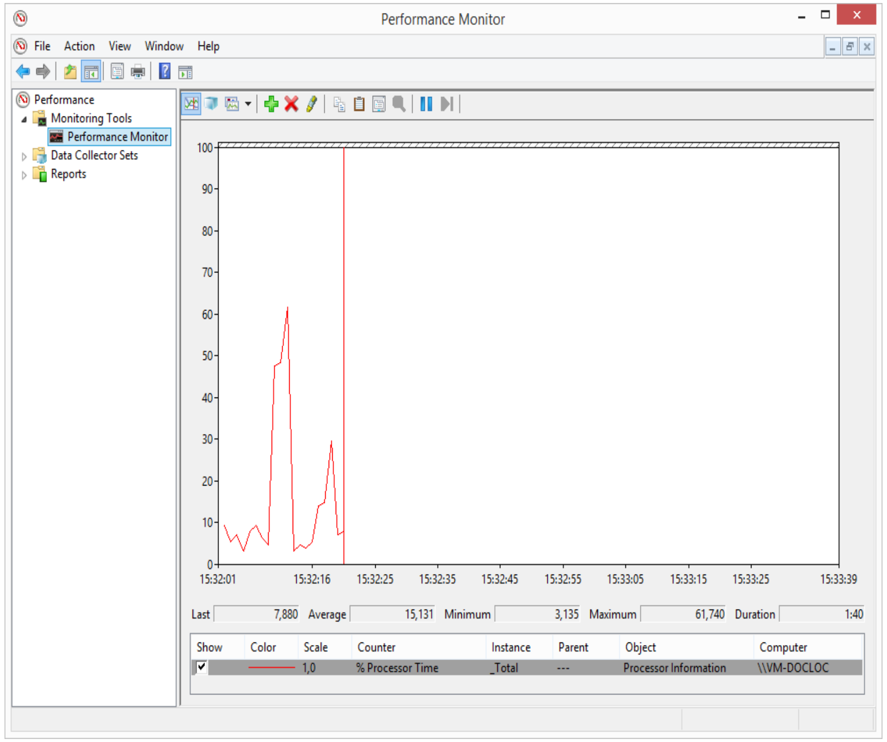
SwyxWare Diagnostics

"Objects"These counters can also be read via SNMP READ (JSNMP READ, Page 449).

How to query performance counters

1 In the command line, call the "Perfmon" Windows program.

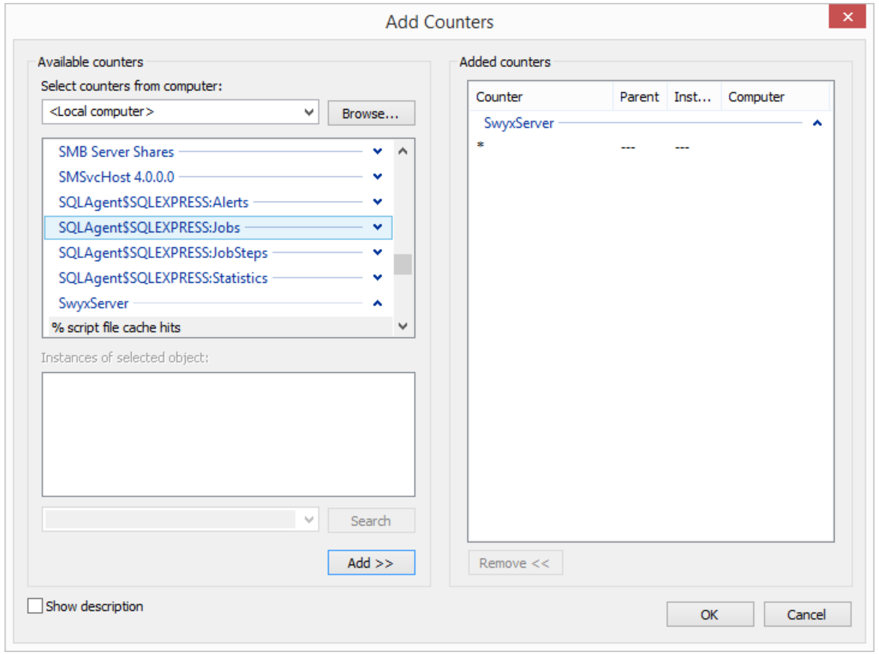
2 The "Performance" window will appear



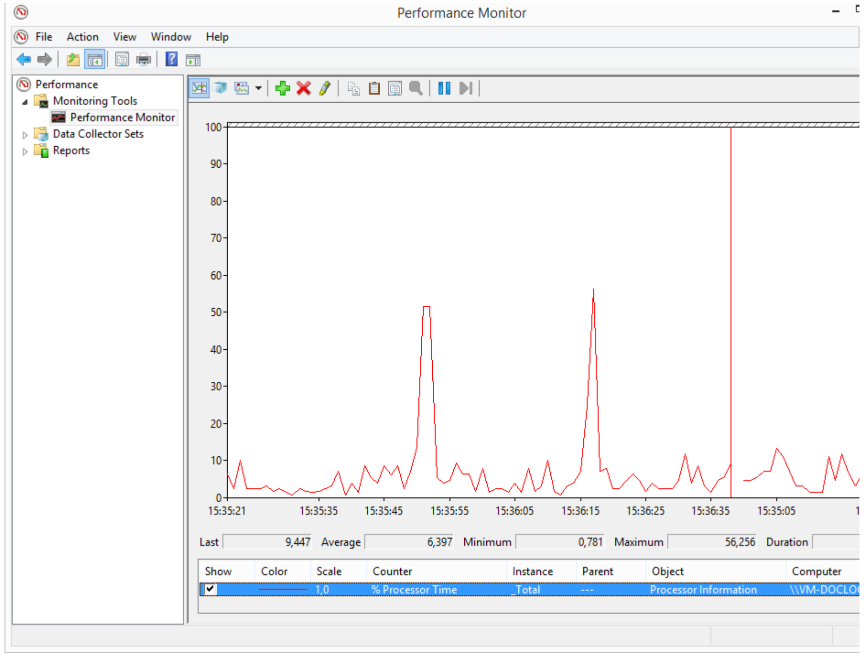
Last 7,880 Average 15,131 Minimum 3,135 Maximum 61,740 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑		1,0	% Processor Time	_Total	---	Processor Information	\\VM-DOCLOC

3 Click on the diagram (right-hand side of window) with the right mouse button and select "Add Counters...".



4 Select SwyxServer in the "Performance object" dropdown list and add the required counter.
The selected counters are added.



Last 9,447 Average 6,397 Minimum 0,781 Maximum 56,256 Duration

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	—	1,0	% Processor Time	_Total	---	Processor Information	\\VM-DOCLO

APP. K:DEVICES

In this appendix you will find information on the different devices (Handsets and Headsets), which are suitable for use with SwyxIt!.

All devices deliverable by Enreach are recognized automatically, as well as some devices from other manufacturers. For these devices, the optimal settings are automatically used.

K.1 OVERVIEW OF AVAILABLE DEVICES

With Swyx you can use different audio end devices which are either connected to a computer (via USB or Bluetooth) and used with SwyxIt! or which can be used stand-alone with SwyxWare.

- *Handsets*
- *Headset*
- *USB hands-free devices*
- *Desktop phones*
- *Conference Phones*
- *Wireless DECT phones*

For an overview of all supported third-party products, see here.

K.1.1 USB AUDIO DEVICES

Handsets

The handsets are connected to the USB port.

- Gigaset ION DECT UC Device

Headset

- Jabra Evolve 20 UC Mono/ Stereo
- Jabra Evolve 40 UC Stereo
- Jabra Evolve 65 UC Stereo
- Jabra Evolve 75 SE UC Stereo
- Jabra Evolve2 40
- Jabra Evolve2 65 Mono/ Stereo
- Jabra PRO 920
- Jabra PRO 930
- Jabra Engage 55 Mono/ Stereo
- Jabra Engage 65 Mono/ Stereo
- Jabra Engage 75 Mono/ Stereo

For more information, see here.

USB hands-free devices

- Jabra SPEAK2 55
- Jabra SPEAK2 75

K.1.2 DESKTOP PHONES

If a SwyxIt! is installed on the PC, it can be used to interact with a phone. You can easily configure your phone via SwyxIt!. Furthermore, you can use SwyxIt! directly to operate a phone. See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/phonecontrol_cti_$.

SwyxPhones

The following SwyxPhones are compatible with SwyxWare

Modell	Explanation/ Quickstart
SwyxPhone L62	help.enreach.com/docs/quickstarts/english/quickstart_SwyxPhoneL62.pdf
SwyxPhone L64	help.enreach.com/docs/quickstarts/english/quickstart_SwyxPhoneL64.pdf
SwyxPhone L66	help.enreach.com/docs/quickstarts/english/quickstart_SwyxPhoneL66.pdf
Key Module 64	Additional key module (with labeling templates) for expansion of SwyxPhone L64.

Modell	Explanation/ Quickstart
Key Module 66	Additional key module (with labeling templates) for expansion of SwyxPhone L66.
SwyxPhone L71	help.enreach.com/docs/quickstarts/english/Quickstart_SwyxPhone_L71.pdf
SwyxPhone L72	help.enreach.com/docs/quickstarts/english/Quickstart_SwyxPhone_L72.pdf
SwyxPhone L74	help.enreach.com/docs/quickstarts/english/Quickstart_SwyxPhone_L74.pdf
SwyxPhone L77	help.enreach.com/docs/quickstarts/english/Quickstart_SwyxPhone_L77.pdf
SwyxPhone Key Module 74	Key module with 16 keys for the SwyxPhone L74 (labeling template)
SwyxPhone Key Module 77	Key module with 2x12 keys for the SwyxPhone L77 (display)

Yealink Desk Phones

Modell	Documentation
Yealink SIP-T31G	help.enreach.com/docs/quickstarts/english/Quickstart_Yealink_T31G.pdf
Yealink SIP-T41S	help.enreach.com/docs/quickstarts/english/quickstart_Yealink_T41S.pdf
Yealink SIP-T42S	help.enreach.com/docs/quickstarts/english/quickstart_Yealink_T42S.pdf
Yealink SIP-T46S	help.enreach.com/docs/quickstarts/english/quickstart_Yealink_T46S.pdf
Yealink SIP-T48S	help.enreach.com/docs/quickstarts/english/quickstart_Yealink_T48S.pdf
Yealink SIP-T53(W)	help.enreach.com/docs/quickstarts/english/Quickstart_Yealink_T53_T53W.pdf
Yealink SIP-T54W	help.enreach.com/docs/quickstarts/english/Quickstart_Yealink_T54W.pdf
Yealink SIP-T57W	help.enreach.com/docs/quickstarts/english/Quickstart_Yealink_T57W.pdf

K.1.3 CONFERENCE PHONES

- Yealink CP920, to the quickstart
- Yealink CP925, to the quickstart
- Yealink CP960, to the quickstart
- Yealink CP965, to the quickstart

K.1.4 WIRELESS DECT PHONES

The prerequisite for using the DECT handsets is compatible DECT base stations in the areas where reachability is to be enabled.

SwyxDECT 500

- SwyxDECT 500 Base station
- SwyxDECT 500 Repeater
- SwyxPhone D510
- SwyxPhone D565
- Desktop charger

SwyxDECT 800

- SwyxDECT 800 Base station (Ascom BS330 GAP/CAP), Power over LAN
- Mains power supply for the base station
- SwyxPhone D843, to the quickstart.
- SwyxPhone D863, to the quickstart.
- SwyxPhone D881, to the quickstart.
- SwyxPhone D883

Enreach DECT 600

DECT 600 components can be used in a backward compatible way with a SwyxDECT 500 system in the context of a replacement purchase under certain circumstances.

- Enreach DECT 600 L base station, to the manual.
- Enreach DECT 600 S base station, to the manual.
- Mains power supply for the base station: DECT BS 600 power supply unit
- SwyxPhone D510 and SwyxPhone D565 with Compatibility Pack, see service.swyx.net/hc/en/articles/4801820497948.
- DECT HS 630 Handset
- DECT HS 650 Handset
- DECT HS 670 Handset
- DECT R 600 Repeater

K.2 CONFIGURATION OF THE TERMINAL DEVICES IN SWYXIT!

Most of the terminal devices can be configured in SwyxIt!.

Configuration of the Output

You can specify which terminal device should be used on the PC in the local settings for SwyxIt! (menu "Settings | Local Configuration", on the "Audio Mode" tab). Here, you can specify different devices for:

- the audio mode "Handset",
- the audio mode "Headset",
- the audio mode "Handsfree",
- the option "Open listening" and
- the output of the ringing tone.

See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/configure_audio_settings_$.

Configuration of SwyxPhone Lxxx

The configuration of a SwyxPhone Lxxx can be carried out easily using SwyxIt!. While doing so, you can

- define the phone buttons and
- assign the phone buttons (e.g. with phone numbers).

See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/configure_buttons_swyxphone_$.

Configuration of Call Signaling

A user status (available, away, speaking, logged off) can be signaled to other users.

If several terminal devices (SwyxIt!, SwyxPhone, SIP device) are logged on under the same user account, you can indicate which type of terminal device should signal the status of the user.

See also help.enreach.com/cpe/latest.version/Client/Swyx/en-US/index.html#context/help/status_signaling_$.

Use of a Headset with a SwyxPhone Lxxx

Frequent callers can connect a headset directly to a SwyxPhone Lxxx. If SwyxPhone Lxxx has a headset connection, you can configure its behavior in the user profile under the "SwyxPhone" tab. The following options are available:

- Option "Use SwyxPhone with headset" not activated
  If the handset is down, the hands-free functionality is enabled in case of an incoming call. In this case, the connected headset will not be activated until the Headset button on the phone is activated.
- Option "Use SwyxPhone with headset" activated
  The acoustic output of the phone is signaled through the headset connection. The handsfree phone is then activated by pressing the Speaker button on the phone.

K.3 TERMINAL DEVICES FROM THIRD PARTY MANUFACTURERS

You can also use other terminal devices from third party manufacturers in addition to the terminal devices supplied by Enreach. Because of the broad variety of availabel devices Enreach cannot ensure the interoperability.

K.3.1 SIP DEVICES

SIP Devices of SwyxWare are supported. The following supplementary services are offered:

- Outgoing Calls
- Incoming Calls
- Fax T.38
- Call Swap, active
  From the device it is possible to switch between an active call and a call on hold.
- Call Swap, passive
  The device can be put on hold by the conversation partner and activated once again.
- Call Forwarding, Unconditional
  The device calls another user, who then immediately forwards this call.
- Call forwarding, No reply
  The device calls another user, who then immediately forwards this call with a delay.
- Call Forwarding Busy
  The device calls another user, who then immediately forwards this call because the line is busy.
- Hold, active
  It is possible to put a call on hold from the device.
- Hold, passive
  The device can be placed on hold.
- Call Transfer, active
  You can transfer a call directly from the device.
- Blind Call Transfer, active
  You can conduct a blind transfer a call directly from the device.
- Call Transfer, passive
  The device can be transferred.
- Conference, active
  You can begin a conference directly from the device.
- Conference, passive
  The device can be added to a conference.
- Call Waiting
  An additional call can be signaled to the device (Call Waiting).
- Group Call
  The device can be a member of a group.
- Second Log On
  The device can be used as a second device (parallel operation).
- Sending and receiving DTMF tones
  It is possible to send or receive DTMF tones from the device. These are sent via SIP INFO (out-band) and are Cisco-compatible; RFC2833 and in-band in the RTP data stream are not supported by SwyxWare.

In case of issues with third party devices, please consult the third party manufacturer or the Swyx forum.

K.3.2 IP A/B ADAPTER

Adapter to connect analog devices (e.g. fax or DECT phones):

- AudioCodes MP 112 (2 SXS/AC/SIP-3)
- AudioCodes MP 118 (8 SXS/AC/SIP-3)
- AudioCodes MP 124 (24 S/AC/SIP)

APP. L: HIGH AVAILABILITY SOLUTION FOR SWYXWARE

Guidance on selecting a SwyxWare High Availability Solution

This document is intended to help you select the right High Availability solution for SwyxWare.

Target group

This document is intended for Enreach partners and administrators who are experts in the chosen virtualization technology. We expect them to have experience with SwyxWare at least beyond the usual Enreach partner certification. We assume that customers who use a SwyxWare HA solution have a professional IT department with experienced administrators who are familiar with the setup and maintenance of the chosen virtualization technology.

L.1 CONCEPT

In the following section, the most important terms on the subject of high availability are explained:

High Availability/Failover

A SwyxWare instance is available to users regardless of a hardware failure or application crash. Downtime should be as short as possible. The SwyxWare HA concept aims for a maximum downtime of a few minutes. Normally the downtime is much shorter, depending on the solution it can even be zero. In general, this approach automatically restores system availability.

Back-up

The SwyxWare installation and the corresponding data are backed up regularly so that a customer can restore a SwyxWare instance from a backup package. Back-ups are also part of an HA/Failover approach when longer downtimes are acceptable. System availability must be restored manually when backups are used.

Disaster Recovery

The entire infrastructure is destroyed at one location. The system is available from another location (geo-redundancy). Alternatively, if longer downtimes are acceptable, the system will be restored from a backup after restoring the infrastructure.

Downtime for update/maintenance

The downtimes of the SwyxWare instance during a software or operating system update are as short as possible.

If it is supported by the selected HA/Failover system, the downtime can be very short. In the SwyxWare HA concept up to 10 minutes are acceptable.

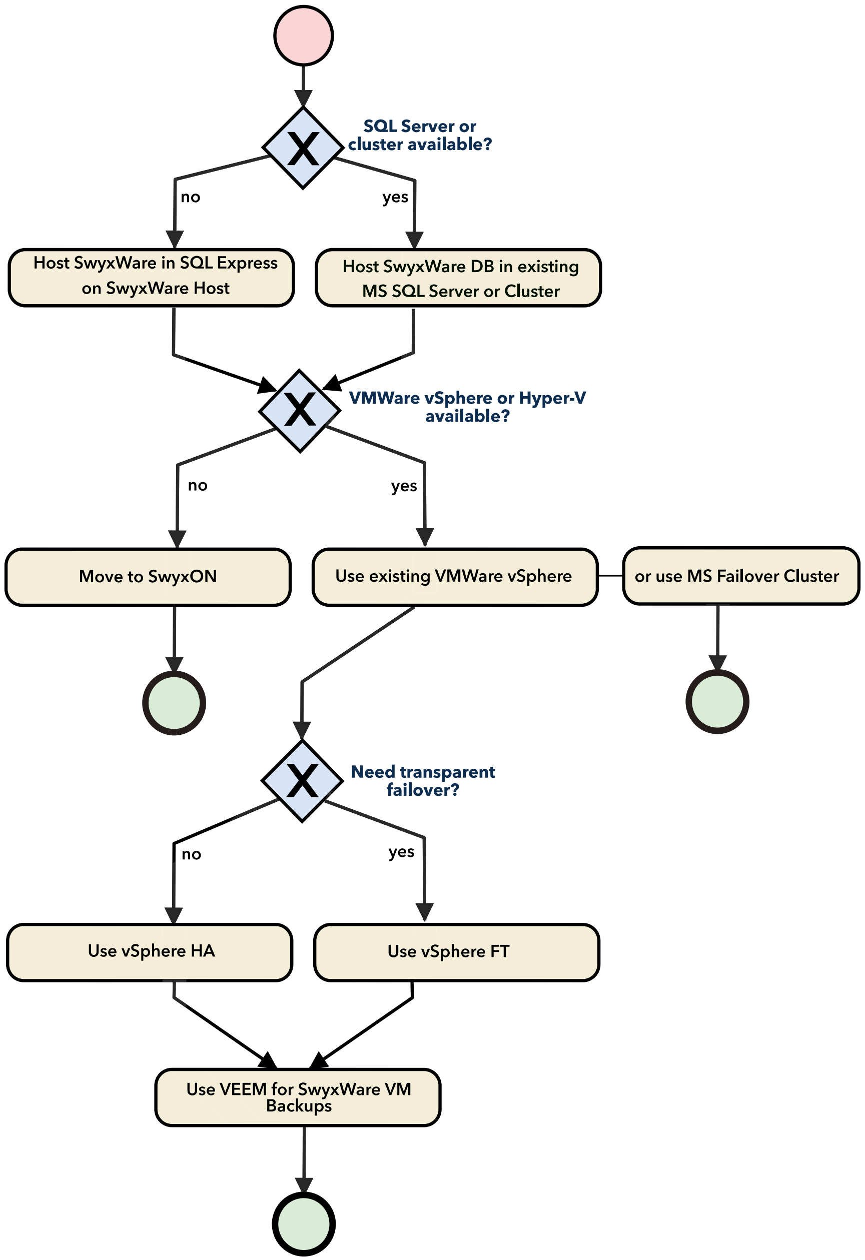
L.2 OPTIONS

With SwyxWare the following high availability solutions can be used:

vSphere HA	vSphere HA + FT	Microsoft Hyper-V Failover Cluster	SwyxON
SwyxWare runs in a VM with the database either in SQL Express or in an existing SQL Server or Cluster.	SwyxWare runs in a VM with the database either in SQL Express or in an existing SQL Server or Cluster.	SwyxWare runs in a VM with the database either in SQL Express or in an existing SQL Server or Cluster.	Customer uses SwyxON
HA/Failover vSphere HA	**HA/Failover** vSphere FT	**HA/Failover** MS Hyper-V Cluster	**HA/Failover** SwyxON
Back-up VEEAM VM Back-up	**Back-up** VEEAM VM Back-up	**Back-up** VEEAM VM Back-up	**Back-up** SwyxON
Disaster Recovery vSphere with geo-redundancy and backup	**Disaster Recovery** vSphere with geo-redundancy and backup	**Disaster Recovery** MS Hyper-V Cluster	**Disaster Recovery** SwyxON

vSphere HA	vSphere HA + FT	Microsoft Hyper-V Failover Cluster	SwyxON
Downtime Few minutes (depending on the virtualization structure and SwyxWare utilization)	Downtime Uninterrupted availability through VMWare Fault Tolerance	Downtime See MS Hyper-V Cluster documentation	Downtime See SwyxON SLA
Maintenance Downtime vSphere. Update in a separate VM. Some recorded data is lost, such as call journal entries created during the update period.	Maintenance Downtime vSphere. Update in a separate VM. Some recorded data is lost, such as call journal entries created during the update period.	Maintenance Downtime vSphere. Update in a separate VM. Some recorded data is lost, such as call journal entries created during the update period.	Maintenance Downtime SwyxON

The displayed decision tree should lead you to one of the following solution options:


SQL Server or cluster available?
no
yes
Host SwyxWare in SQL Express on SwyxWare Host
Host SwyxWare DB in existing MS SQL Server or Cluster
VMWare vSphere or Hyper-V available?
no
yes
Move to SwyxON
Use existing VMWare vSphere
or use MS Failover Cluster
Need transparent failover?
no
yes
Use vSphere HA
Use vSphere FT
Use VEEM for SwyxWare VM Backups

:

> You should use an existing virtualization-based high availability solution such as VMware vSphere to run SwyxWare in a virtual machine.
> If you do not have such a virtualization infrastructure, Enreach recommends its own SwyxON Cloud Service instead.

L.3 MIGRATION FROM THE STANDBY SCENARIO TO A VIRTUAL MACHINE

This section describes how to migrate an existing SwyxWare Master/ Standby installation to a virtual machine to make it highly available through appropriate virtualization platform features.

After this migration, the availability of SwyxWare is no longer realized by switching from a master to a standby system, but by a VM restart (vSphere HA) or a seamless switch to a mirrored VM (VSphere FT).

The migration can be carried out in the following steps:

1. *Converting a Master SwyxWare to a Single System*
2. *Create a Back-up of SwyxWare data base*
3. *Reinstall SwyxWareon a virtual machine and back-up it*

L.3.1 CONVERTING A MASTER SWYXWARE TO A SINGLE SYSTEM

1. Open SwyxWare Administration, Server Properties and make sure that the master system is passive.
2. Stop the "SwyxWare" service on the master system.
3. Convert the master system to a stand-alone SwyxServer, see *23.1 Convert Master or Standby System to a Stand-alone System*, Page 358

L.3.2 CREATE A BACK-UP OF SWYXWARE DATA BASE

Make sure that the MS SQL Server service has write permissions in the directory where you store the backup.

1. To create a backup, run the following command:

```
ippbxconfig.exe /backup /file:<BackupfilepfadUndName>
```

✓ A backup of the SwyxWare database is created by MS SQL Server and stored in the location you specified under "/file:".

L.3.3 REINSTALL SWYXWAREON A VIRTUAL MACHINE AND BACK-UP IT

1. Install SwyxWare, as a single system in a virtual machine, see *5 SwyxWare Installation*, Page 47
   In the configuration wizard, you do not create a new database, but restore the backup you created in the last step.
2. Continue with SwyxWare HA 2.0 - Installing and running a SwyxWare with VMware vSphere to configure the VM in vSphere.

L.4 INSTALLATION AND OPERATION OF A SWYXWARE WITH VMWARE VSPHERE

This section describes how to install and run SwyxWare in the vSphere virtual machine and make it highly available with vSphere.

SwyxWare is installed complete with a SQL Server Express in a virtual machine. Alternatively, SwyxWare can be installed without SQL Express and the database can be run on an existing SQL Server cluster.

vSphere High Availability and vSphere Fault Tolerance

VMware vSphere offers various functions to make virtual machines highly available:

- vSphere High Availability and vSphere Fault Tolerance

monitors the VM and the application running in it and restarts the VM if the operating system or application in the VM stops responding.

- vSphere Fault Tolerance

maintains a constantly updated copy of the virtual machine on a second host and automatically switches to the copy if one host fails.

For more information, see the vSphere documentation: docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.avail.doc/GUID-63F459B7-8884-4818-8872-C9753B2E0215.html

SwyxWare HealthMonitor

So that vSphere can monitor not only the VM but also the SwyxWare running in it, install the SwyxWare HealthMonitor service in addition to SwyxWare. This monitors the SwyxWare services and uses the vSphere Heartbeat interface. If all SwyxWare services are available, the Health-Monitor sends a "Heartbeat" every twenty seconds via the vSphere Heartbeat interface. If one of the services stops responding, the heartbeat fails. vSphere uses the failure of the heartbeat to detect a nonresponding application and restart the VM.

In addition, you should always combine a vSphere HA/FT solution with a VM backup solution.

L.4.1 INSTALLING SWYXWARE IN A VIRTUAL MACHINE

To create a virtual machine, refer to the vSphere documentation for details: docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-55238059-912E-411F-A0E9-A7A536972A91.html

The dimensioning of the VM should be done as for a normal SwyxWare installation based on the known Windows Server and SwyxWare hardware requirements.

We recommend to keep the number of vCPUs and the RAM low at the beginning, to observe the VM in operation with vSphere means and to adjust vCPUs and RAM accordingly to get optimal values.

The installation of SwyxWare in a VM is no different from the installation on physical hardware, see *5 SwyxWare Installation*, Page 47SwyxWare Installing HealthMonitor

L.5 INSTALLATION AND OPERATION OF A SWYXWARE WITH MICROSOFT HYPER-V FAILOVER CLUSTER

This section describes how to install and run SwyxWare in a Hyper-V virtual machine.

SwyxWare is installed complete with a SQL Server Express in a virtual machine. Alternatively, SwyxWare can be installed without SQL Express and the database can be run on an existing SQL Server cluster.

Microsoft Hyper-V Failover Cluster

Microsoft offers several features to make virtual machines highly available.

For more information, see the vSphere documentation: docs.microsoft.com/en-us/windows-server/failover-clustering/failover-clustering-overview

SwyxWare HealthMonitor

To enable Hyper-V to monitor not only the VM, but also the SwyxWare running in it, install the SwyxWare HealthMonitor service in addition to SwyxWare. This monitors the SwyxWare services and operates the Hyper-V application health monitoring interface, and transmits the status via the Hyper-V clock integration services (Heartbeat Integration Services) to Hyper-V. This state information can be used by Microsoft's failover cluster, for example to restart the VM.

Additionally, you should always combine a Hyper-V solution with a VM backup solution.

L.5.1 INSTALLING SWYXWARE IN A VIRTUAL MACHINE

To create a virtual machine, refer to the vSphere documentation for details: docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/create-a-virtual-machine-in-hyper-v

L.6 CONFIGURING THE SWYXWARE HEALTHMONITOR

The SwyxWare HealthMonitor is a Windows service that must be installed separately in the VM. This section describes the installation and configuration of this service.

1 Download the ZIP file of the HealthMonitor service from the Swyx website enreach.com/products/support/support-downloads.html

2 Run the Windows PowerShell console as an administrator.

3 Create a directory under %program files%:

```
mkdir "$env:ProgramFiles\Swyx.Core.HealthMonitor"
```

4 Extract the HealthMonitor files to this directory:

```
Expand-Archive -Path Swyx.Core.HealthMonitor.zip -
DestinationPath
"$env:ProgramFiles\Swyx.Core.HealthMonitor"
```

5 Change to the directory where you unpacked the files and install SwyxWare HealthMonitor with one of the following commands:
For use with VMware vSphere

```
./install-service.ps1
```

For use with Hyper-V Failover Cluster

```
./install-service.ps1 -EnableHyperVSupport
```

The parameter "-EnableHyperVSupport" configures the SwyxWare HealthMonitor service to run with local administration rights. This is necessary because Microsoft Windows only allows administrators to use Hyper-V Heartbeat Integration Services interface.

The installation script has some optional parameters to customize the installation. In most cases, the default settings are sufficient. You can get a description of the options with the normal PowerShell help function:

```
get-help ./install-service.ps1 -full
```

6 Adjust the configuration of the service as described in the next section before starting the service.

As of SwyxWare Health Monitor 1.2 the steps in this section can be omitted for standard setups, because the file "appSettings.json" is adjusted automatically by the installation script.

1 Open the configuration file "appSettings.json" in a text editor.

2 Make sure that VSphereHeartbeat is set to "true".

3 Remove the comment characters (//) in front of the lines in the "Probes" section.

4 Replace in all "destination" lines the target "sip://example.com" with "sip://<server-ip>". "<server-ip>" is the IP address of SwyxServer.
If you have an installation with multiple network interfaces and the SwyxWare services are fixed to one of the interfaces (see *Network card(s)*, Page 40), use the IP address of that interface. If you use the machine name instead of the IP address, HealthMonitor will use the

first IP address provided by Windows for the machine name and not necessarily the fixed one configured in SwyxWare.

5. Make sure that there is an entry in the probes list in the "appSettings.json" for each installed SwyxWare service. If you have not installed a service, also remove it from the Probes list.

Services that are monitored via HTTP instead of SIP have an HTTP instead of SIP URL in the "appSettings.json" file at "destination". If the service does not have a verifiable TLS certificate, you can disable the HealthMonitor TLS certificate check for monitoring. To do this, add the setting "skipTlsCheck": "false".

The installation script adjusts the service restart options of the SwyxWare services in Windows. A SwyxWare service that stops unexpectedly is restarted only once by Windows. The installation script only adjusts the services configured in "Probes" in appSettings.json. Therefore, run the installation script again when you add or remove probes.

The following example shows a typical configuration for a server with IP 10.0.0.1:

```
{
  "HealthMonitorApp": {
    "Prometheus": false,
    "VSphereHeartbeat": true
    "HyperVHeartbeat": false
  },
  "Probes": [
    {
     "Name": "server",
     "Type": "Network",
     "Configuration": {
       "destination": "sip://10.0.0.1:5060",
       "probingIntervalSeconds": 10,
       "responseTimeoutMilliseconds": 5000
     }
    },
    {
     "Name": "uaCSTA",
     "Type": "Network",
     "Configuration": {
       "destination": "sip://10.0.0.1:65012",
       "probingIntervalSeconds": 10,
       "responseTimeoutMilliseconds": 500
     }
    },
    {
     "Name": "linkmgr",
     "Type": "Network",
     "Configuration": {
       "destination": "sip://10.0.0.1:65001",
       "probingIntervalSeconds": 10,
       "responseTimeoutMilliseconds": 500
     }
    },
    {
     "Name": "conferencemgr",
     "Type": "Network",
     "Configuration": {
       "destination": "sip://10.0.0.1:5062",
       "probingIntervalSeconds": 10
     }
    },
    {
     "Name": "phonemgr",
     "Type": "Network",
     "Configuration": {
       "destination": "sip://10.0.0.1:65007",
       "probingIntervalSeconds": 10
     }
    },
    {
     "Name": "swyxgate",
     "Type": "Network",
     "Configuration": {
       "destination": "sip://10.0.0.1:5064",
       "probingIntervalSeconds": 10
     }
    },
    {
     "Name": "ctiplus",
     "Type": "Network",
     "Configuration": {
       "destination": "sip://10.0.0.1:65009",
       "probingIntervalSeconds": 10
     }
    },
    {
     "Name": "faxserver",
     "Type": "Network",
     "Configuration": {
       "destination": "sip://10.0.0.1:61000",
       "probingIntervalSeconds": 10
     }
    },
    {
     "Name": "cds",
     "Type": "Network",
     "Configuration": {
       "destination": "https://10.0.0.1:9100/ippbx/
client/v1.0/login/systemhealth",
       "probingIntervalSeconds": 10,
       "responseTimeoutMilliseconds": 1000
     }
```

```
  }
],
"HealthRules": [
  {
    "ProbeName": "server",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 3
  },
  {
    "ProbeName": "uaCSTA",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
  },
  {
    "ProbeName": "linkmgr",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
  },
  {
    "ProbeName": "conferencemgr",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
  },
  {
    "ProbeName": "phonemgr",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
  },
  {
    "ProbeName": "swyxgate",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
  },
   {
    "ProbeName": "cds",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
   },
   {
    "ProbeName": "pns",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
   },
   {
    "ProbeName": "faxserver",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
   },
   {
    "ProbeName": "ctiplus",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
   },
   {
    "ProbeName": "ctiplus",
    "MetricName": "swyx_number_of_failed_probes",
    "LessThanOrEqual": 2
   }
  ],
  "Serilog": {
   "MinimumLevel": {
    "Default": "Information"
   },
   "WriteTo": [
    {
     "Name": "Console",
    "Args": {
     "outputTemplate":
      "{Timestamp:dd HH:mm:ss.fff} {Level:u4}
{ThreadId} {SourceContext}
{Message}{NewLine}{Exception}",
     "theme":
"Serilog.Sinks.SystemConsole.Themes.AnsiConsoleTheme::
Code, Serilog.Sinks.Console"
    }
   },
   {
    "Name": "File",
    "Args": {
     "path":
"C:\\ProgramData\\Swyx\\Traces\\Swyx.Core.HealthMonito
r.txt",
     "rollingInterval": "Day",
     "retainedFileCountLimit": 7,
     "outputTemplate":
      "{Timestamp:dd HH:mm:ss.fff} {Level:u4}
{ThreadId} {SourceContext,-50}
{Message}{NewLine}{Exception}"
    }
   }
  ],
  "Enrich": ["FromLogContext", "WithThreadId"]
 },
 "AllowedHosts": "*"
}
```

L.6.1 CONFIGURATION OF THE SWYXWARE SERVICES

For a default installation of SwyxWare, Windows is configured to automatically restart SwyxWare services from Windows when they unexpectedly stop.

The HealthMonitor installation script changes this configuration for all SwyxWare services monitored by HealthMonitor as follows:

Service Error	HealthMonitor not installed	HealthMonitor installed
1st Service Failure	Service is restarted	Service is restarted
2nd Service Failure	Service is restarted	No action
Subsequent service outages	Service is restarted	No action

This setting causes a SwyxWare service that stops unexpectedly to be restarted once by Windows. If a service is terminated more than once, it will not be restarted. The HealthMonitor detects the missing response of the service and stops the VMWare Heartbeat so that the VM is restarted.

If, in your deployment scenario, restarting a service takes longer than the HealthMonitor monitoring threshold, adjust the HealthMonitor configuration accordingly:

1 Open the configuration file "appSettings.json" in a text editor.

2 In the "HealthRules" section, find the entry for the service which monitoring you want to customize.

3 Increase the value "LessThanOrEqual" so that "probingIntervalSeconds" of the service (see configuration of the service in the section "Probes" in the "appSettings.json" file) multiplied by "LessThanOrEqual" is smaller than the value, the service needs for restarting.

Example:

The service is queried every 10 seconds (probingIntervalInSeconds=10). If more than 2 queries remain without a response (LessThanOrEqual=2), the service has less than 30s to restart.

> If you add services to SwyxWare, run the HealthMonitor installation script again to adjust the restart configuration of the new service accordingly. Alternatively, you can manually customize the restart options using the Windows Services Manager.

L.6.2 START HEALTHMONITOR

During installation, the service is set to "Start automatically", but is not started immediately. Start it using the Windows Service Manager or the command:

```
start-service Swyx.Core.HealthMonitor
```

L.6.3 CHECK INSTALLATION

To check whether the installation of SwyxWare and the HealthMonitor was successful, you can carry out the following steps:

1 In the Windows Service Manager, check that all SwyxWare services are running. Alternatively, you can use this PowerShell command to do this:

```
get-service | where-object { $_.Displayname -match
"Swyx" -and $_.StartType -match "Auto" } | format-table
Status, Name, DisplayName
```

2 Make sure VMWare in vSphere vCenter receives the Heartbeat from SwyxWare.

In operation

Set HealthMonitor

The default settings of the HealthMonitor should be appropriate in most cases. The HealthMonitor checks the SwyxWare services by sending a "SIP Options" or "HTTP Request" every 10 seconds to each SwyxWare service and waiting for a response for 500ms. You can adjust both the interval and the waiting time for each service. To do this, set the following values for the corresponding service in the "appSettings.json" file:

```
        "probingIntervalSeconds": 10,
        "responseTimeoutMilliseconds": 500
```

Restart the HealthMonitor service once to make the changes effective.

Back-up/Restore via VEEAM

For details on backing up and restoring virtual machines using VEEAM, see: https://www.veeam.com

If you have installed SwyxWare HealthMonitor and are using the Heartbeat in VMWare vSphere or Hyper-V for monitoring, make sure to stop the HealthMonitor service BEFORE you have to stop the SwyxWare services e.g. for maintenance purposes. The HealthMonitor logs off from vSphere or Hyper-V when the service is stopped, so vSphere or Hyper-V no longer expects heartbeats.

L.7 MONITORING WITH GRAFANA AND PROMETHEUS

You can use various interfaces to monitor SwyxWare:

- Windows Performance Counter
  SwyxWare offers various Windows Performance Counters, which you can query via the Windows Performance Counter interface or via Windows Management Instrumentation.
- Prometheus
  SwyxWare HealthMonitor optionally offers an interface that can be queried and stored by a Prometheus server (https://prometheus.io). To visualize this data e.g. on a dashboard Grafana can be used (https://grafana.com) or tools of your choice that support Prometheus.

The current section describes how to add a Grafana dashboard to SwyxWare.

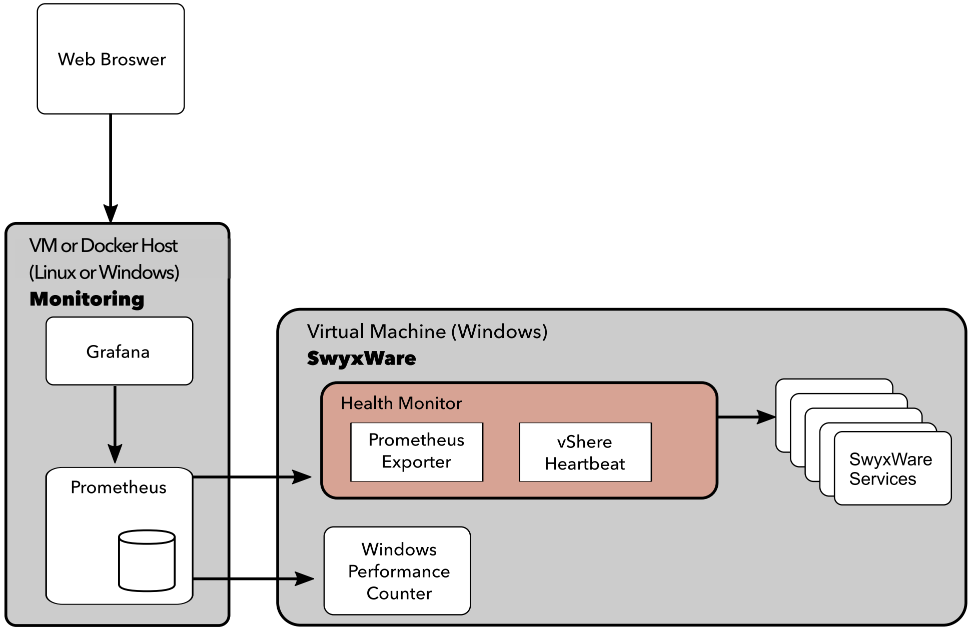
L.7.1 CONCEPT

For monitoring, SwyxWare HealthMonitor provides the "Prometheus Exporter" interface. The Prometheus Exporter provides the "health status" of SwyxWare as determined by the HealthMonitor, as well as some other parameters, such as the response times of individual checks.

Prometheus queries the Prometheus Exporter at regular intervals, e.g. every 10 seconds, and stores the delivered metrics in a time series database. You can configure the query time.

In order to be able to include other data in the Prometheus database, such as the Windows Performance Counter of SwyxWare, you can use another open source component "sonar-perfmon": https://www.infragravity.com/knowledge-base/sonar-023-install-windows-host/. This is also a Prometheus Exporter.

With Grafana, you can query the data stored in the time series database and visualize it on the dashboard:



If you are already using another monitoring system instead of Prometheus, you can also use this if it can query Prometheus Exporter. Zabbix also supports the Prometheus interface: https://www.zabbix.com/documentation/4.4/manual/config/items/itemtypes/prometheus

L.7.2 INSTALLATION

Since both Grafana and Prometheus have their roots in the Linux world, we recommend using the Linux versions of both services. The following explains how you can easily run Grafana and Prometheus as Linux Docker Container.

Information on a direct installation under Windows can be found in the respective documentation on the Grafana and Prometheus homepages. The sample dashboards provided with the HealthMonitor also work with the Grafana Windows version.

Please observe the following sequence during installation:

1 *Install Docker*
2 *Customize configuration files*
3 *SwyxWare Configure Core HealthMonitor*
4 *Grafana and Prometheus launch*
5 *Optional: install sonar-perfmon exporter*
6 *Install SwyxWare HealthMonitor Grafana Dashboard (as an example)*
7 *Check Installation*

L.7.3 INSTALL DOCKER

1 For information on the insallation of Docker on Linux, please refer to the official instructions: https://docs.docker.com/install/

2 Make sure that "docker-compose" is also installed.

On an Ubuntu-Linux for example with

```
apt-get install docker-compose
```

L.7.4 CUSTOMIZE CONFIGURATION FILES

Before you can use Grafana and Prometheus you have to configure in the Prometheus configuration how to reach the SwyxWare Core HealthMonitor.

The directory "Monitoring" is part of the SwyxWare Core HealthMonitor file package.

1 Copy the contents of the "Monitoring" directory to the Linux VM where you have set up Docker.

2 Open "Monitoring/prometheus/prometheus.yml" in a text editor and search for the "SwyxWare Job":

```
# Swyx.Core.HealthMonitor
 - job_name: "SwyxWare"
  static_configs:
  - targets:
   - <swyxware ip>:5000
```

3 Replace <swyxware ip> with the IP address of the SwyxServer.

4 If you have configured the HealthMonitor on a port other than 5000, adjust it accordingly.

5 If you want to monitor multiple SwyxWare systems, add each in a separate line below "targets".

Example:

```
# Swyx.Core.HealthMonitor
 - job_name: "SwyxWare"
  static_configs:
  - targets:
   - 10.0.0.1:5000
   - 10.0.0.2:5000
```

6 If you want to monitor Windows performance counters and therefore install "sonar-perfmon" (see below), remove the comment characters of the "sonar" job and enter the IP address and the "sonar-perfmon" port of the SwyxWare system there as well:

```
# sonar-perfmon windows performance counter
  - job_name: sonar
    static_configs:
    - targets:
      - 10.0.0.1:5001
```

7 Save the file.

The supplied configuration sets port 3000 for Grafana. If you want to use a different port, change "docker-compose.yml" as follows:

8 Open "Monitoring/docker-compose.yml" with a text editor.

9 To set the port to 8080, for example, change the port configuration for the Grafana service from

```
- "3000:3000"
```

to

```
- "8080:3000"
```

10 In the delivery state of the docker-compose.yml file, the Prometheus service is configured so that it is only accessible from the Grafana container, not from the host and not from other systems.

11 If you want to access the Prometheus web interface e.g. for troubleshooting, add a "Ports:" definition in the file.

Example:

```
ports:

  - "9090:9090"
```

L.7.5 SWYXWARE CONFIGURE CORE HEALTHMONITOR

The standard installation of SwyxWare Core HealthMonitor only provides the Prometheus metrics on localhost. In this step, you adjust the configuration to make the Prometheus interface accessible from the monitoring system.

1 On the SwyxWare system, open the PowerShell console with administrator privileges and change to the SwyxWare Core HealthMonitor installation directory.

2 Call up the installation script again and specify the ListeningUrls parameter:

```
.\install-service.ps1 -ListeningUrls "http://*:5000" -
StartAfterInstallation
```

✓ This configures the service so that it provides the Prometheus interface on all its own IP addresses on port 5000.

3 Configure an exception in the Windows firewall

```
netsh advfirewall firewall add rule
name="Swyx.Core.HealthMonitor" dir=in action=allow
protocol=TCP localport=5000 remoteip=<ip-monitoring>
```

Replace <ip-monitoring> with the IP address of the monitoring system. If you do not want to restrict the accessibility of the Prometheus interface, omit the "remote-ip" parameter.

L.7.6 GRAFANA AND PROMETHEUS LAUNCH

To easily configure and start the Grafana and Prometheus containers, use "docker-compose".

1 Open the PowerShell console with administrator rights in the "Monitoring" directory.

2 Start the services with

```
docker-compose up -d
```

3 Check whether both services have been started.

```
docker container ls
```

✓ Two active containers are displayed.

4 Open "http://<monitoring-vm>:3000" in a web browser.
<monitoring-vm> is the computer name or IP address of your Linux system.

5 Log in as an administrator.
Default user name is "admin", password is "admin". Grafana prompts you to set a new, secure password for the admin user after logging in.
✓ Both containers are configured so that they are automatically restarted after a computer restart.

L.7.7 OPTIONAL: INSTALL SONAR-PERFMON EXPORTER

You can install and configure the sonar-perfmon exporter on the SwyxWare system so that Prometheus can also query and save Windows performance counters and you can visualize them on a Grafana dashboard. This also includes the values provided by SwyxWare via the Performance Monitor API.

In deviation from the sonar-perfmon installation instructions (https://www.infragravity.com/knowledge-base/sonar-023-install-windows-host/), we recommend not to run the sonar-perfmon service under the LOCALSYSTEM account, but to use an account with less rights.

This manual applies to sonar-perfmon 0.25:

1 Download sonar-perfmon, extract the ZIP file on the SwyxWare VM to c:\sonar.

If you use a different path, adjust it accordingly in the following steps.

2 Open a PowerShell with administrator rights.

3 Install the service:

```
sc.exe create sonard binpath= c:\sonar\out\Sonard.exe
start= auto obj= "NT AUTHORITY\LocalService" depend=
"WinRM"
```

4 Configure a service SID:

```
sc.exe sidtype sonard unrestricted
```

5 Give the service the necessary access rights to the installation directory:

```
icacls.exe C:\Sonar /grant "NT
Service\sonard:(OI)(CI)(M)"
```

6 Add the service account to the local group "Remote Management Users" so that the service can use the WMI interface:

```
Add-LocalGroupMember -Group "Remote Management Users" -
Member "nt service\sonard"
```

On older Windows systems on which "Add-LocalGroupMember" is not available, you can use "net.exe":

```
net localgroup "Remote Management Users" "NT
Service\sonard" /add
```

The group name depends on the Windows system language. Adjust the command line accordingly.
On a German-language Windows, use the group name "Remoteverwaltungsbenutzer" instead of "Remote Management Users" in this step.

7 In the file "c:\sonar\out\sonard.dll.config", adjust the path to the configuration (parameter "ConfigPath").
Set the parameter to "c:\Sonar\sonard.config". Set the "ExporterPort" on which the service provides the data to 5001.

> ⚠ Do not use port 5000, as this is already used by the HealthMonitor service.

The configuration file should look like this:

```
<?xml version="1.0"?>
<configuration>
  <configSections>
    <section name="Sonar"
type="Infragravity.Sonar.SonarConfigurationSection,
Sonar"/>
  </configSections>
  <appSettings>
    <add key="ConfigPath"
value="c:\Sonar\sonard.config"/>
    <add key="RuntimeType" value="Service"/>
    <add key="LogLevel" value="Information"/>
    <add key="LogPath" value="c:\Sonar\sonar.log"/>
    <add key="ExporterPort" value="5001"/>
    <add key="ExporterCacheMilliseconds" value="60000"/
>
    <add key="ExporterEnabled" value="true"/>
  <appSettings>
</configuration>
```

8. Release the port that you configured in the previous step in the Windows firewall:

   ```
   netsh advfirewall firewall add rule name="sonard"
   dir=in action=allow protocol=TCP localport=5001
   remoteip=<ip-monitoring>
   ```

   Replace <ip-monitoring> with the IP address of the monitoring system. If you do not want to restrict the accessibility of the Prometheus interface, omit the "remote-ip" parameter.
9. For a German-speaking Windows system, copy the file "sonard.de.config" from the directory "Monitoring/sonar-perfmon" to "c:\sonar\sonard.config".
10. For an English-speaking Windows system, copy the "sonard.en.config" file from the "Monitoring/sonar-perfmon" directory to "c:\sonar\sonard.config".
11. Start the sonar-perfmon service:

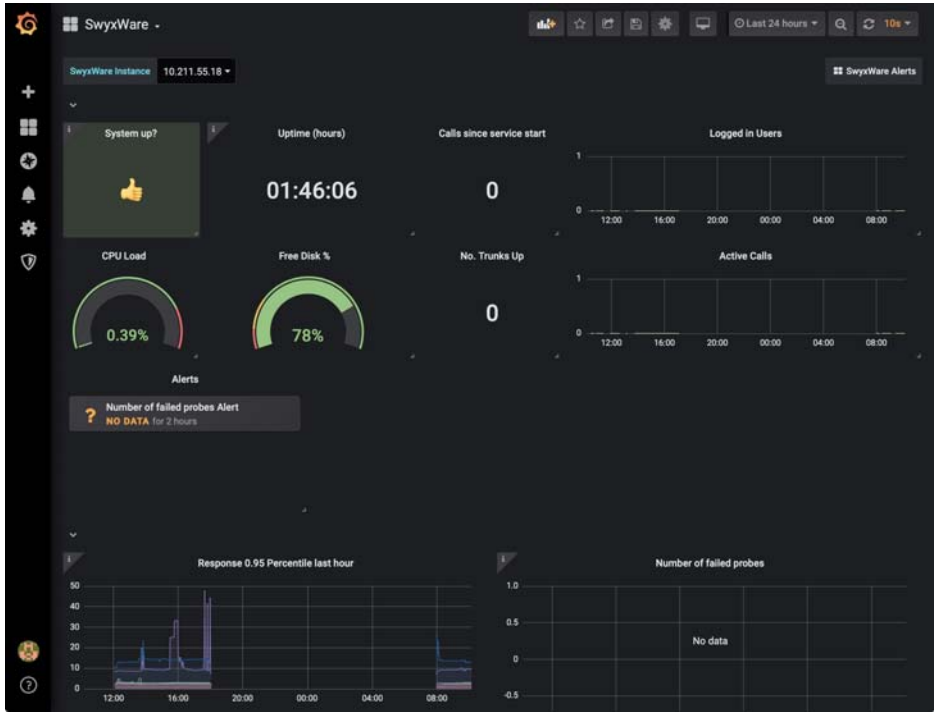
    ```
    start-service sonard
    ```

12. Open the page "http://localhost:5001/metrics" in a web browser.
    ✓ You should see a text output with all the metrics that are configured in "sonard.config".

L.7.8 INSTALL SWYXWARE HEALTHMONITOR GRAFANA DASHBOARD (AS AN EXAMPLE)

In the "Monitoring/grafana" directory you will find two ready-made dashboard templates that you can use as a starting point for configuring your own Grafana dashboards. To install these, proceed as follows:

1. Open the Grafana website in a web browser and log in.
2. Select "Manage Dashboards" from the navigation bar on the left.
3. Select "Import | Import json file".
4. Import the file "SwyxWare HealthMonitor Overview.json".
   ✓ Grafana displays a page with options.
5. Under "Select a prometheus data source", select "Prometheus" and click on "Import".
6. Repeat steps 3-5 for the file "SwyxWare HealthMonitor Alerts.json". This is a sample dashboard for a Grafana alarm that is triggered when HealthMonitor stops reaching a service.



For information on adjusting the dashboard and configuring notifications for alarms, see the Grafana documentation: https://grafana.com/docs/grafana/latest/.

L.7.9 CHECK INSTALLATION

1 Check that the Grafana and Prometheus containers are running. On the monitoring system, enter the following as administrator

```
docker container ls
```

ein.

✓ You should see two running containers (Prometheus and Grafana). In the Grafana container, the "Ports" column should contain

```
0.0.0.0:3000->3000/tcp
```

so that Grafana is accessible in your network.

2 Check whether Grafana is accessible and working:

- Open http://<monitoring-system>:3000 in a web browser. <monitoring-system> is the computer name or IP address of the monitoring system. You should see the Grafana login page.
- Log in with your admin account.

3 Verify that SwyxWare HealthMonitor is running in a PowerShell console on the SwyxWare system:

```
get-service Swyx.Core.HealthMonitor
```

✓ The service should have the status "Running".

4 Verify that Grafana can reach the Prometheus service and that Prometheus can query HealthMonitor and Sonar-Perfmon metrics:

- Navigate to the Explore page
- Select Prometheus as the data source.
- Enter swyx_response_time_milliseconds in the text field "Enter a PromQL Query". You should now see the response times of the individual SwyxWare services provided by HealthMonitor. If this is the case, the HealthMonitor is installed, running and providing data.
- For example, enter "win_logicaldisk_PercentFreeSpace. You should now see the free disk space metrics provided by the sonar-perfmon exporter. If this is the case, the HealthMonitor is installed, running and providing data.

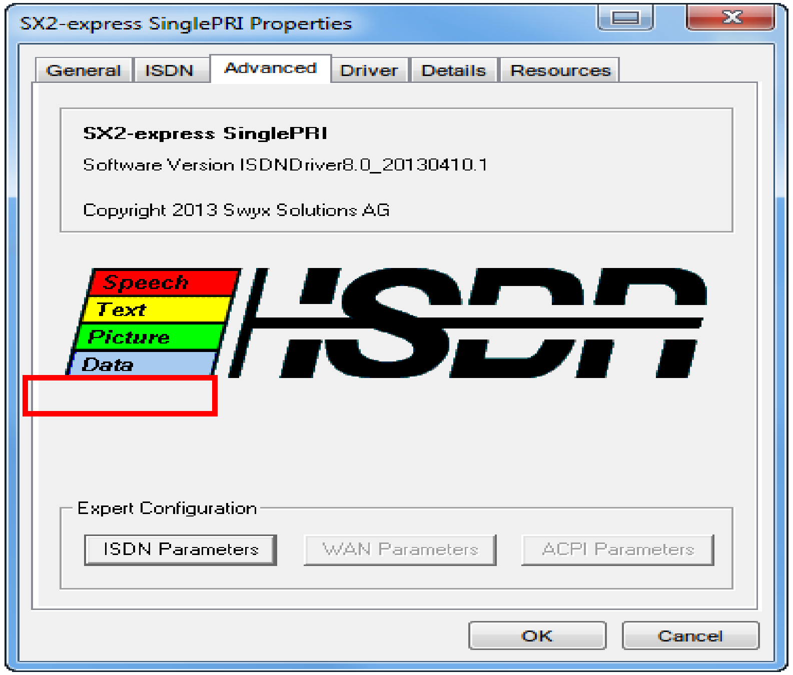
APP. M:CONFIGURATION OF THE ISDN DRIVER

This chapter describes the configuration options for the ISDN drivers.

For further information on ISDN connections and corresponding hardware installation, *15 ISDN connections*, Page 245.

The properties of an installed ISDN card can be called up under "Network adapter" in the Windows Device Manager.

Click with the right mouse button on the respective ISDN card and select "Properties".



SX2-express SinglePRI
Software Version ISDNDriver8.0_20130410.1

Copyright 2013 Swyx Solutions AG

M.1 SX2 ISDN CARD PROPERTIES

The following description contains the driver options for the complete product range of SX2 ISDN cards.

Thus, some options and menu items of certain ISDN cards may be missing or deactivated.

M.1.1 THE "ADVANCED" TAB

Expert configuration - ISDN parameters:

Click here to start the ISDN parameter configuration.

ISDN Parameters

Expert configuration - WAN parameters:

Click here to start the WAN miniport configuration.

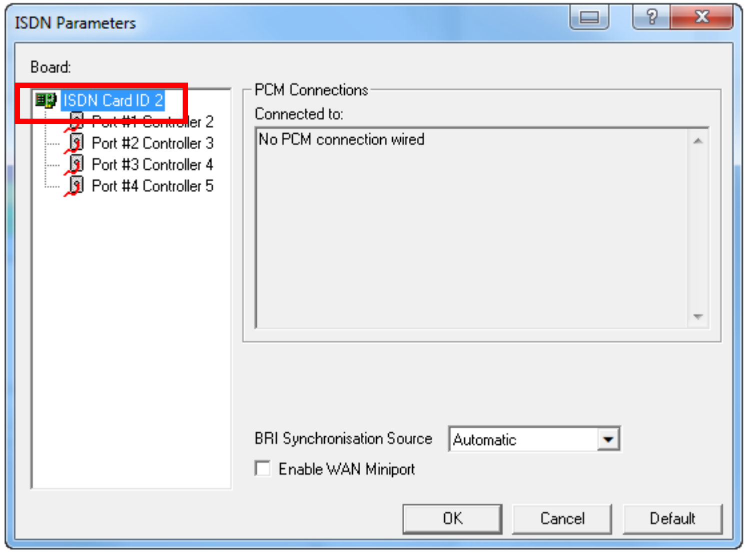
> ⚠ The "WAN parameter" button is deactivated by default. WAN parameters can only be configured, if WAN miniport is activated, *Activate WAN miniport:*, Page 473.

WAN parameter

Standard:

Resets all parameters to the original (factory) settings.

M.1.2 ISDN PARAMETERS



ISDN Parameters

Board:

ISDN Card ID 2
Port #1 Controller 2
Port #2 Controller 3
Port #3 Controller 4
Port #4 Controller 5

PCM Connections

Connected to:

No PCM connection wired

BRI Synchronisation Source: Automatic

☐ Enable WAN Miniport

Controller:

List of installed ISDN controllers, including all available lines.

BRI synchronization source (only for BRI cards):

In this list field, you can select the source for the clock synchronization. Instead of selecting automatic synchronization, you may also define one of the four ISDN interfaces as synchronization source.

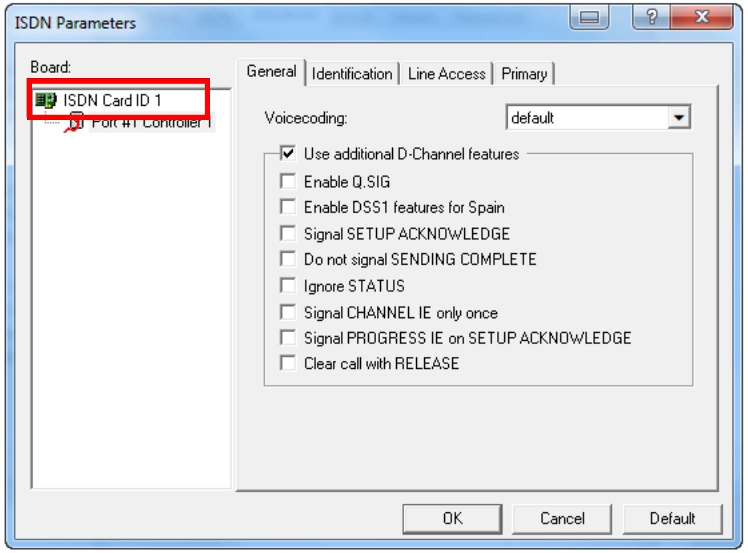
Activate WAN miniport:

Mark this checkbox, if you want to allow WAN access via the ISDN card, *M.1.3 WAN parameter*, Page 475

STOP

For security reasons, the WAN miniport is deactivated by default on SwyxWare ISDN cards. Only select this option, if a WAN access via the ISDN card is necessary.

M.1.2.1 THE "GENERAL" TAB



ISDN Parameters

Board:

ISDN Card ID 1
Port #1 Controller 1

Voicecoding: default

☑ Use additional D-Channel features

☐ Enable Q.SIG
☐ Enable DSS1 features for Spain
☐ Signal SETUP ACKNOWLEDGE
☐ Do not signal SENDING COMPLETE
☐ Ignore STATUS
☐ Signal CHANNEL IE only once
☐ Signal PROGRESS IE on SETUP ACKNOWLEDGE
☐ Clear call with RELEASE

Use the additional D channel function:

Mark this checkbox, if you need additional D channel settings for special telecommunication systems (PBXs) or countries.

Activate Q.SIG:

Allows connections between special telephone systems according to the QSIG protocol, which has been defined by the ECMA (European Computer Manufacturers Association).

Activate DSS1 functions for Spain:

Adjust the DSS1 protocol to specific ISDN requirements in Spain.

Signalize "setup acknowledge":

Allows the editing of this D channel information element, in order to adjust it to different telephone systems (PBXs).

Don't signalize "sending complete":

Allows the editing of this D channel information element, in order to adjust it to different telephone systems (PBXs).

Ignore STATUS:

Allows the editing of this D channel information element, in order to adjust it to different telephone systems (PBXs).

Signal CHANNEL IE only once:

Allows the editing of this D channel information element, in order to adjust it to different telephone systems (PBXs).

Signalize PROGRESS IE in SETUP ACKNOWLEDGE

Allows the editing of this D channel information element, in order to adjust it to different telephone systems (PBXs).

Disconnect with RELASE

Allows the editing of this D channel information element, in order to adjust it to different telephone systems (PBXs).

M.1.2.2 "IDENTIFICATION" TAB

Called Numbering Plan:

Defines, which "numbering plan" type is used.

Overwrites the numbering plan of the called destination defined by the application, unless "Standard" has been selected in the drop down menu.

Called Numbering Type:

Defines, how the dialed number will be interpreted by the switchboard.

Overwrites the number format of the called destination defined by the application, unless "Standard" has been selected in the drop down menu.

Calling Numbering Plan:

Defines, which "numbering plan" type is used.

Overwrites the numbering plan of the sender defined by the application, unless "Standard" has been selected in the drop down menu.

Calling Numbering Type:

Defines, how the dialed number will be interpreted by the switchboard.

Overwrites the number format of the sender defined by the application, unless "Standard" has been selected in the drop down menu.

Calling Line Identification Presentation (CLIP) restrictions:

- "CLIP always suppressed":
  Allows the transmission of the extension to the dialed destination
- "Deactivate CLIP message element":
  Prevents the transmission and display of the calling subscriber's phone number at the called subscriber.

M.1.2.3 "CONNECTION" TAB

Point to Point:

Activate this checkbox, if you operate your ISDN card on an ISDN point-to-point interface.
The ISDN line type (point-to-point or multipoint interface) is defined by the network operator.

Point-to-multipoint:

Activate this checkbox, if you operate your ISDN card on an ISDN multipoint interface.
The ISDN line type (point-to-point or multipoint interface) is defined by the network operator.

Permanent D channel layer 2:

When the checkbox is activated, the D channel layer 2 is permanently activated.

Required for the adjustment to different telephone systems (PBXs).

TEI (Terminal Endpoint Identifier):

Define here, which TEI (protocol element of D channel layer 2) shall be used.

Fixed TEI:

Required value between 1 and 63 (assigned by your ISDN service provider) to assign an unique identification to your ISDN card. TEI=0 is the default value for the point-to-point protocol.

Auto TEI (default):

By selecting "Auto TEI", the ISDN card automatically assigns a TEI value. Only in case of point-to-multipoint connections.

Terminal Equipment side:

Device side

e.g. connection to a public line

Network Termination side:

Network termination side

e.g. connection to a subsystem

M.1.2.4 "PRIMARY" TAB (ONLY PRI CARDS)

First B channel:

If you use an ISDN interface with less B channels than the standard ISDN interface, enter the first B channel to be used during connection setup.

Standard setting: 1, for E1 and T1 (European and US standard).

Last B channel:

If you use an ISDN interface with less B channels than the standard ISDN interface, enter the last B channel to be used during connection setup.

Standard setting:

30 for E1 (European standard)

23 for T1 (US standard)

Line code:

Select the line code for the T1 or E1 interface in the list field.

B8ZS for T1 (US standard)

HDB3 for E1 (European standard)

Framing format:

Select the framing format for the T1 or E1 interface in the list field.

Standard setting:

ESF - for T1 (US standard)

CRC4 Multi Frame - for E1 (European standard)

Double Frame - mainly used in France and Belgium.

Bus termination:

Select a bus termination resistance between 75 and 120 ohm in this list field.

M.1.3 WAN PARAMETER

The "WAN parameter" button is deactivated by default. WAN parameters can only be configured, if WAN miniport is activated, *Activate WAN miniport:*, Page 473.

You can choose the "WAN parameter" button directly after activation of the WAN miniport. Close and restart the ISDN card settings.

Incoming calls

Settings for the behavior in case of incoming calls.

Outgoing calls

Settings for the behavior in case of outgoing calls.

B channel protocol:

This option allows you to define the ISDN B channel protocol to be used for incoming calls.

- **HDLC transparent** - required for standard PPP connections.
- X.75 - used for a secure connection (ESS) with suitable remote terminals.
- Automatic Recognition - the ISDN service of the incoming call is recognized automatically.

Standard B channel protocol:

This option allows you to define the default ISDN B channel protocol to be used for outgoing calls.

- HDLC transparent - required for standard PPP connections.
- X.75 - used for a secure connection (ESS) with suitable remote terminals.

Standard: HDLC transparent.

Own MSN/DN (Multiple Subscriber Number / Directory Number):

designates the own Multiple Subscriber Number, which is displayed at the switchboard in case of outgoing calls. Configuration is only required in case of certain switchboards/ telephone systems.

APP. N: APPROVALS, CODES, DATA SHEETS

International codes and approvals for the implemented ISDN- or analogue Gateway boards

N.1 ISDN CARD SX2 QUADBRI

The SX2 QuadBRI is an ISDN card with four S_0 connections. It works with Cologne Chip HFC-4S and was developed especially for the use with SwyxWare. It is manufactured exclusively for Enreach.

This document will use SX2 QuadBRI, if both type of boards are characterized (SX2 QuadBRI and SX2-express DualPRI). Differences, e.g. in the power configuration, are pointed out especially.

ISDN Interface

- 4 x BRI interface
- Each line can be configured individually using a jumper field for the TE or NT mode. The BRI connector (adapter to use an internal S_0) is not necessary for the SX2 QuadBRI
- Short circuit resistance is provided for the ISDN connection via a special fuse (non-blowing, auto-recovery)
- Line termination (100Ohm) is adjustable for each connection individually via a DIP switch.
- A maximum of 4 different cards (SX2 QuadBRI, SX2 SinglePRI and SX2 DualPRI) can be used in one computer. In doing so, a maximum of 76 B channels will be supported. Please note that the SX2 DualPRI is counted as two cards because it will appear as two network cards in the Windows device manager.

PCI Interface

- SX2 QuadBRI
  PCI Interface for 3.3V and 5V PCI 2.2 slots. If necessary, 5V is reduced to 3.3V using a voltage regulator located on the card.
- SX2-express DualPRI
  The board has a PCI express x1 Interface without any further configuration.

PCM Highway

- Tact synchronization between the different SX2 cards is possible. The cards are connected with a ribbon cable.

A mixed usage of PCI and PCI-express board is not supported (incompatible plugs).

- 2/4/8 Mbit/s data transfer rate
- Chipset: Cologne Chip HFC-4S Chip
- Exact 49,152 MHz quartz oscillator
- 512x8bit serial EEPROM for programming the PCI configuration information

Chipset

- Cologne Chip HFC-4S Chip
- Exact 49,152 MHz quartz oscillator
- 512 x 8 bit serial EEPROM for programming the PCI configuration information

General purpose I/O

- Four two-color LEDs (red/green) on the mounting bracket of the SX2 QuadBRI
- Three DIP switches that can be used for the identification of the card
- You will find more recent drivers for the SX2 QuadBRI in the download area of the homepage:
  enreach.com/products/support/support-downloads.html

Conformity Declaration

The ISDN card family SX2 conforms to the hardware specifications of the ISDN standards (I.430, CTR3).

Dimensions of the SX2 QuadBRI

15.5 x 10.5 x 1.3 cm

N.2 ISDN BOARDS SX2-EXPRESS SINGLEPRI / SX2-EXPRESS DUALPRI

ISDN Interface

- SX2-express SinglePRI: 1 x PRI$_{2m}$ interface orSX2-express DualPRI: 2 x PRI $_{2m}$-interface
- Each line can be configured individually using a jumper field for the TE or NT mode.
- Failover relay on the SX2 DualPRI. This enables the two lines to be directly connected to each other in the event of power failure or software problems, so that a PRI external line can be looped through the card.
- A maximum of 4 different cards (SX2 QuadBRI, SX2 SinglePRI and SX2 DualPRI) can be used in one PC. In doing so, a maximum of 76 B channels will be supported.

PCM Highway

- Tact synchronization is only possible between the different SX2-express cards. The cards are connected with a ribbon cable.
- 2/4/8 Mbit/s data transfer rate
- Chipset: Exar XRT86VL
- 6 DIP Switches
- Exact 32,768 MHz quartz oscillator
- PCIe x1 Interface

General purpose I/O

- Four LEDs (red/green) on the mounting bracket of the ISDN card per PRI interface
- Four DIP switches per PRI interface that can be used for the identification of the card
- You will find more recent drivers for the SX2 cards in the download area of the homepage: enreach.com/products/support/support-downloads.html

This is how you install the ISDN cards in your computer

This is how you install the drivers for the ISDN card

This is how you modify the ISDN card driver configuration

This is how you change the line termination of SX2-express SinglePRI or SX2-express DualPRI

N.3 ISDN CARD SX2 SINGLEPRI

- SX2 SinglePRI1 x PRI$_{2m}$ interface (SX2 SinglePRI)
- The line can be configured individually using a jumper field for the TE or NT mode.
- Line termination (120Ohm or 75Ohm) is adjustable via a DIP switch.
- A maximum of 4 different cards (SX2 QuadBRI, SX2 SinglePRIand SX2 DualPRI) can be used in one computer. In doing so, a maximum of 76 B channels will be supported. Please note that the SX2 DualPRI is counted as two cards because it will appear as two network cards in the Windows device manager.

PCI Interface

PCI Interface for 3.3V and 5V PCI 2.2 slots. If necessary, 5V is reduced to 3.3V using a voltage regulator located on the card.

PCM Highway

- Tact synchronization between the different SX2 cards is possible. The cards are connected with a ribbon cable.
- 2/4/8 Mbit/s data transfer rate
- Chipset: Cologne Chip HFC-E1 Chip
- Exact 32,768 MHz quartz oscillator
- 512x8bit serial EEPROM for programming the PCI configuration information

General purpose I/O

- Four LEDs (red/green) on the mounting bracket of the ISDN card
- Four DIP switches that can be used for the identification of the card
- You will find more recent drivers for the SX2 in the download area of the homepage:
  enreach.com/products/support-downloads.html

This is how you install the ISDN cards in your computer

This is how you modify the ISDN card driver configuration

N.4 ISDN CARD SX2 DUALPRI

SX2 DualPRI ISDN Interface

- 2 x PRI $_{2m}$-interface
- Each line can be configured individually using a jumper field for the TE or NT mode.
- Line termination (120Ohm or 75Ohm) is adjustable for each connection individually via a DIP switch.
- Failover relay on the SX2 DualPRI. This enables the two lines to be directly connected to each other in the event of power failure or software problems, so that a PRI external line can be looped through the card.
- A maximum of 4 different cards (SX2 QuadBRI, SX2 SinglePRIand SX2 DualPRI) can be used in one computer. In doing so, a maximum of 76 B channels will be supported. Please note that the SX2 DualPRI is counted as two cards because it will appear as two network cards in the Windows device manager.

PCI Interface

PCI Interface for 3.3V and 5V PCI 2.2 slots. If necessary, 5V is reduced to 3.3V using a voltage regulator located on the card.

PCM Highway

- Tact synchronization between the different SX2 cards is possible. The cards are connected with a ribbon cable.
- 2/4/8 Mbit/s data transfer rate
- Chipset: Cologne Chip HFC-E1 Chip
- Exact 32,768 MHz quartz oscillator
- 512x8bit serial EEPROM for programming the PCI configuration information

General purpose I/O

- Four LEDs (red/green) on the mounting bracket of the ISDN card per PRI interface
- Four DIP switches per PRI interface that can be used for the identification of the card
- You will find more recent drivers for the SX2 in the download area of the homepage:
  enreach.com/products/support-downloads.html

This is how you install the ISDN cards in your computer

This is how you install the drivers for the ISDN card

This is how you modify the ISDN card driver configuration

APP. O:TECHNICAL TERMS

This appendix contains a list of technical terms used in this documentation including their explanations.

Term	Explanation
Line	ISDN line for operating a single ISDN terminal. This is usually a telecommunications system with the option of dialing to an extension. In comparison to the multiple connection, the line has the advantage that the number of extension numbers is not limited.
ACD	Automatic Call Distribution
API	Application Programming Interface Interface for application programs
Block Dialing	All numbers of the destination phone number are entered before the handset has been lifted. In this case, it is still possible to change the phone number after it has been entered. The phone number will be dialed completely (as a block) when the handset is lifted. The opposite of this is ‘Overlap Sending’.
CAPI	Common ISDN Application Programmable Interface CAPI is the software interface, which regulates the data transfer between the ISDN card and the applications. The CAPI is a standard, which also supports the D-channel protocol of the Euro-ISDN (DSS1) in the CAPI Version 2.0.
CCITT	Comité Consultatif International Télégraphique et Téléphonique International consulting committee for telegraph and telephone service; known as ITU-T today
CDR	Call Detail Record A call detail record provides statistical information, such as caller, duration and cost of the connection.
Client computer	The client computer is a single workstation computer (PC). Many client computers are connected to a server via the network.
CLIP	CLIP (Calling Line Identification Presentation) is a feature for incoming calls, and can only be activated or deactivated for these. With CLIP, the number of the caller is transmitted to the called subscriber, unless previously restricted on the calling side (CLIR). If the called subscriber has a terminal device with CLIP capability, the caller's number is displayed. If this device has an address book with the possibility of storing names, the corresponding name can also be displayed.
CLIP no screening	CLIP -no screening- is a feature for outgoing calls, and can only be activated or deactivated for these. In addition to the network provided number for the caller, a user provided number, specified by the caller and not screened, can also be sent to the called party. "no screening" in this context means that the customer-specific number for the caller is not checked for correctness by the transmitting phone network. It can be any number determined by the caller himself. This feature is only possible for ISDN connections on the calling side, and only takes effect for such on the incoming side. For analog connections, only the network provided number is transmitted - assuming CLIR was not activated on the calling side; otherwise none. For example, the caller can suppress his network provided number with CLIR, and send the caller a different customer-specific number, e.g. the company switchboard or a service number. In general both the caller's numbers, the network-provided and the customer-specific, will be transferred in the public telephone network (if CLIP -no screening- is activated). However, activated services such as CLIP/CLIR on the respective subscriber side (and the type of connection) will decide which number is transmitted to the subscriber himself. Device-specific settings on the receiving side ultimately decide which number is displayed, or whether both are.
CMI	Cordless Multicell Integration Multicellular wireless network for cordless equipment

Term	Explanation
CorNet®	A protocol developed by Siemens AG and used by SwyxPhone Lxxx to communicate with SwyxServer. This connection is only used to transmit information to the server, e.g. via an activated button, and to send display information from the server to SwyxPhone. The actual telephony functions are carried out in SwyxServer.
CTI	Computer Telephony Integration Term used for the connection of telecommunications systems and computer systems (e.g. databases) using a special interface. This enables the user to use telephony services from a computer.
DECT	Digital Enhanced Cordless Telecommunication European Standard for the digital cordless communication between a base station and a transportable device for the range of a few hundred meters.
DHCP	Dynamic Host Configuration Protocol Instead of permanently assigning an IP address to a computer in a LAN, DHCP makes it possible to assign IP addresses dynamically and variably. Applications, which depend on an IP address, are immediately assigned one upon request.
DDI	Direct Dial In DDI refers to the direct dial from a telephone network to a subscriber. Direct dial allows you to dial specific extensions directly via this number.
DMZ	Demilitarized Zone In the context of firewalls, a DMZ is a protected logical network segment which contains the publicly accessible services of a company. Thus, a DMZ prevents external access to internal IT structures.
DNS	Domain Name Server A server, which translates the symbolic name (e.g. www.microsoft.com) into an IP address.
DTMF	Dual Tone Multi Frequency Seven different frequencies and additional mixture frequencies are transmitted in the telephone line in order to clearly communicate the activated button.

Term	Explanation
DSP	Digital Signal Processor
Direct Dialing-In line	ISDN line, to which a telecommunications system with so-called extension numbers is connected, which can be used to directly contact a subscriber. In the case of the number "(0231) 4777-227, "227" is the extension number within a telecommunications system. An extension number allows you to dial a specific extension of a telecommunications system directly via this defined number.
E.164	ITU-T standard for global telephone numbering (country code, local area code and subscriber number, e.g.+44 (20) 123456-789.
ENUM	tElephone NUmber Mapping ENUM is an application of the Domain Name System for converting telephone numbers (in the E.164 format) to Internet addresses. An ENUM registration of a VoIP number allows calls to be placed directly via the Internet, for example.
Ethernet	Network for limited local operation (10 m to 10 km) in the LAN. The individual computers are connected via a cable network. Data is transferred within this network at a rate of 10Mbit/s, 100Mbit/s or 1Gbit/s.
FD	Full Duplex (DX, sometimes also FDX, permits simultaneous transmission of information in both direction, e.g. in telephony)
FTP	File Transfer Protocol (Network protocol for file transmission)
G.711	ITU standard for compression, here: Audicodec 64 kbit/s
G.722	ITU standard for compression, here: Audicodec 64 kbit/s
G.723.1	ITU standard for compression, here: Audiocodec 5.3 kbit/s and 6.3 kbit/s
G.729	ITU standard for compression, here: Audicodec 8 kbit/s

Term	Explanation
GAP	Generic Access Protocol Standard for DECT Handsets, which allows the communication between handsets and basis stations of different manufacturers.
Gateway	A gateway is a system, which connects two different networks and which can transfer the data in one network to the other network and vice versa. This means that the physical networks can be different and the protocols used (e.g. IP network and ISDN) can also be different.
GSM	Global System for Mobile Communication Global system for mobile communication
H.323	A collection of international specifications (ITU), which define the transmission of multimedia data to packet-oriented data connections.
H.323 Alias Name	A symbolic name (e.g. TOMMY), which can be used as the address of an H.323 terminal instead of an IP address.
H.450	Standard for additional performance specifications in H.323, such as Conference, Call Forwarding, Hold, Call Swap, etc.
HTTP	Hypertext Transfer Protocol. A protocol for transmission of data over a network. It is mainly used for loading websites and other data from the World Wide Web (WWW) into a Web browser.
Hub	A hub creates a network node in a star-shaped LAN and it connects several clients to the network.
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers International standardization committee

Term	Explanation
Instant Messaging	(Immediate message transfer). A service that uses the Instant Messenger software (client) to enable real-time communication (chat) with other subscribers. Short text messages are sent using push technology via a network (server) to the recipient (usually via the Internet), who can respond to them immediately. Files can usually also be exchanged by this means. In addition, many messaging programs offer video or telephone conferences.
IPEI	Hardware address (12 digits) of a DECT handset which allows an unique identification.
IP	Internet Protocol Fundamental protocol of the Internet, which combines packet-oriented networks with different technical bases to one large network. Thus this protocol (on layer 3 of the OSI layer model) is used for addressing and distributing data into packets.
IP-adress	An IP address is a 32-bit number, which is usually shown as a four-part number, e. g. 192.177.65.4, and which is assigned to every computer connected to the Internet. Domain names, which are unambiguously assigned to IP addresses using a DNS server, were introduced in order to make these addresses simpler and clearer for users.
IP PBX	IP Private Branch Exchange A telephone private branch exchange (PBX) which is created by a software application. It uses Voice-over-IP (VoIP) technology for voice transmission.
ISDN	Integrated Services Digital Network Service integrating digital network
ITSP	Internet Telephony Service Provider. An Internet telephony service provider offers an interface via a gateway between Internet telephony and the classic telephone network. Thus via an ITSP, VoIP users can also reach subscribers in the classic telephone network, and vice versa.
IVR	Interactive Voice Response Interactive Call handling

Term	Explanation
LAN	Local Area Network A local network, which is made up of numerous, interconnected computer terminals within one company location and which is used to transfer data.
LDAP	Lightweight Directory Access Protocol A network protocol that allows querying and modification of information of a directory service (a distributed hierarchical database in the network). The current version is specified in RFC 4511.
LED	Light Emitting Diode Light emitting diode (small light) for displaying status information, e.g. for SwyxPhone.
MAC-adress	Medium Access Control Address Each network card identifies itself with the MAC address. This address is an 8-byte address, which is uniquely defined worldwide.
MAPI	Mail Application Programming Interface This Microsoft interface can be used by applications to send E-mails.
Multiple connection	Basic Rate Interface for operating up to eight ISDN terminals (ISDN telephones etc.) on a S0 bus. It is possible to operate ISDN telephones, ISDN cards or ISDN telecommunications systems on a multiple connection. The devices are addressed via MSNs.
MSN	Multiple Subscriber Number A non-direct dialing-in line can have several numbers (MSNs). The assignment of these MSNs to the terminals takes place in the terminals themselves.

Term	Explanation
Name Resolution	Automatic association of a name to a phone number. ***Example:*** *You receive a call from the public telephone network and the caller's phone number is transmitted. SwyxWare then searches, e.g. in Microsoft Outlook Contacts and in the Personal Phonebook, for a contact matching this phone number. If a contact is found, SwyxIt! will show the name of the caller in addition to the phone number in the display.*
NAT	Network Address Translation is a method for replacing an IP address by another within a data package. This method is frequently used to map private IP addresses to public IP addresses.
NT mode	Network Terminator For ISDN (and other protocols) a different behavior is often required, depending on functionality. For ISDN, the exchange operates in NT mode and the telephones (terminals) operate in TE mode. An example of different behavior is the transfer of charging information, which of course is only possible from NT to TE, and not the other way round.
NetBIOS Name	A symbolic name (e.g. WS-SJONES), which is used for addressing a computer, if this computer should be contacted using the Microsoft NetBIOS protocol.
Opus	Open Standard RFC 6716 (.opus) Dynamically adjustable bit rate. Best audio quality / storage space ratio.
Overlap Sending	The numbers entered are dialed immediately. The destination phone number can no longer be edited. The opposite of this is 'Block dialing'.
P2P	see *Peer-to-Peer*, Page 484
PABX	Private Automatic Branch Exchange Private branch exchange

Term	Explanation
PBX	Private Branch Exchange Controlling device for telephone systems within a small telephone network, including transition to a public telephone network.
PDA	Personal Digital Assistant. Small portable computer, usually equipped with a quick start operating system, and used along with many other programs mainly for personal calendar, address and task management.
PIN	Personal Identification Number This number is linked to the user name, and is used for user authentication.
Peer-to-Peer	Network principle in which the data exchange occurs decentrally, directly between the individual computers. In the VoIP field, this means that the connection exists directly between the two subscribers, without server or provider.
POTS	Plain Old Telephony System This is the classic analog telephone.
Power over LAN	Power over LAN is used to identify a property of devices with Ethernet connection, e.g. IP telephones. Thus, the power supply is provided via the Ethernet connection line and not via a power mains plug, as usual. In this case, the Switch or the Hub to which this device is connected per Ethernet must be able to guarantee the power supply via the Ethernet line.
PSTN	Public Switched Telephone Network Umbrella term for analog telephone networks, which usually use digital switches.
QoS	Quality of Service The quality in communication networks. Depending on the standard or protocol, different parameters are used for evaluating the properties, such as loss rate, availability, transfer rate and delay.

Term	Explanation
Router	A router connects different kinds of networks to each other. It recognizes the bordering networks and neighboring routers and it determines the path of the data packet. This connection can be created by using either a software or a hardware solution.
RSVP	Resource Reservation Protocol IETF standard to guarantee a certain transmission qualities, such as bandwidth and priority via TCP/IP.
Servers	The workstation computers are connected (e.g. via Ethernet) to the server, which is the "central computer".
SIP	Session Initiation Protocol A network protocol which establishes a communication session between two or more subscribers.
Smartphone	A smartphone unites the functional scope of a mobile phone with that of a PDA. You can use a full keypad or touch screen and speak from a PDA phone. Digital cameras are sometimes also incorporated, as in many mobile phones.
SNMP	Simple Network Management Protocol Network protocol developed by the IETF - an open international voluntary association of network engineers, manufacturers and users, which is responsible for proposals for Internet standardization -, to enable network elements (e.g. routers, servers, switches, printers, computers etc.) to be monitored and controlled from a central station.
SNTP	Simple Network Time Protocol Standard for synchronizing clocks in computer systems over packet-based communication networks. Although mostly handled via UDP, can also be transported using other layer 4 protocols such as TCP. Specifically developed to enable reliable timing over networks with variable packet propagation time (ping).
Voice Compression	The voice data are compressed and sent via the network. This reduces the amount of data to be transmitted. This is especially important for the Home Office connection and the coupling of several branch offices via the Internet.

Term	Explanation
STUN	STUN is a simple network protocol that recognizes the existence and type of firewalls and NAT routers and uses this information to bypass them.
Subnet	A network can be divided into several subnets. For example, it is possible to use the IP address 192.177.65.xxx to address all computers, which have the number 192.177.65. in common and which only differ from one another in terms of the last three digits (xxx). The subnet mask indicates which positions should be used for differentiation within the subnet. In a subnet, two subscribers communicate directly with each other. The IP packets only have to pass through the router if subscribers communicate outside of the subnet.
Switch	A Switch is an active hub, which functions as a kind of exchange. In contrast to the hub, the switch does not forward the incoming data packets to all lines, but rather only to that line which leads to the destination of the packet.
TA	Terminal Adapter
TAPI	Terminal Application Programming Interface Interface for programming terminal applications
TE mode	Terminal Endpoint see *NT mode*, Page 483
TEI	Terminal Endpoint Identifier With the help of the TEI, different terminals are addressed to an ISDN bus on Layer 2.
TCP/IP	Transmission Control Protocol / Internet Protocol Two commonly used protocols for the transfer of data and for Internet connection, which can be implemented on different types of transport media.
TLS	Transport Layer Security Internet protocol for encrypted data transfer (SSL advancement)
TSP	TAPI Service Provider, driver for TAPI devices

Term	Explanation
Unified Messaging	Message management system developed in 1989. It refers to a method of converting incoming and outgoing messages in any form (e.g. voice messages, e-mail, fax, SMS, MMS, etc.) into a standardized form and granting the user access to these via various clients (landline or cell phone, e-mail client).
USB	Universal Serial Bus. Bus system for connecting a computer to ancillary equipment. A USB port takes little space, and can supply power to simple devices such as a mouse, a phone or a keyboard. Devices equipped with USB can be connected to each other during active operation (hot plugging), and their properties can be detected automatically.
VLAN	Virtual LAN. Virtual local network within a physical network. A widespread technical implementation of VLANs is partially defined in the standard IEEE 802.1Q.
VoIP	Voice over IP Collective term for all techniques for transmitting voice over IP networks.
WAP	Wireless Application Protocol. The Wireless Application Protocol denotes a collection of technologies and protocols, whose aim is to make Internet content available for the slower transmission rates and the longer response times in mobile radio, as well as for the small displays of mobile telephones. WAP is thus in direct competition with the i-mode services.
WAV	File format in which speech or music is recorded, e.g. announcement texts, music on hold or voice messages. 16KB of memory are required for each recorded second.